CONFIDENCIALITAT,

NORMES D'ÚS DELS RECURSOS TIC I

PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

CCOO de Catalunya

DRETS I DEURES DE LA

PERSONA USUÀRIA

(LABORAL/SINDICALISTA)

DELS SISTEMES D'INFORMACIÓ

Informació del document

Títol	Confidencialitat, normes d'ús dels recursos TIC i protecció de dades de caràcter personal
Arxiu	20240124_SGCN _NO_Confidencialitat, normes d'ús dels recursos TIC i protecció de dades de caràcter personal_v04
Tipus de document	Norma
Versió	04

Control de canvis

CONTROL DE CANVIS					
Versió	Data	Canvis	Organisme responsable	Revisor	Aprovador
01	22.03.2003	Creació	DICONC	DICONC	
02	01.02.2007	Actualització	DICONC		
03	01.06.2008	Actualització	DICONC		
04	06.03.2024	Actualització	SISCOM	GRUP TEN	CN

Llista de distribució

Col·lectius	Canal	Data
Persones usuàries de la intranet	GESPER, acceptació	

1. OBJECTIU DEL DOCUMENT

Aquest document té per objecte contribuir a racionalitzar la utilització dels sistemes d'informació de la CS de la CONC i les seves entitats vinculades (Fundació Paco Puerto, Fundació Cipriano Garcia, Fundació Pau i Solidaritat i Associació CITE) —d'ara en endavant, l'organització— i donar compliment a la legislació sobre protecció de dades personals i de serveis en la societat de la informació, en què s'estableix que els responsables de tractament d'informació i comunicació d'informació tenen l'obligació d'adoptar les mesures tècniques i organitzatives que garanteixin la seguretat de les dades.

Aquestes normes d'ús poden ser modificades com a conseqüència de circumstàncies legals o organitzatives que així ho requereixin, així com de l'harmonització necessària amb les normes confederals, incloent-hi les que derivin dels acords en el marc de les relacions laborals de l'organització. Així mateix, aquestes normes han d'estar complementades per les polítiques i els procediments definits en el marc del sistema de gestió de seguretat de la informació. Aquest document es troba a la xarxa corporativa INTEGRA, a l'apartat de "Compliment normatiu", perquè pugui ser consultat per les persones usuàries del sistema d'informació de l'organització.

La seguretat sempre ha estat un concepte present a tots els sistemes de gestió de la informació i d'ús de les tecnologies de la informació i la comunicació (TIC). La seva implementació no és senzilla, perquè abasta totes les baules de la cadena de gestió de la informació i requereix un gran conjunt de mesures organitzatives i tecnològiques.

Una de les baules normalment més febles de la cadena de gestió de la informació és precisament la persona usuària final del sistema, en l'àmbit informàtic i en paper.

La persona usuària necessita, per tant, ser conscienciada en matèria de seguretat de la informació i, alhora, ha de disposar d'unes normes de compliment obligat respecte de l'ús dels sistemes informàtics al seu abast, així com suports o documents en paper, i, amb una rellevància especial, quant a preservar la confidencialitat de la informació de caràcter personal que estigui sent tractada.

Aquest document estableix les normes d'ús de l'ordinador assignat al lloc de treball, la xarxa corporativa, els equips portàtils, les aplicacions informàtiques, les línies corporatives de telèfon fix i de mòbil, i, en definitiva, de tots aquells elements que integren el sistema d'informació, així com l'accés i el tractament de dades de caràcter personal, en l'àmbit informàtic i en suport paper, per a la realització de les tasques relacionades amb les funcions pròpies del lloc de treball o de la responsabilitat sindical, segons es tracti de personal laboral o sindicalista.

És fonamental que totes les persones usuàries que utilitzen equipament informàtic i hi accedeixin o tractin informació de caràcter personal per a la realització de les seves funcions i tasques siguin coneixedores d'aquestes normes.

El Departament de Sistemes d'Informació i Compliment Normatiu —d'ara en endavant, SISCOM—, responsable dels equipaments informàtics i de l'atenció a les persones usuàries, s'ha d'encarregar de definir l'equipament necessari i la configuració de maquinari i programari dels llocs de treball i administrar-los accessos a la xarxa confederal conjuntament amb les persones responsables corresponents de les organitzacions de la CONC.

La persona usuària ha de conèixer i tenir present les obligacions que assumeix quan utilitza els sistemes d'informació titularitat de l'organització.

2. CONFIDENCIALITAT I DEURE DE SECRET

Tot el personal, en el marc de la relació laboral, dedicació sindical o prestació de serveis que l'uneix a l'organització, es compromet a:

1. No revelar a cap persona aliena a l'organització, sense el consentiment de la mateixa organització, la informació referent a la qual hagi tingut accés durant l'exercici de les seves funcions, excepte en el cas que això sigui necessari per acomplir les seves obligacions imposades per lleis o normes que siguin aplicables, o sigui requerit per fer-ho per mandat de l'autoritat competent d'acord amb el dret.
2. Utilitzar la informació a què al·ludeix l'apartat anterior únicament de la manera que exigeixi l'exercici de les seves funcions i no disposar-ne de cap altra manera o amb una altra finalitat.
3. No utilitzar de cap manera qualsevol altra informació que s'hagi pogut obtenir prevalent-se de la seva condició de persona usuària o col·laboradora, i que no fos necessària per a l'exercici de les seves funcions.
4. Complir, en el desenvolupament de les seves funcions per a l'organització i les entitats vinculades, la normativa vigent relativa a la protecció de dades de caràcter personal i, en particular, el Reglament (UE) 2016/679 (Reglament general de protecció de dades), la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), i els protocols i les normes internes que s'hagin aprovat en el desenvolupament d'aquesta matèria.
5. Complir els compromisos anteriors, fins i tot després d'extingida, per qualsevol causa, la relació de la persona usuària amb l'organització.
6. En funció de les seves responsabilitats sindicals assumides, cal observar un deure especial de secret i confidencialitat de les dades personals i informacions conegudes.
7. En el cas de ser delegat o delegada sindical o membre de l'RLPT (representació legal de les persones treballadores) dels diferents àmbits del grup CS de la CONC, l'Estatut dels treballadors (ET) estableix un deure de sigil, aplicable als membres de l'RLPT de l'organització i del comitè en el seu conjunt, així com, si escau, les persones expertes que els assisteixin respecte d'aquella informació que, en legítim i objectiu interès de l'entitat i en compliment de la legalitat vigent, se'ls hagi comunicat expressament amb caràcter reservat. Tal com estableix l'ET, en tot cas, cap tipus de document lliurat per l'organització a l'RLPT no pot ser utilitzat fora de l'estricte àmbit d'aquella ni per a fins diferents dels que en van motivar l'entrega. El deure de sigil subsisteix, fins i tot, després de l'expiració del mandat i independentment del lloc on es trobin.

3. POLÍTICA D'ÚS DELS SISTEMES O DISPOSITIUS POSATS A DISPOSICIÓ DE LA PERSONA USUÀRIA

Els recursos TIC de l'organització i els dispositius digitals que es descriuen en aquesta política són per a fins professionals, laborals i sindicals, i, per tant, no s'han d'utilitzar per a fins particulars, tret dels usos autoritzats en els termes que s'exposen en aquest document.

4. PROPIETAT I ÚS DELS ORDINADORS PERSONALS

L'organització facilita a les persones usuàries els dispositius i l'equipament informàtic necessaris per a la realització de les tasques relacionades amb la seva activitat professional o sindical.

Aquest equipament és propietat de l'organització i no es permet utilitzar-lo amb finalitats personals.

La regulació dels equips propis posats a disposició de la dedicació sindical és objecte d'una instrucció específica.

El SISCOM, d'acord amb els criteris generals establerts per l'Organització, és el responsable de definir la configuració bàsica de maquinari i programari dels llocs de treball i d'administrar els accessos a la xarxa corporativa. Qualsevol necessitat de modificació del lloc ha de ser formulada per la persona responsable de la direcció o unitat que la sol·licita.

Les persones usuàries han de complir les mesures de seguretat següents establertes per l'organització per a l'ús dels ordinadors personals:

1. No es permet alterar la configuració física dels equips ni connectar altres dispositius a iniciativa de la persona usuària, així com variar-ne la ubicació.
2. No es permet alterar la configuració del programari dels equips ni desinstal·lar o instal·lar programes o qualsevol altre tipus de programari diferent del de la configuració lògica predefinida.
3. No es permet la connexió de cap tipus d'equip o dispositiu a la xarxa corporativa.
4. La còpia de seguretat periòdica de les dades allotjades als servidors corporatius és responsabilitat del SISCOM.
5. Està prohibit utilitzar, copiar o transmetre informació continguda als sistemes informàtics per a ús privat o qualsevol altra de diferent del servei al qual està destinada.
6. Els dispositius mòbils (portàtils, tauletes, telèfons mòbils…) tenen la mateixa consideració de llocs de treball i es regeixen per aquestes mateixes normes. L'ús al qual estan destinats i la possibilitat que aquests equips s'utilitzin fora de l'entorn de seguretat de la xarxa corporativa de l'organització fa necessaris procediments de seguretat específics en relació amb l'actualització dels sistemes antivirus i del programari instal·lat.
7. Els equips portàtils, així com els dispositius o els suports informàtics únicament i exclusivament estan posats a disposició amb la finalitat de permetre l'exercici de les funcions i les tasques professionals o sindicals encomanades.
8. Les contrasenyes d'accés a l'equip, al sistema i/o a la xarxa concedits per l'organització són personals i intransferibles, i la persona usuària és l'única responsable de les conseqüències que es puguin derivar del seu mal ús, divulgació o pèrdua. D'aquesta manera, està prohibit, entre d'altres:
    a. Emprar identificadors i contrasenyes d'altres persones usuàries per accedir al sistema i a la xarxa de l'organització.
    b. Intentar modificar o accedir al registre d'accessos.
    c. Burlar les mesures de seguretat o de control establertes al sistema informàtic.
    d. En general, emprar la xarxa corporativa, els sistemes, els equips informàtics i qualsevol mitjà posat a l'abast de la persona usuària, vulnerant el dret de tercers, els propis de l'organització o bé per fer actes que es puguin considerar il·lícits.
9. Queda prohibit terminantment apropiar-se d'informació de qualsevol tipus de suport titularitat de l'organització per a ús particular i/o de tercers. És per això que, en aquest sentit, cal abstenir-se de copiar la informació continguda als fitxers on s'emmagatzemen dades de caràcter personal o un altre tipus d'informació de l'organització en ordinador propi, llapis de memòria o qualsevol altre suport informàtic. En cas que fos necessari, han de ser eliminats una vegada hagin deixat de ser

útils i pertinents per a la satisfacció dels fins que en van motivar la creació. Així mateix, durant el període de temps en què els fitxers o els arxius romanguin a l'equip o al suport informàtic propietat de la persona, s'ha de restringir l'accés i la utilització de la informació que contenen.

10. En cas que, excepcionalment, fos necessari l'ús de dispositius extraïbles (llapis de memòria, per exemple), caldrà sempre que estiguin xifrats i autoritzats pel SISCOM.
11. En relació amb això, s'ha de restringir a tercers (familiars, amistats o qualssevol altres) l'accés als arxius o als fitxers titularitat de l'organització i disposats únicament per a les funcions o les tasques exercides per a l'organització.
12. S'han d'establir mesures de protecció addicionals que assegurin la confidencialitat de la informació emmagatzemada a l'equip quan la persona usuària així ho sol·liciti o quan es tracti de dades de caràcter personal que requereixin les mesures de seguretat establertes per la legislació vigent.

5. ÚS DE LA XARXA CORPORATIVA

La xarxa corporativa és un recurs compartit i limitat. Aquest recurs serveix no només per a l'accés de les persones usuàries a la intranet o a Internet, sinó també per a l'accés a les diferents aplicacions informàtiques corporatives i a la comunicació de dades entre sistemes de temps real i explotació.

Com a regla general, la persona usuària ha de saber que tots els recursos de l'organització, inclosa la connexió a Internet, els ordinadors i els dispositius mòbils o portàtils, i la línia corporativa de telèfon mòbil, són per a fins estrictament laborals i sindicals. Per tant, no poden ser utilitzats amb altres fins.

Emmagatzematge d'informació a la xarxa informàtica corporativa. Tota la informació ha de ser emmagatzemada al servidor o servidors habilitats a aquest efecte, i s'ha d'evitar albergar informació fora d'aquest entorn (discos locals, discos extraïbles, sistemes o serveis de fitxers externs, etc.).

La capacitat d'emmagatzematge és limitada. La persona usuària es compromet a fer bon ús de l'espai habilitat per l'organització, revisant regularment la informació continguda amb l'objectiu de comprimir aquesta informació i d'eliminar la que ja no li sigui necessària.

La persona usuària, quan finalitzi la relació amb l'organització, ha de deixar intacta la informació que hagi tingut una finalitat professional o sindical, i queda prohibida la sortida de l'organització de tota mena d'informació, suport, programa, document, etc., a què hagi tingut accés durant la prestació del servei professional o sindical.

Nota important: queda prohibit emmagatzemar dades de qualsevol índole als discs durs locals o a l'espai local. El SISCOM no es fa responsable de la informació no emmagatzemada als servidors. Els fitxers de caràcter temporal han de ser esborrats una vegada hagin deixat de ser necessaris per als fins que en van motivar la creació.

6. ACCÉS I ÚS D'APLICACIONS I SERVEIS

Gran part dels procediments administratius es gestionen actualment accedint des d'ordinadors personals a aplicacions que resideixen en servidors connectats a la xarxa corporativa.

Les persones usuàries han de complir les mesures de seguretat següents establertes per l'organització per a l'ús d'aplicacions i serveis corporatius:

1. Tant l'accés a l'ordinador com a les diferents aplicacions corporatives ha de ser identificat (mitjançant usuari i contrasenya, o un altre mecanisme) i prèviament autoritzat per la persona responsable corresponent. Tots els comptes d'accés han de tenir un sistema de verificació addicional per evitar la suplantació d'identitat.
2. La custòdia de la contrasenya és responsabilitat de la persona usuària. No s'ha d'utilitzar mai el compte d'usuari assignat a una altra persona.
3. Les contrasenyes no s'han d'anotar, sinó que s'han de recordar.
4. Les contrasenyes s'han de canviar sistemàticament segons els procediments establerts en cada moment. Les persones usuàries disposen de mecanismes per modificar la contrasenya d'accés sempre que ho considerin convenient. Això en garanteix l'ús privat.
5. Quan es consideri que la identificació d'accés s'ha vist compromesa, s'ha de comunicar a la persona responsable corresponent.
6. En abandonar el lloc de treball s'han de bloquejar o tancar les sessions amb les aplicacions establertes, i apagar els equips en finalitzar la jornada laboral, excepte en els casos en què l'equip hagi de romandre encès.

Utilització de programes no autoritzats:

7. La instal·lació de programes informàtics l'ha de fer sempre el SISCOM, garantint la disposició de les llicències necessàries per a la utilització del programari que correspongui.
8. Es prohibeix expressament la utilització de programes per als quals l'organització no hagi obtingut una llicència prèvia. Cal advertir que la utilització de programes informàtics sense l'autorització deguda (pirateig de programari) pot ser constitutiva de delicte i que la persona usuària pot incórrer, així mateix, en responsabilitats de diferent ordre. Per evitar aquestes infraccions, l'organització pot fer ús de la seva facultat de revisió en els termes descrits en aquest document.
9. Si per motius justificats, i excepcionalment, la persona usuària requereix l'emmagatzematge d'arxius informàtics de caràcter privat o de programari específic diferent de l'estàndard, ho ha de sol·licitar expressament al SISCOM.

7. ÚS D'INTERNET

7.1. Principis generals d'ús i navegació per Internet

1. És política de l'organització que les connexions a Internet i l'accés a pàgines web obeeixin sempre a fins professionals, tot això amb el propòsit d'obtenir el millor aprofitament possible dels recursos informàtics.
2. Queden expressament prohibides les descàrregues de pel·lícules, clips, vídeos, música, imatges, fotografies, programari o presentacions, i l'ús de programes de compartició de continguts que no obeeixin a fins estrictament professionals.
3. Queda expressament prohibit l'accés a aquelles adreces d'Internet les pàgines de les quals tinguin algun dels continguts següents: (*i*) pornografia, pedofília, racisme que promoguin delictes d'odi i violència de génere i, en general, continguts que puguin resultar ofensius o que puguin atemptar

contra la dignitat humana, (*ii*) apostes i jocs, (*iii*) xats restringits (*chatrooms*) o comunicacions personals en línia i (*iv*) qualsevol altres de naturalesa anàloga a les anteriors que no obeeixin a fins estrictament laborals o sindicals.

4. Sens perjudici de la prohibició general establerta en el paràgraf anterior, es permet l'accés a determinades adreces a aquelles persones usuàries que ho necessitin per a l'exercici de la seva feina, sempre que hagi estat prèviament autoritzat pel SISCOM.
5. Queda garantit, no obstant això, l'accés a l'espai reservat dins dels dominis de CCOO de Catalunya per a la informació sindical i laboral que es determini de mutu acord amb l'RLPT.
6. Es recomana no utilitzar una xarxa oberta de wifi, així com evitar la navegació per pàgines no segures o altres programes maliciosos que malmetin la informació del sindicat.

7.2. Internet i copyright

1. La informació difosa o divulgada a Internet pot estar protegida per les lleis de propietat intel·lectual o per les lleis reguladores del dret de marca, tant de caràcter nacional com internacional.
2. La còpia, sense l'autorització deguda, de continguts protegits per les lleis de propietat intel·lectual o per les lleis de propietat industrial està expressament prohibida.
3. Les persones usuàries han de comprovar amb cura, abans d'utilitzar informació provinent de la xarxa, si aquesta està protegida per les lleis de la propietat intel·lectual o per les lleis de marques, patents, etc.
4. En cas que la informació hagi estat protegida, la persona usuària s'ha d'abstenir d'utilitzar aquesta informació, llevat que hi hagi autorització expressa de la persona titular del dret. En cas de dubte, la persona usuària o empleada s'ha d'abstenir de fer servir aquesta informació amb fins professionals.
5. En tot cas, les persones usuàries que utilitzin documents o informació per a ús professional que trobin mitjançant cerques a Internet han de citar la font de la qual han obtingut aquesta informació, d'acord amb les regles estàndard de fonts esmentades.

8. ÚS DEL CORREU ELECTRÒNIC

8.1. Principis generals

1. L'organització pot subministrar al personal una adreça individual de correu electrònic per a l'exercici de la seva activitat i, com a tal, la seva utilització ha d'estar relacionada amb les comeses encomanades.
2. Està prohibida la seva utilització com a instrument per a l'intercanvi de missatges de text, imatges, programes, arxius o qualsevol altre tipus d'informació quan el seu contingut pugui ser considerat ofensiu o il·lícit, o bé atemptar contra la dignitat humana o els drets fonamentals.
3. En conseqüència, el correu electrònic ha de ser utilitzat per comunicar-se amb finalitats professionals o sindicals. Els enviaments massius d'informació només els poden fer les persones usuàries autoritzades i s'han de realitzar pels mitjans que indiqui l'organització a través del sistema de gestió.
4. Igual que la resta d'informació que s'utilitza en l'exercici del treball, això no podrà sortir de l'espai de l'organització. Aquest pot emmagatzemar els missatges de correu als servidors de l'organització o on indiqui el SISCOM mentre mantinguin alguna utilitat.
5. En cas d'accés al correu electrònic corporatiu al dispositiu mòbil privat, s'ha de canalitzar a través del SISCOM per adoptar les mesures de seguretat oportunes.

6. Sens perjudici del que estableixen aquestes normes i el procediment de gestió de les persones usuàries i sempre per un interès legítim de l'organització, pot ser necessari disposar de la informació disponible al correu electrònic. És per això que no es pot garantir la privadesa de les comunicacions realitzades a través del correu electrònic, per la qual cosa, atesa la finalitat professional o sindical del compte de correu electrònic, aquestes no es poden considerar privades i no són apropiades per remetre informació de caràcter privat.
7. En finalitzar la relació professional o sindical amb el sindicat, el correu electrònic deixarà d'estar operatiu i no se'n farà ni clonatge ni derivació de missatges a un altre correu personal.

8.2. Responsabilitat de la persona usuària

1. Cada persona usuària serà l'única responsable de l'ús inadequat del seu compte de correu electrònic.
2. La persona usuària pot ser subjecte actiu de determinats delictes o faltes previstos en el Codi penal mitjançant la utilització del correu electrònic, com ara pirateig ètic (*hacking*), propagació de virus, pornografia, etc. Així com en tot allò descrit en l'apartat 7.13, queda terminantment prohibida la utilització del correu o d'altres instruments de treball per a aquests propòsits. La persona usuària és l'única responsable per la comissió d'aquests fets delictius i no serà, en cap cas, responsabilitat de l'organització, que manifesta, a través d'aquest document, el seu clar i exprés compromís per evitar la comissió d'aquests actes delictius per part de personal i persones col·laboradores.
3. Queda prohibit l'enviament de missatges obscens, ofensius o difamatoris, o que puguin suposar assetjament laboral o sexual. L'organització no tolera cap tipus d'actuació a través dels mitjans de comunicació posats a disposició de les persones usuàries que pugui considerar-se assetjament laboral o sexual a la feina, i convida les persones afectades a fer arribar aquesta circumstància, en cas que es conegui, a les persones responsables o a través dels canals de comunicació habilitats per l'organització a aquest efecte.
4. A l'efecte del que preveu la clàusula anterior, es considera difamació la publicació de qualsevol declaració, manifestació o afirmació que tendeixi a infravalorar o desmerèixer en la consideració aliena una persona concreta i determinada.

9. ÚS DELS SISTEMES DE COMUNICACIÓ TELEFÒNICA

9.1. Ús del telèfon fix

L'organització pot posar a disposició del personal terminals de telèfon fixos a fi de facilitar-ne el desenvolupament de l'activitat professional. L'ús ha de ser estrictament professional.

L'ús indegut dels telèfons de l'organització per part de les persones usuàries o empleades donarà lloc a l'aplicació de les mesures disciplinàries oportunes per part de l'organització.

9.2. Ús del telèfon mòbil de l'organització o línea corporativa de mòbil

En funció de les característiques de l'activitat professional que hagi de desenvolupar determinat personal de l'organització, es pot posar a disposició l'ús de telèfon o de línia mòbil corporativa.

1. La línia de telèfon mòbil és propietat de l'organització i, com a eina necessària de treball, el seu ús per part de la persona usuària ha de ser professional.

2. En finalitzar la relació professional o sindical amb el sindicat, la línia mòbil o dispositiu pot ser reutilitzada per una altra persona usuària, si així ho determina l'organització.
3. L'ús indegut de les línies esmentades per a fins privats pot donar lloc a l'adopció, per part de l'organització, de les mesures disciplinàries que consideri oportunes. En qualsevol cas, l'organització es reserva la possibilitat de facturar el cost en trucades personals realitzades per la persona usuària en cas que se superin els límits individualitzats estipulats per l'organització.

9.3. Ús del telèfon mòbil privat durant la jornada laboral

En cas que, per necessitat derivada de l'activitat, es requereixi la connexió del telèfon mòbil privat a la xarxa de dades corporativa, cal establir-ho a través dels sistemes i protocols establerts pel SISCOM.

La regulació de l'ús de dispositius personals (portàtils, telèfon intel·ligent, tauletes), propietat de l'usuari, en l'àmbit corporatiu es recollirà en una instrucció específica a aquestl efecte.

10. USOS AUTORITZATS

1. No es permet l'ús del correu electrònic corporatiu per a fins privats o particulars d'acord amb el que estableixen aquestes normes.

2. Per a qüestions particulars podreu accedir al correu electrònic diferent del que proporciona l'organització (Hotmail, Yahoo, Gmail, etc.).

3. Es permet, amb caràcter excepcional, l'ús del mòbil corporatiu amb finalitat personal tolerable i no abusiva. S'informa les persones usuàries que l'organització té coneixement de les trucades fetes quan es procedeix a la gestió de la facturació.

4. Queda restringit a un ús racional i ocasional l'accés a Internet per a fins no relacionats amb les funcions laborals o sindicals encomanades.

5. Es permet una utilització excepcional dels equips i dispositius per a activitats personals no confidencials, sempre sota el criteri de la prudència i l'ús racional. En cas que hi hagi arxius de caràcter personal dins d'aquest ús permès, la persona usuària els ha d'eliminar com més aviat millor.

6. No es permet l'ús de programes xat, missatgeria instantània, etc., llevat que estiguin vinculats a l'exercici professional de les funcions encomanades. L'ús de xarxes socials es limita a un ús racional, llevat del personal autoritzat en funció del perfil i per motius professionals.

7. L'ús del telèfon mòbil personal durant la jornada laboral s'ha de limitar a aquelles circumstàncies en què sigui estrictament necessari i sempre que no afecti el desenvolupament normal de l'activitat professional exercida.

8. Queda garantit l'accés a l'espai reservat dins dels dominis de CCOO de Catalunya per a la informació sindical o laboral que es determini de comú acord amb l'RLPT.

11. ACCÉS I TRACTAMENT DE DADES DE CARÀCTER PERSONAL INFORMÀTICAMENT I EN PAPER

Les instruccions anteriors són aplicables a l'observança del compliment d'una normativa d'especial importància: la protecció de dades de caràcter personal. Atès que aquesta normativa tracta de salvaguardar un dret fonamental, mitjançant l'adopció de diferents mesures de seguretat, tècniques i organitzatives, les persones usuàries que accedeixen i tracten informació de caràcter personal en l'exercici de les seves funcions i tasques han d'atendre les obligacions següents.

Dades de caràcter personal: informació alfabètica, numèrica, gràfica, fotogràfica, acústica o de qualsevol altre tipus, relativa a un aspecte físic, psíquic, fisiològic, cultural, social o econòmic de la persona, susceptible de recollida, registre, tractament o transmissió i que concerneix una persona física identificada o identificable.

11.1. FITXERS INFORMÀTICS

En particular, respecte de la informació de caràcter personal continguda en fitxers informàtics, s'han de complir, d'acord amb allò que s'ha exposat en apartats anteriors, les diligències següents:

- Claus d'accés al sistema informàtic. Les contrasenyes d'accés al sistema informàtic són personals i intransferibles, i la persona usuària és l'única responsable de les conseqüències que es puguin derivar del mal ús, la divulgació o la pèrdua d'aquestes. Queda prohibit, així mateix, utilitzar identificadors i contrasenyes d'altres persones usuàries per accedir al sistema informàtic. En cas que calgués accedir al sistema en absència d'un company o companya, s'ha de sol·licitar al SISCOM l'habilitació de l'accés eventual. Un cop finalitzada la tasca que ha motivat l'accés, aquest fet ha de ser comunicat, de nou, al SISCOM.
- Bloqueig o apagament de l'equip informàtic. Cal bloquejar la sessió de la persona usuària en cas d'absentar-se temporalment del lloc de treball, a fi d'evitar accessos d'altres persones a l'equip informàtic. Això, sobretot, cal que sigui tingut en compte per part del personal que estigui fent atenció al públic.
- No emmagatzematge de fitxers no autoritzats a la xarxa informàtica.
- Manipulació dels arxius o dels fitxers informàtics. Únicament les persones autoritzades poden introduir, modificar o anul·lar les dades personals contingudes als fitxers. Els permisos d'accés de les persones usuàries als diferents fitxers són concedits per l'organització, en concret, pel SISCOM. En cas que qualsevol persona usuària requereixi, per al desenvolupament de la seva feina, accedir a fitxers l'accés dels quals no estigui autoritzat, ho ha de comunicar al departament esmentat.
- Generació de fitxers de caràcter temporal. Els fitxers de caràcter temporal són aquells en què s'emmagatzemen dades de caràcter personal, generades a partir d'un fitxer general per al

desenvolupament o el compliment d'una tasca determinada. Aquests fitxers han de ser esborrats una vegada hagin deixat de ser necessaris per als fins que van motivar-ne la creació i, mentre estiguin vigents, han de ser emmagatzemats a la carpeta habilitada a la xarxa informàtica. Si transcorregut un mes la persona usuària detecta la necessitat de continuar utilitzant la informació emmagatzemada al fitxer, ho ha de comunicar al SISCOM per adoptar les mesures oportunes sobre aquest.

- No es pot fer ús del correu electrònic per a enviaments d'informació de caràcter personal sensible.
- No s'ha d'utilitzar el correu electrònic (corporatiu o no) per a l'enviament d'informació de caràcter personal especialment sensible (és a dir, salut, ideologia, religió, creences, origen racial o ètnic). Aquest enviament només es pot fer si s'adopten els mecanismes necessaris per evitar que la informació sigui intel·ligible o manipulada per tercers. Per aquest motiu, s'ha d'informar el SISCOM perquè implementi el xifratge, l'encriptació o qualsevol mecanisme que salvaguardi la integritat i la privadesa de la informació.
- Comunicació d'incidències que afectin la seguretat de dades de caràcter personal. Cal comunicar al SISCOM, mitjançant el correu dpd@ccoo.cat, les incidències de seguretat de què es tingui coneixement.

Entre d'altres, tenen la consideració d'incidència de seguretat que afecta els fitxers informàtics els successos següents:

- Pèrdua de contrasenyes d'accés als sistemes d'informació.
- Ús indegut de contrasenyes.
- Accés no autoritzat a fitxers superant els perfils.
- Pèrdua de suports informàtics amb dades de caràcter personal.
- Pèrdua de dades per mal ús de les aplicacions.
- Atacs a la xarxa.
- Infecció dels sistemes d'informació per virus o altres elements nocius.
- Fallada o caiguda dels sistemes d'informació, etc.

11.2. FITXERS EN PAPER

En relació amb els fitxers en suport o document paper, la persona usuària ha de complir amb les diligències següents:

1. Custòdia de claus d'accés a arxivadors o dependències. Mantenir degudament custodiades les claus d'accés als locals, a les dependències o als despatxos, així com als armaris, als arxivadors o a altres elements que continguin suports o documents en paper amb dades de caràcter personal.
2. Tancament de despatxos o dependències. En cas de disposar d'un despatx, tanqueu amb clau la porta al final de la jornada laboral o quan us hàgiu d'absentar temporalment d'aquesta ubicació, a fi d'evitar accessos no autoritzats.
3. Emmagatzematge de suports o documents en paper. Cal guardar tots els suports o els documents que continguin informació de caràcter personal en un lloc segur, quan aquests no siguin usats, particularment, fora de la jornada laboral. Quan aquests suports o documents no

estiguin emmagatzemats, per ser revisats o tramitats, ha de ser la persona que estigui al seu càrrec qui custodiï i impedeixi, en tot moment, que una tercera persona no autoritzada hi pugui tenir accés.

4. No s'han de deixar a fotocopiadores, faxos o impressores papers amb dades de caràcter personal. Assegureu-vos que no queden documents impresos que continguin dades personals a la safata de sortida de la fotocopiadora, la impressora o el fax.
5. No s'han de deixar documents visibles als escriptoris, als taulells o en un altre mobiliari. S'ha de mantenir la confidencialitat de les dades personals que constin als documents dipositats o emmagatzemats als escriptoris, als taulells o en un altre mobiliari.
6. Rebuig i destrucció dels suports o els documents en paper amb dades personals. No s'han de llençar suports o documents en paper que continguin dades personals a papereres o contenidors, de manera que la informació pugui ser llegible o fàcilment recuperable. A aquests efectes, la documentació sempre ha de ser rebutjada o destruïda mitjançant una destructora de paper o un altre mitjà de què disposi l'organització. Es prohibeix terminantment rebutjar en papereres o en contenidors de cartró o paper suports o documents que continguin dades personals.
7. Arxiu de suports o documents. Els suports o els documents en paper s'han d'emmagatzemar seguint el criteri d'arxivament de l'organització. Aquests criteris han de garantir la correcta conservació dels documents, així com la localització i la consulta de la informació. Els suports o els documents s'han d'arxivar al lloc corresponent, de manera que se'n permeti una bona conservació, classificació, accés i ús. No podreu accedir o utilitzar els fitxers pertanyents a altres departaments que comparteixin la sala o la dependència habilitada per a fitxer.
8. Trasllat de suports o documents en paper amb dades de caràcter personal. En els processos de trasllat de suports o documents s'han d'adoptar mesures dirigides per impedir l'accés o la manipulació per tercers, de manera que no es pugui veure el contingut d'aquests, sobretot si hi ha dades de caràcter personal. S'ha d'evitar:
    a. Utilitzar carpetes transparents o especialment fràgils.
    b. Sostraure o posar a la vista de terceres persones el contingut dels documents durant el trajecte.
9. Trasllat de dependències. En cas de canviar de dependència, en el procés de trasllat dels suports o dels documents en paper, aquesta tasca s'ha de realitzar amb l'ordre degut. Així mateix, s'ha de procurar mantenir fora de l'abast de la vista de qualsevol persona de l'entitat aquells documents o suports en paper on constin dades de caràcter personal.
10. Enviament de dades personals sensibles en un sobre tancat. Si s'envien a terceres persones alienes a l'organització dades especialment sensibles (és a dir, salut, ideologia, afiliació sindical, religió, creences, origen racial o ètnic), contingudes en suport o en document paper, s'ha de realitzar en un sobre tancat i, en qualsevol cas, cal tenir present que s'ha d'efectuar per mitjà de correu certificat o a través d'una forma de correu ordinari que en permeti la confidencialitat completa.
11. Lliurament de documentació amb detalls d'ocupació a Recursos Humans. Quan les persones usuàries lliurin a les persones responsables de Recursos Humans una documentació determinada —nòmines signades, justificants d'alta o de baixa, o altra documentació que contingui informació relativa als detalls d'ocupació—, aquesta ha de ser lliurada en mà a la persona responsable o bé dins d'un sobre tancat en què s'indiqui a qui va dirigit.
12. Comunicació d'incidències que afectin la seguretat de dades de caràcter personal. Cal comunicar les incidències de què es tingui coneixement i que puguin afectar la seguretat de les dades personals.

Entre d'altres, tenen la consideració d'incidència de seguretat que afecta els fitxers en paper els successos següents:

- Pèrdua de les claus d'accés als fitxers, armaris i/o dependències on s'emmagatzema la informació de caràcter personal.
- Ús indegut de les claus d'accés.
- Accés no autoritzat als arxius, als armaris i/o a les dependències on es troben fitxers amb dades de caràcter personal.
- Pèrdua de suports o documents en paper, amb dades de caràcter personal.
- Deteriorament dels suports, dels documents, dels armaris o dels arxius on es troben dades de caràcter personal.

12. SEGUIMENT / CONTROL / MESURES DISCIPLINÀRIES

L'organització, a través del SISCOM, per motius de seguretat i amb l'objectiu de garantir la integritat de la informació, ha de vetllar per l'ús correcte i pel funcionament de l'accés a Internet i dels dispositius que conformen la xarxa confederal, i pot adoptar les mesures de verificació dels sistemes informàtics que cregui necessàries a fi de comprovar-ne l'aplicació correcta, poder certificar el rendiment òptim i de seguretat de la xarxa de l'organització i que la seva utilització per part de les persones treballadores usuàries no derivi en fins extraprofessionals.

Així mateix, en compliment de la legislació vigent, especialment de la Llei 9/2014, ha de retenir les dades de connexió i trànsit generades, amb el contingut i l'abast del que preceptua aquesta llei, garantint, en tot cas, el dret a la intimitat, l'honor i el secret de les comunicacions.

En l'adopció de les mesures de verificació dels sistemes telemàtics, cal tenir en compte el següent:

- L'accés ha de ser necessari per facilitar raonablement les operacions; si hi ha mitjans de menor impacte per a les persones, l'organització n'ha de fer ús.
- La privadesa i la dignitat de la persona usuària han d'estar sempre garantides.
- El correu electrònic i els arxius han de ser inspeccionats al lloc de treball, durant les hores de treball normals, amb l'assistència de l'RLPT o, si no, d'un altra persona de l'organització.
- La denegació d'accés per part de l'usuari o de la usuària, d'acord amb els termes establerts en aquest capítol, dona lloc a les mesures disciplinàries establertes.
- El respecte a la normativa legal establerta a aquest efecte, especialment la referida a la Llei orgànica de protecció de dades.

(Vegeu l'article 20.3 de l'Estatut dels treballadors i l'article 78 del Conveni col·lectiu d'oficines i despatxos de Catalunya.)

Es determina en una instrucció específica la participació de les funcions del gestor de dades i usuaris i usuàries en l'aplicació d'aquestes normes TIC.

Ateses les conseqüències negatives que pot representar per a l'organització la utilització inadequada dels sistemes d'informació, l'incompliment per part de les persones usuàries de qualsevol de les obligacions establertes en aquest document té la consideració de falta (lleu, greu o molt greu), cosa que pot donar lloc a l'obertura d'expedient disciplinari segons la normativa laboral, l'acord laboral o la normativa interna sindical vigent.

Aquest document pot ser actualitzat i completat amb instruccions específiques, i cal informar-ne les persones usuàries a través de les vies habituals de l'organització.

13. DIFUSIÓ

Aquestes normes han de ser comunicades, conegudes i acceptades per totes les persones usuàries mitjançant els sistemes informàtics implantats a l'organització.