REGLAMENT DE MITJANS TIC

DATA D'ELABORACIÓ DEL DOCUMENT	MARÇ 2018
NÚM. DE REVISIÓ	00

ÍNDEX DE CONTINGUTS

1. DISPOSICIONS GENERALS

1.1. Objecte

L'objectiu d'aquest Reglament és establir una regulació específica sobre les Tecnologies de la Informació i la Comunicació de les entitats de Fundalis, i del tractament no automatitzat de les dades personals. Es tracta d'un reglament d'usuari, per a que el personal compti amb la informació que permeti assegurar la confidencialitat, la integritat i la disponibilitat de la informació personal, interna i del client, així com l'ús adequat dels recursos.

1.2. Definició de Tecnologies de la Informació i la Comunicació (TIC)

Les Tecnologies de la Informació i la Comunicació (TIC) són aquelles eines informàtiques que permeten processar, emmagatzemar, sintetitzar, recuperar i presentar informació exposada de forma variada.

Són components d'aquestes tecnologies, entre d'altres, els ordinadors personals, els projectors multimèdia, els telèfons mòbils, internet, etc.

1.3. Principis de confidencialitat i protecció de dades

Els principis que regeixen a les entitats de Fundalis sobre la confidencialitat i protecció de dades com a reglament d'usos de recursos informàtics de les seves entitats són:

- El personal tindrà accés únicament a informació que precisi per al desenvolupament de les seves funcions i pel qual haurà estat autoritzat conseqüentment.
- Tota persona de les entitats de Fundalis haurà de guardar secret i mantenir la més estricta confidencialitat sobre tota la informació i dades de caràcter personal i de tercers als quals tingui accés en virtut del seu treball, obligació que subsistirà fins i tot després de finalitzar la seva relació amb l'empresa.
- Cada treballador/a és responsable dels mecanismes d'accés als locals i sistemes d'informació pels quals ha estat autoritzat en funció del seu càrrec o responsabilitats.
- Qualsevol incidència que afecti a la seguretat de la informació personal o de l'organització, haurà de ser comunicada al responsable de Seguretat de la Informació o a Direcció.
- Tots els/les treballadors/es que es donin de baixa, tindran la obligació de retornar, al seu responsable tota la informació i documentació, així com els suports informàtics, que tinguin a la seva disposició, indicant l'estat en el que es troben.

2. DEURE D'INFORMACIÓ PRÈVIA DEL REGLAMENT DE TIC AL PERSONAL DE L'ENTITAT

Les normes que integren el reglament de TIC s'hauran de comunicar a tot el personal de l'entitat, així com incloure's a la documentació a entregar al personal en el moment de la contractació. Així és deixa constància del coneixement de la mateixa i del compromís de confidencialitat i de secret professional que en cada cas apliqui, així com de les instruccions i responsabilitats contemplades en el cas d'ús d'eines tecnològiques, la propietat de les quals sigui de qualsevol de les entitats que pertanyin a Fundalis o en les quals participi.

3. DEURE DE FORMACIÓ EN EL REGLAMENT TIC

Les entitats de Fundalis volen assegurar que totes les persones treballadores són coneixedores d'aquest reglament i que entenen el seu contingut. En aquest sentit, es comprometen a formar a aquestes persones amb el que estableix el present Codi per a que puguin entendre el seu contingut i així puguin respectar les bones pràctiques de Fundalis.

4. CRITERIS RESPECTE A L'ÚS DE LES TIC

4.1. Classificació de la informació

Caldrà classificar la documentació com a restringida, confidencial, interna o pública. Conforme l'establert a continuació:

- **Restringida:** Aquesta és la informació de caràcter personal i estrictament circumscrita a nivell organitzatiu. La seva revelació a una persona o organització no autoritzada és una violació al dret d'intimitat o privadesa de les persones, per la qual cosa, la seva divulgació és il·legal i pot ser objecte de denúncia i penalització. L'accés a aquesta informació està estrictament limitat i controlat en tot moment. Ex.: Dades de propietats, patrimoni, renda o dades mèdiques.

- **Confidencial:** Aquesta és la informació de sensibilitat personal molt alta o pròpia de l'organització que pot implicar pèrdues econòmiques, danys a la privadesa personal o de l'organització. En cas que es produeixi la seva pèrdua, adulteració o eliminació pot ser objecte de sanció interna, independentment d'assumir les responsabilitats externes que poguessin derivar-se. Qualsevol persona que sol·liciti accedir a aquest tipus d'informació i que no sigui l'específicament designada per a això, haurà d'obtenir l'autorització prèvia del Responsable de seguretat de la Informació o de la Direcció. En qualsevol cas, les finalitats per les quals es sol·liciti accedir a la documentació confidencial hauran de ser estrictament necessàries. Ex.: Nòmines.

- **Interna:** És la informació que genera o utilitza l'organització contínuament. Les atribucions de generació, modificació o eliminació estan limitades d'acord a les funcions de cada treballador/a.

Cada treballador/a té la responsabilitat de vetllar per la seguretat de la informació cedida. Tot canvi en els privilegis haurà de ser sol·licitat al superior immediat i al responsable de Seguretat de la Informació. Ex.: Contractes amb proveïdors.

- **Pública:** És la documentació que l'empresa considera que sigui de coneixement públic. Ex.: Revistes o publicacions.

Si es comprova que el treballador ha modificat, eliminat, sostret o perdut informació (Restringida, Confidencial o Interna) podrà suposar causa suficient d'obertura d'expedient disciplinari, d'acord amb el que preveu el Conveni aplicable.

4.2. Contrasenyes

Segons les funcions de cada treballador/a, aquest tindrà accessos a les aplicacions de l'empresa mitjançant autenticació única.

El/la treballador/a haurà de canviar la contrasenya en els períodes que el sistema li comuniqui. Aquest sistema està planificat de manera que el propi sistema envia la proposta de canvi amb almenys deu dies d'antelació, termini en el que s'haurà de realitzar el canvi.

Respecte a la utilització de les contrasenyes, es recomana:

- No utilitzar les funcions de recordar les contrasenyes en cap de les aplicacions proporcionada o requerides per l'organització.
- És important no teclejar la contrasenya a la vista de terceres persones.
- En cas de no recordar la contrasenya, els usuaris hauran de posar-se en contacte amb el responsable de TIC.
- Els comptes administratius no poden ser compartits. En cas que diversos usuaris requereixin aquest tipus d'accés, només seran atorgats a través d'un grup d'usuaris administratius de sistemes.
- Les contrasenyes no hauran d'estar escrites en suports de fàcil pèrdua o divulgació. (Ex.: post-it, paper reciclat, etc.)
- Per cap motiu el personal informàtic podrà sol·licitar les contrasenyes dels comptes a la persona treballadora, tret que sigui urgent o necessàriament requerit per resoldre per exemple una incidència informàtica.

4.3. Seguretat de suports informàtics

En relació a la seguretat dels suports informàtics, en els que s'inclouen els suports portàtils o remots de cada entitat, de cara a evitar possibles danys, pèrdues o accessos no autoritzats, s'estableix:

- El/la treballador/a és responsable de mantenir operatius els equips disposats al seu càrrec.

- Les labors quotidianes de manteniment hauran de ser: Prendre totes les precaucions necessàries per evitar la pèrdua o dany de l'equip (trasllats, neteja, ubicació de l'equip, etc.), així com guardar el portàtil, si escau, en un armari sota clau, quan finalitzi la jornada laboral.
- S'ha de procurar connectar el portàtil a la xarxa interna de Fundalis o a Internet de forma segura perquè automàticament s'actualitzin les aplicacions de protecció de l'equip.
- El manteniment o manipulació dels equips informàtics haurà de ser realitzat pel personal tècnic especialitzat, i haurà de ser autoritzat pel Responsable de Seguretat o Direcció.
- L'assignació definitiva o puntual, així com la sortida de suports informàtics de les entitats, haurà de ser expressament autoritzada pel responsable de Seguretat, utilitzant per a això el document: Sortida de suports.

4.4. Eliminació de documents i unitats d'emmagatzematge d'informació

Tota documentació en paper que contingui informació classificada com a confidencial o restringida i es desitgi eliminar, haurà de ser destruïda en la destructora de paper que a aquest efecte haurà de disposar-se en cada organització de Fundalis.

Els dispositius d'emmagatzematge (*CDs i *DVDs) que es desitgin eliminar i que continguin informació classificada com a confidencial o restringida hauran de ser destruïts en la destructora de *CDs (si està disponible), o s'hauran de destruir manualment.

Els components d'emmagatzematge (Discos Durs, Cintes, memòries, etc.) que es desitgin eliminar i continguin informació classificada com a confidencial o restringida hauran de (segons sigui el dispositiu): eliminar les particions, formatar a baix nivell i/o sobreescriure amb informació (classificada com a pública) abans de la seva eliminació o reutilització.

4.5. Còpia de seguretat d'informació

Les còpies de seguretat dels servidors de Fundalis hauran de ser realitzades, registrades i controlades periòdicament, sota la responsabilitat del personal assignat en el seu cas i, en última instància, per la Direcció de Seguretat.

4.6. Política de protecció de la informació

Tota documentació classificada com a confidencial o restringida (impresa o escrita), així com la informació continguda en dispositius d'emmagatzematge (*CDs, *DVDs, Memòries, etc.) haura de ser guardada a l'armari personal o del departament, assegurat sota clau.

A més, s'ha de mantenir l'escriptori de treball ordenat i lliure de documentació obsoleta o inservible ja que podria confondre's amb documentació valuosa.

I en el mateix sentit, està prohibit escriure informació confidencial o restringida en suports fàcils de perdre o espatllar. (Ex.: post-it, paper reciclat, etc.).

4.7. Escriptoris nets

Es recomana no beure (en envasos sense tap) o consumir aliments en els escriptoris de treball ja que poden originar deterioració dels equips i de la documentació.

4.8. Bloqueig d'ordinadors

Totes les estacions de treball i portàtils estan configurats per bloquejar automàticament l'equip una vegada transcorregut com a màxim 10 minuts d'inactivitat. D'igual forma el/la treballador/a haurà de bloquejar l'equip cada vegada que es retiri del seu lloc de treball.

4.9. Protecció davant codi maliciós

Únicament es podran instal·lar, en les estacions de treball o portàtils, aplicacions permeses per l'empresa, prèvia sol·licitud del treballador/a i posterior autorització del responsable de Seguretat de la Informació.

El/la treballador/a que sospiti d'un determinat programa o arxiu haurà d'informar immediatament a la Direcció de Seguretat de Fundalis o al seu responsable de seguretat local.

El/la treballador/a que sospiti del contingut d'un dispositiu de emmagatzemant extern (*CD, *DVD, *PenDrive, etc.) haurà de consultar directament, al responsable de Seguretat de la Informació.

4.10. Ús de la xarxa interna, d'internet i serveis compartits

L'ús d'Internet i correu electrònic per part del personal queda restringit a finalitats estrictament laborals; excepcionalment els responsables de departament poden autoritzar als/les treballadors/es a utilitzar-lo amb fins personals. Els privilegis de connexions remotes hauran de ser sol·licitades al superior immediat i al responsable de Seguretat de la Informació.

En relació al correu electrònic, es fan les següents consideracions:

- Està prohibit enviar missatges de correu electrònic que continguin dades de caràcter personal o de tercers que puguin vulnerar la seguretat dels mateixos.
- No s'utilitzarà el correu electrònic per enviar o rebre missatges amb continguts inadequats, discriminatoris, difamatoris o nocius que puguin atemptar contra els drets i llibertats de les persones.
- En tots els correus electrònics que s'enviïn, s'ha d'incloure el peu de signatura automàtic, d'acord amb el model corporatiu establert, que inclou la clàusula de confidencialitat. Quan es

tracti de missatges amb finalitats personals, autoritzades pels responsables de departament, cal suprimir el peu de signatura.

- Es recomana no obrir documents adjunts de correus electrònics l'emissor dels quals sigui desconegut o l'assumpte dels quals pugui induir a sospitar de la presència d'un virus informàtic.
- Els correus electrònics que s'envien o reben des de les diferents entitats de Fundalis es gestionen des del Departament de TIC mitjançant sistemes segurs SSL (*Service *Socket *Layer) d'Internet, a través del Servei de correu de l'organització gestora interna. El sistema d'emmagatzematge disposa de certificació acreditada per part d'Entitat Certificadora (*FNMT o unes altres), que al seu torn garanteix la seguretat d'enviament/recepció des de/fins al correu emissor/receptor, igualment amb SSL.

4.11. Mobilitat

Els equips portàtils (smartphones, tauletes, portàtils) són lliurats al/la treballador/a en perfecte estat i funcionament. Si el/la treballador/a detectés algun desperfecte, mal funcionament o contingut inadequat en l'equip, aquest s'haurà de comunicar immediatament al responsable directe.

L'usuari haurà de vetllar per la seguretat i confidencialitat de la informació continguda en els seus equips, especialment quan es trobi fora de les dependències de l'empresa. Per a això:

- No és recomanable emmagatzemar en l'equip, informació confidencial o restringida. Si es dóna el cas, haurà d'assegurar-se que es realitzen còpies de seguretat de la mateixa.
- En cas d'haver de viatjar amb l'equip, mai es facturarà amb l'equipatge.
- Mai s'ha de deixar el portàtil desatès i a la vista del públic, especialment en situacions que puguin augmentar el risc de robatori. Als hotels, el portàtil haurà de guardar-se amb cadenat o en un espai tancat sota clau.

En cas de pèrdua de l'equip portàtil, l'incident haurà de ser comunicat immediatament a la Direcció de Seguretat i Sistemes (TIC).
Abans d'introduir/descarregar informació en els equips portàtils, des de qualsevol dispositiu d'emmagatzemament, aquest ha de ser examinat per l'aplicació d'antivirus.

Per verificar el correcte funcionament dels equips i el bon ús dels mateixos, el responsable de Sistemes realitzarà inspeccions periòdiques (de forma aleatòria entre tot el personal de l'empresa segons el criteri de la mateixa, tantes vegades com l'empresa estimi oportú) amb l'objecte d'examinar els següents aspectes:

- Aplicacions instal·lades.
- Estat de l'antivirus.
- Configuració estàndard del Sistema Operatiu.
- Actualitzacions del sistema
- Estat físic de l'equip.

Quan el/la treballador/a no hagi obrat amb la deguda diligència en la salvaguarda dels dispositius informàtics, o incompleixi els punts d'aquesta política aquí establerta, podrà estar subjecte a accions disciplinàries o compensatòries.

El/la treballador/a que posseeixi privilegis de connexió remota haurà de prendre les següents precaucions:

- No compartir les dades del certificat personal VPN.
- En tant que sigui possible, no connectar el portàtil en establiments amb *wi-fi lliures (no segurs).

Quan el/la treballador/a es doni de baixa tindrà l'obligació de retornar al responsable tots els equips i dispositius a la seva disposició.

El/la treballador/a queda informat amb aquest Reglament, que els recursos de *hard* i *soft* facilitats per part de qualsevol de les entitats de Fundalis són propietat de les mateixes i el seu accés i ús ho és com a eina exclusiva de treball, mentre el/la treballador/a sigui membre de les plantilles de Fundalis. La propietat dels continguts i del seu accés són i seguiran sent propietat de Fundalis, tot i la sortida de l'organització del treballador/a.

5. DIRECCIÓ I CONTROL DE L'ACTIVITAT LABORAL

5.1. Àmbit

Les entitats de Fundalis podran adoptar les mesures de vigilància i control que estimin més oportunes per a verificar el compliment per part del/la treballador/a de les seves obligacions i deures laborals.

5.2. Control de mitjans productius corporatius

Les entitats de Fundalis podran controlar els mitjans productius corporatius per verificar el compliment de les persones treballadores de les seves obligacions i deures laborals, entenent per mitjans productius corporatius aquells que la entitat posa a disposició del/la treballador/a pel desenvolupament de la seva activitat laboral.

L'entitat està legitimada per realitzar intervencions, com el control dels ordinadors i comptes de correu electrònic mitjançant programes informàtics d'intervenció, així com la intervenció de línies telefòniques titularitat de l'entitat.

5.3. Monitorització de les sessions d'accés a internet

Amb l'objectiu de preveure un ús fraudulent, il·legal, abusiu o no autoritzat, l'entitat podrà monitoritzar i comprovar de forma aleatòria, sempre amb previ avís, qualsevol sessió d'accés a Internet.

Així mateix, Fundalis ha instal·lat sistemes per impedir l'accés a alguns llocs o per detectar una possible utilització abusiva, i especificar, quan procedeixi, l'ús de dades recollides sobre les persones que visiten llocs específics.

És per això que, en cas de que algun/a treballador/a necessiti utilitzar internet amb fins privats, amb l'autorització del seu superior, haurà de comunicar-ho al responsable del TIC.

5.4. Revisió del correu electrònic

L'entitat podrà revisar, sempre amb previ avís, missatges de correu electrònic dels usuaris de la ret de l'entitat i els arxius del servidor, assegurant que el control realitzant serà proporcionat amb la seva finalitat.

5.5. Expectativa d'ús privatiu de mitjans productius corporatius

Les entitats de Fundalis reconeixen l'existència d'una certa expectativa d'ús privatiu dels mitjans per part de les persones treballadores. Alguns exemples són: recepció de missatges sindicals, telèfon de l'entitat per la comunicació fora del horari laboral, etc... Però en cap cas s'autoritza un ús habitual d'aquests mitjans per a fins exclusivament privats.

5.6. Instal·lacions de micròfons i càmeres

L'entitat fent ús de la seva facultat de control de l'activitat, estarà legitimada per realitzar la instal·lació de micròfons i càmeres per garantir la seguretat. Però en cap cas estarà autoritzada per instal·lar aquests dispositius en zones sensibles per a la intimitat personal.

5.7. Mesures contra el *hacking* o aplanament informàtic

L'entitat adoptarà mesures contra el *hacking* o aplanament informàtic a través de la identificació i autentificació d'usuaris i gestió de credencials.

5.8. Controls específics en matèria de propietat intel·lectual

Fundalis compleix amb la normativa sobre propietat intel·lectual i adoptarà controls específics, com per exemple: revisió de cada terminal mitjançant programes d'auditoria de la ret o del lloc de treball, llista de programes homologats, control de contingut i base de dades, inventari de llicències d'ús, correlació entre llicències existents i programes instal·lats.