Aquestes informacions hauran de realitzar-se de forma correcta i prèvia ja que en cas contrari no podran ser utilitzades les imatges captades com a mitjà de prova per qüestions laborals al no disposar de la legitimació necessària per falta d'informació.

Notificació usuaris – empleats de les funcions i obligacions respecte al tractament de dades

Per a finalitzar aquest punt, i tenint en compte el que hem comentat anteriorment, a cada usuari nou, se li haurien d'entregar unes normes i obligacions de preceptiu compliment. Aquest model, que es mostra a continuació- es troba en la plataforma i haurà de ser degudament notificat, disposant còpia de la correcta notificació a cada usuari.

FUNCIONS I OBLIGACIONS DEL PERSONAL

1 RESPONSABLE DE SEGURETAT I ADMINISTRADOR DEL SISTEMA

FUNCIONS DEL RESPONSABLE DEL FITXER

El responsable del fitxer és l'encarregat jurídicament de la seguretat del fitxer i de les mesures establertes en el present document, implantarà les mesures de seguretat establertes en ell i adoptarà les mesures necessàries perquè el personal afectat per aquest document sigui coneixedor de les normes que afecten al desenvolupament de les seves funcions.

FUNCIONS DEL RESPONSABLE DE SEGURETAT

És l'encarregat de coordinar i controlar les mesures definides en el present document.

CLASSIFICACIÓ DEL PERSONAL D'ADMINISTRACIÓ O PERSONAL INFORMÀTIC

Es distingeixen dues situacions diferents, que condicionen el tipus de personal que té accés als fitxers en cada cas:

- *Tractament habitual, sense incidències tècniques. Explotació diària.*
- *Errors, talls, incidències tècniques de qualsevol tipus que para la producció.*

PERSONAL AUTORITZAT EN PRODUCCIÓ HABITUAL

En el primer cas, l'accés es limita als següents perfils:

- *Usuari / Administrador del sistema.*
- *Operador.*

ADMINISTRADORS TÈCNICS I INFORMÀTICS GENERALS QUE INTERVENEN EN SITUACIONS NO HABITUALS

Quan no existeix personal tècnic determinat que es pugui relacionar de forma directa amb un Fitxer o sistema informàtic i que accedeixi habitualment a l'esmentat Fitxer o sistema.

Sempre serà possible conèixer el personal que intervingué amb posterioritat a la intervenció, deixant constància, identificant al personal tècnic, anotant-ho al Registre d'Incidències.

FUNCIONS DELS ADMINISTRADORS O PERSONAL INFORMÀTIC

El personal que administra el sistema d'accés als fitxers es pot classificar a la vegada en diverses categories, que no necessàriament hauran d'estar presents en tots els casos, essent alguns cops assumides per una mateixa persona o persones. Aquestes categories són:

- ***ADMINISTRADORS** (Xarxa, sistemes operatius i bases de dades). Són els responsables dels màxims privilegis i per tant de màxim risc que una actuació errònia pugui afectar al sistema. Tindran accés al software (aplicacions i dades) del sistema, a les eines necessàries pel desenvolupament de la seva tasca i als fitxers o base de dades necessaris per resoldre els problemes que sorgeixin.*

- ***OPERADORS** (Xarxa, sistemes operatius, bases de dades i aplicació). Les seves actuacions estan limitades a l'operació dels equips i xarxes utilitzant les eines de gestió a disposició. En principi no han de tenir accés directe a les dades dels fitxers perquè la seva actuació no precisa d'aquest accés.*

- ***MANTENIMENT DELS SISTEMES I APLICACIONS**. Personal responsable de la resolució d'incidències que puguin sorgir en l'entorn hardware / software dels sistemes informàtics o de la pròpia aplicació d'accés als fitxers.*

- ***QUALSEVOL ALTRE PERSONA QUE L'ORGANITZACIÓ ESTABLEIXI.***

OBLIGACIONS DEL RESPONSABLE DEL FITXER

Implantar les mesures de seguretat establertes en aquest document.

El responsable del fitxer haurà de garantir la difusió d'aquest Document entre tot el personal que l'hagi d'utilitzar.

Haurà de mantenir-lo actualitzat sempre que es produeixin canvis rellevats en el sistema d'informació o en l'organització del mateix.

Haurà d'adequar en tot moment el contingut del mateix a les disposicions vigents en matèria de seguretat de dades.

Haurà de designar un o diversos responsables de seguretat.

ENTORN DE SISTEMA OPERATIU I DE COMUNICACIONS

- *El responsable del fitxer aprovarà o designarà a l'administrador que es responsabilitzarà del sistema operatiu i de comunicacions.*
- *En el cas més simple, com és en què el fitxer es trobi ubicat en un ordinador personal i que s'hi accedeixi mitjançant una aplicació local monolloc, l'administrador del sistema operatiu podrà ser el mateix que accedeixi normalment als fitxers.*

SISTEMA INFORMÀTIC O APLICACIONS D'ACCÉS ALS FITXERS

- *El responsable del fitxer s'encarregarà de que els sistemes informàtics d'accés als fitxers tinguin el seu accés restringit mitjançant un codi d'usuari i contrasenya.*

- *Així mateix, tindrà cura que tots els usuaris autoritzats per accedir al/s fitxer/s, tinguin un codi d'usuari que serà únic, i que estarà associat a la contrasenya corresponent, que només serà coneguda pel propi usuari.*

SALVAGUARDA I PROTECCIÓ DE LES CONTRASENYES PERSONALS

- *Només les persones autoritzades podran tenir accés a les dades dels fitxers.*

GESTIÓ DE SUPORTS

- *La sortida de suports informàtics que continguin dades dels fitxers fora dels locals on està ubicat el fitxer haurà d'estar expressament autoritzada pel responsable del fitxer.*

ENTRADA I SORTIDA DE DADES PER XARXA

- *Totes les entrades i sortides de dades del Fitxer que s'efectuïn mitjançant correu electrònic es realitzaran des d'un únic compte o adreça de correu controlada per un usuari especialment autoritzat pel responsable del Fitxer. Igualment si es realitza l'entrada o sortida de dades mitjançant sistemes de transferència de fitxers per xarxa, únicament un usuari o administrador estarà autoritzat per a realitzar aquestes operacions.*

PROCEDIMENT DE CÒPIA DE SEGURETAT I RECUPERACIÓ

El responsable del fitxer s'encarregarà de verificar la definició i correcta aplicació de les còpies de seguretat i recuperació de les dades.

- *Serà necessària l'autorització per escrit del responsable del fitxer per a l'execució dels procediments de recuperació de les dades i haurà de deixar-ne constància al registre d'incidències de les manipulacions que s'hagin realitzat per aquestes recuperacions, incloent la persona que va realitzar el procés, les dades restaurades i les dades que hagin degut ser gravats manualment en el procés de recuperació.*

Controls periòdics de verificació del compliment

- *El responsable del fitxer juntament amb el responsable de seguretat analitzen amb periodicitat almenys trimestral les incidències enregistrades en el llibre corresponent, per a independentment de les mesures particulars que s'hagin adoptat en el moment que van produir-se, posar les mesures correctores que limitin aquestes incidències en el futur.*

- *Almenys cada any, es realitzarà una auditoria externa que dictamini el correcte compliment i l'adequació de les mesures del present document de seguretat o les exigències del Reglament de seguretat, identificant les deficiències i proposant les mitjana correctores necessàries. Els informes d'auditoria seran analitzats pel responsable de seguretat, qui proposarà al responsable del Fitxer les mesures correctores corresponents.*

- *Els resultats de tots aquests controls periòdics, així com de les auditories seran adjuntades a aquest document de seguretat en l' apartat corresponent.*

OBLIGACIONS DEL RESPONSABLE DE SEGURETAT

El responsable de seguretat coordinarà la posta en marxa de les mesures de seguretat, col·laborarà amb el responsable del fitxer en la difusió del Document de Seguretat i cooperarà amb el responsable del fitxer controlant el compliment de les mateixes.

GESTIÓ D'INCIDÈNCIES

- *El responsable de seguretat habilitarà un Llibre d'Incidències a disposició de tots els usuaris i administradors del fitxer amb la finalitat que s'hi registri qualsevol incidència que pugui suposar un perill per la seguretat del mateix.*

Analitzarà les incidències registrades, prenent les mesures oportunes en col·laboració amb el responsable dels fitxers.

CONTROLS PERIÒDICS DE VERIFICACIÓ DEL COMPLIMENT

- *El responsable de seguretat del Fitxer comprovarà, amb una periodicitat almenys trimestral, que la llista d'usuaris autoritzats es correspon amb la llista d'usuaris realment autoritzats en l'aplicació d'accés al Fitxer, per al que recollirà la llista d'usuaris i els seus codis d'accés a l'administrador o administradors del Fitxer. A més d'aquestes comprovacions periòdiques, l'administrador comunicarà al responsable de seguretat, quan es produeixi, qualsevol alta o baixa d'usuaris amb accés autoritzat al Fitxer. En el document de seguretat s' actualitzarà anualment el llistat d' usuaris.*

Es comprovarà també almenys amb periodicitat trimestral, l'existència de còpies de seguretat que permetin la recuperació de Fitxer.

- *Al seu torn, i també amb periodicitat almenys trimestral, els administradors del Fitxer comunicaran al responsable de seguretat qualsevol canvi que s'hagi realitzat en les dades tècniques dels annexos, com per exemple canvis en el software o hardware, base de dades o aplicació d'accés al Fitxer, procedint igualment a l'actualització d'aquests annexos.*

- *El responsable de seguretat, verificarà, amb periodicitat almenys trimestral, el compliment del previst en els apartats 7 i 8 d'aquest document en relació amb les entrades i sortides de dades, siguin per xarxa o en suport magnètic.*

- *El responsable del fitxer juntament amb el responsable de seguretat, analitzaran amb periodicitat almenys trimestral les incidències enregistrades en el llibre corresponent, per a independentment de les mesures particulars que s'hagin adoptat en el moment que es van produir, posar les mesures correctores que limitin aquestes incidències en el futur.*

- *Almenys cada any es realitzarà una auditoria, externa o interna que dictamini el correcte compliment i l'adequació de les mesures del present document de seguretat o les exigències del Reglament de seguretat, identificant les deficiències i proposant les mesures correctores necessàries. Els informes d'auditoria seran analitzats pel responsable de seguretat, qui proposarà al responsable del Fitxer les mesures correctores corresponents.*

- *Els mecanismes que permeten el registre d'accessos estaran sota el control directe del responsable de seguretat sense que s'hagi de permetre , en cap cas la desactivació dels mateixos.*

- *El responsable de seguretat s'encarregarà de revisar periòdicament la informació de control enregistrada.*

Els resultats de tots aquests controls periòdics, així com de les auditories seran adjuntades.

OBLIGACIONS DELS ADMINISTRADORS I PERSONAL INFORMÀTIC

ENTORN DE SISTEMA OPERATIU I DE COMUNICACIONS

Cap eina o aplicació d'utilitat que permeti l'accés als fitxers haurà de ser accessible a cap usuari o administrador no autoritzat .
A la norma anterior s'inclou qualsevol mitjà d'accés en brut, és a dir, no elaborat o editat, a les dades del fitxer, com els anomenats "querys", editors universals, analitzadors de fitxers, etc., que hauran d'estar sota el control dels administradors autoritzats relacionats.
L'administrador o persona designada com a Responsable de Còpies de Seguretat haurà de responsabilitzar-se de guardar en un lloc protegit les còpies de seguretat dels fitxers, de manera que cap persona no autoritzada hi tingui accés.

Si l'aplicació o sistema d'accés als fitxers utilitzés normalment fitxers temporals, fitxers d'històrics, o qualsevol altre mitjà que pogués tenir emmagatzemat còpies de les dades protegides, l'administrador haurà d'assegurar-se que aquestes dades no són accessibles posteriorment per personal no autoritzat.
Si l'ordinador en què es troba ubicat el fitxer està integrat en una xarxa de comunicacions de manera que des d'altres ordinadors connectats a la mateixa sigui possible l'accés als fitxers, l'administrador responsable del sistema haurà d'assegurar-se que aquest accés no es permet a persones no autoritzades.

SISTEMA INFORMÀTIC O APLICACIONS D'ACCÉS AL FITXER

Si l'aplicació informàtica que permet l'accés als fitxers no compta amb un control d'accés haurà de ser el sistema operatiu, on s'executi aquesta aplicació, la que bloquegi l'accés no autoritzat, mitjançant el control dels esmentats codi d'usuari i contrasenya.

En qualsevol cas es controlaran els intents d'accés fraudulent al Fitxer, limitant el nombre màxim d'intents fallits, i, quan sigui tècnicament possible, guardant en un fitxer auxiliar la data, hora, codi i clau erronis que s'han introduït, així com altres dades rellevants que ajudin a descobrir l'auditoria d'aquests intents d'accés fraudulents.

Si durant les proves anteriors a la implantació o modificació de l'aplicació d'accés al Fitxer s'utilitzessin dades reals, s'haurà d'aplicar a aquests fitxers de prova el mateix tractament de seguretat que s'aplica al mateix Fitxer.

SALVAGUARDA I PROTECCIÓ DE LES CONTRASENYES PERSONALS

Les contrasenyes s'assignaran i es canviaran mitjançant el mecanisme i periodicitat que es determina pel responsable. Aquest mecanisme d'assignació i distribució de les contrasenyes haurà de garantir la confidencialitat de les mateixes, i serà responsabilitat de l'administrador del sistema.
El fitxer on s'emmagatzemen les contrasenyes haurà d'estar protegit i sota la responsabilitat de l'administrador del sistema.

PROCEDIMENT DE CÒPIA DE SEGURETAT I RECUPERACIÓ

Existirà una persona, bé sigui l'administrador, o bé, un altre usuari expressament designat, que serà el responsable d'obtenir periòdicament una còpia de seguretat dels fitxers, a efectes de còpia de seguretat i possible recuperació en cas de fallida.
Aquestes còpies hauran de realitzar-se amb una periodicitat, com a mínim, setmanalment, excepte en el cas que no s'hagi produït cap actualització de les dades.

En cas de fallida del sistema amb pèrdua total o parcial de les dades del fitxer/s hi haurà un procediment, informàtic o manual, que partint de la última còpia de seguretat i del registre d'operacions realitzades des del moment de la còpia, es puguin reconstruir les dades dels fitxers a l'estat en que es trobava en el moment de fallida.
Serà necessària l'autorització per escrit del responsable del fitxer per a l'execució dels procediments de recuperació de les dades, i haurà de deixar-se constància al registre d'incidències de les manipulacions que s'hagin realitzat per a aquestes recuperacions, incloent la persona que va realitzar el procés, les dades restaurades i les dades que hagin hagut de ser gravats manualment en el procés de recuperació.

2. OBLIGACIONS QUE AFECTEN A TOT EL PERSONAL

LLOCS DE TREBALL

- *Els llocs de treball estaran sota la responsabilitat d'algun usuari autoritzat que garantirà que la informació que ensenyin no pugui ser visible per persones no autoritzades.*

- *Això implica que tan les pantalles com les impressores o un altre tipus de dispositiu connectats al lloc de treball hauran d'estar físicament ubicats en llocs que garanteixin aquesta confidencialitat.*

- *Quan el responsable d'un lloc de treball l'abandoni, bé temporalment o bé per finalitzar el seu torn de treball, haurà de deixar-lo en un estat que no permeti la visualització de les dades protegides. Això es portarà a terme mitjançant el bloqueig de l'estació de treball per part de l'usuari. El restabliment del treball, per tant, implica que es desbloquegi l'estació mitjançant la introducció de l'identificador d'usuari i contrasenya corresponents.*

- *En el cas de les impressores s'assegurarà que no quedin documents impresos en les safates de sortida que continguin dades protegides. Si les impressores són compartides amb altres usuaris no autoritzats per accedir a les dades del fitxer/s, els responsables de cada lloc de treball hauran de retirar els documents a mesura que vagin essent impresos.*

- *Queda expressament prohibida la connexió a xarxes o sistemes exteriors dels llocs de treball des dels que es realitza l'accés al fitxer. La revocació d'aquesta prohibició serà autoritzada pel Responsable dels fitxers, quedant constància d'aquesta modificació en el Llibre d'Incidències.*

- *Els llocs de treball des dels que es té accés al fitxer tindran una configuració fixa d'aplicacions i sistemes operatius que només podrà ser canviada sota l'autorització del Responsable de Seguretat o pels Administradors autoritzats expressament.*

SALVAGUARDA I PROTECCIÓ DE LES CONTRASENYES PERSONALS

- *Cada usuari serà responsable de la confidencialitat de la seva contrasenya i, en cas que la mateixa sigui coneguda fortuïta o fraudulentament per persones no autoritzades, s'haurà de registrar com incidència i procedir immediatament al seu canvi.*

GESTIÓ D'INCIDÈNCIES

- *Qualsevol usuari que tingui coneixement d'una incidència és responsable del registre de la mateixa en el Llibre d'Incidències dels fitxers o en el seu cas de la comunicació per escrit al responsable de seguretat o al responsable del fitxer.*

- *El coneixement i la no notificació o registre d'una incidència per part d'un usuari serà considerat com una falta contra la seguretat del fitxer per part d'aquest usuari.*

GESTIÓ DE SUPORTS

- *Els suports que continguin dades del fitxers, bé com conseqüència d'operacions intermitges pròpies de l'aplicació que els tracta, o bé com a conseqüència de processos periòdics de suport o qualsevol altra operació esporàdica, hauran d'estar clarament identificats amb una etiqueta externa que indiqui de quin fitxer es tracta, quin tipus de dades conté, procés que els ha originat i data de creació.*

- *Aquells mitjans que siguin reutilitzables, i que hagin contingut còpies de dades dels fitxers, hauran de ser esborrats físicament abans de la seva reutilització, de forma que les dades que contenien siguin irrecuperables.*

- *Els suports que continguin dades dels fitxers hauran de ser emmagatzemats en un lloc que no hi tingui accés persones no autoritzades per a l'ús dels fitxers que no estiguin expressament autoritzades.*

- *Quan la sortida de dades del Fitxer es realitza per mitjà de correu electrònic els enviaments es realitzaran, sempre i únicament, des d'una adreça de correu controlada per l'administrador de seguretat, deixant constància d'aquests enviaments en el directori històric d'aquesta adreça de correu o en algun altre sistema de registre de sortides que permeti conèixer en qualsevol moment els enviaments realitzats, a qui anaven dirigits i la informació enviada.*

- *Quan les dades dels Fitxers hagin de ser enviades fora del recinte físicament protegit on es troba situat el Fitxer, bé sigui mitjançant un suport físic d'enregistrament de dades o bé sigui mitjançant correu electrònic, hauran de ser encriptats de forma que només puguin ser llegides i interpretades pel destinatari.*

- *S'hauran d'enregistrar mitjançant correu electrònic o transferència de dades per xarxa, de forma que es pugui sempre identificar el seu origen, tipus de dades, format, data i hora de l'enviament i destinatari dels mateixos.*

2.1 NORMES DE BON ÚS DELS SISTEMES D'INFORMACIÓ

1.- Els Sistemes d'Informació i els equips informàtics i de telecomunicacions pertanyen a la societat i estan al seu servei. En tenim cura i ens assegurem que donen sempre el màxim i millor servei possible.

1.1 No manipuleu els equips ni els programes. La instal·lació i la configuració física (les màquines i els aparells) i lògica (els programes) dels equips informàtics i de telecomunicacions la fan només els especialistes informàtics del Servei d'Informàtica.

1.2 Els canvis en la ubicació física d'equips els han de fer els tècnics del Servei d'Informàtica. Cal preveure'ls i demanar-los amb temps suficient. Podeu fer-ho utilitzant el formulari sol·licitud adequat a la Intranet.

1.3 Deixeu cada dia els equips informàtics en el millor estat de disponibilitat, ordre i neteja per tal que les persones que puguin venir després els trobin tal com a vosaltres us agradaria trobar-los.

1.4 Informeu al Servei d'Informàtica de qualsevol avaria o mal funcionament dels sistemes encara que no us afectin en aquell moment. Podeu fer-ho mitjançant el tècnic d'informàtica assignat al vostre servei, a través de l'adreça de correu corresponent o trucant a la Unitat de Suport Informàtic.

2.- L'empresa entitat només utilitza un programari en adequades condicions de legalitat, actualització i compatibilitat.

2.1 Els equips ja vénen amb tot el programari necessari preinstal·lat. Si malgrat això, us calen d'altres productes homologats que no vinguin amb l'ordinador, els podeu demanar utilitzant el formulari de sol·licitud adequat.

2.2 Feu servir exclusivament el programari homologat, és a dir, el programari oficial que l'empresa posa a disposició del personal en les versions que garanteixen la compatibilitat de tots els equips connectats en xarxa.

2.3 No instal·leu ni utilitzeu programari que no estigui homologat. Qualsevol programari no homologat que s'instal·li en un equip de la societat pot ser esborrat des del Servei d'Informàtica de forma automàtica en qualsevol moment i sense cap advertència o comunicació prèvia.

2.4 En cap moment heu de "baixar" programes d'Internet, ni tampoc instal·lar-ne. A més de la falta d'homologació, són una font molt perillosa de virus.

2.5 No manipuleu la configuració del programari instal·lat als PC. La configuració dels programes, que es guarda a cada PC, es pot actualitzar de forma massiva i automàtica des del Servei d'Informàtica, per la qual cosa convé no modificar-la.

2.6 No heu de canviar el fons de l'escriptori ni el protector de pantalla. Cal que tingueu sempre instal·lats els corporatius, ja que així es manté el rendiment de l'equip i es preserva la imatge corporativa.

2.7 No utilitzeu cap programa que permeti l' intercanvi de dades o l' emmagatzemament d' aquestes que no estigui configurat pel departament informàtic, atenent que aquests poden provocar accessos de tercers no autoritzats, així com transferències internacionals no autoritzades. Recordeu que no es permet l' utilització de cap programa dels denominats P2P, "Cloud computing" o similars

3.- Estalviem en el consum dels recursos informàtics per tal de millorar l'eficiència de l'empresa i en benefici del medi ambient.

3.1 Apagueu completament el vostre equip (PC, pantalla, etc) cada dia en sortir de la feina per tal d'estalviar energia i permetre les tasques de manteniment dels equips i les aplicacions. Des del Servei d'Informàtica se us podran donar instruccions que modifiquin o anul·lin aquest apartat quan l'evolució tecnològica o les necessitats de manteniment ho facin recomanable.

3.2 Feu impressions només si és imprescindible, les fotocòpies són més econòmiques. Abans de fer qualsevol impressió examineu acuradament el resultat amb l'opció de vista prèvia disponible en la majoria dels programes. Si teniu l'opció d'imprimir a doble cara, feu-ho tant com us sigui possible. La tecnologia Làser també és més econòmica que la d'injecció de tinta.

3.3 Utilitzeu, sempre que sigui possible, el correu electrònic per enviar documents a d'altres usuaris. És molt més ràpid i econòmic.

3.4 Es recomana compartir els dispositius informàtics, sempre que això sigui possible i d'acord amb els responsables del servei al qual pertanyeu, estalviareu consumibles, espai en disc, trànsit d'informació a la xarxa, costos de manteniment, entre d'altres.

3.5 Treballeu en discos de xarxa i amb bústies departamentals sempre que els mètodes de treball i procediments del vostre servei ho permetin. La utilització d'espais comuns d'emmagatzemament evita la duplicitat d'informació.

3.6 Manteniu ocupat el mínim espai en disc necessari, reviseu periòdicament l'organització de les carpetes i els documents. No guardeu documents sense una causa justificada.

3.7 Esborreu periòdicament la informació digital (documents de text o fulls de càlcul, missatges de correu, etc.) que ja no fareu servir. Utilitzeu sistemes externs per guardar informació històrica (per exemple disc dur externs o CD's).

4.- Protegim les xarxes informàtiques i de telecomunicacions de l'empresa de danys que en perjudiquin el funcionament diari en benefici propi, de tots els companys.

4.1 Un virus informàtic no és més que un programa malintencionat desenvolupat per perjudicar a qui l'executa. No tots són igualment perjudicials però els més malignes poden saturar les xarxes, destruir la informació emmagatzemada, inutilitzar els sistemes o produir avaries.

4.2 Les xarxes telemàtiques corporatives estan protegides a diferents nivells contra els atacs dels virus que puguin provenir de l'exterior (per correu electrònic, Internet) i contra la infecció i propagació interna (a través dels servidors de fitxers). Ateneu acuradament els missatges que us puguin enviar les eines antivíriques i actueu segons les recomanacions i els procediments establerts per a aquests casos.

4.3 A més dels recursos compartits en xarxa, també es poden protegir els PC's de possibles infeccions (produïdes generalment a través dels servidors de les disqueteres). Si teniu un antivirus instal·lat, manteniu-lo en activitat permanent i no modifiqueu la seva configuració ja que està pensada de forma coherent i consistent amb la xarxa.

4.4 Tingueu cura dels missatges i/o avisos que envien els ordinadors i procediu en conseqüència. Poden venir de l'aplicació que esteu fent servir, del sistema operatiu o de la xarxa de comunicacions, com també de l'administració del sistema corporatiu. Normalment requereixen alguna acció de l'usuari, que s'ha d'atendre per a un adequat funcionament de les xarxes corporatives, per tal de trobar-hi solucions.

4.5 Informeu al Servei d'Informàtica de qualsevol situació de risc que pugui afectar al correcte funcionament de les xarxes corporatives, per tal de trobar-hi solucions.

5.- L'empresa posa les eines informàtiques i de telecomunicacions a disposició dels seus treballadors perquè les utilitzin en l'àmbit exclusiu del seu entorn en treball.

5.1 Utilitzeu els recursos informàtics i de telecomunicacions únicament pel desenvolupament de les tasques que teniu encomanades en els vostres llocs de treball i d'acord amb els responsables del vostre servei.

5.2 No és permès l'ús personal o privat de les eines informàtiques i de telecomunicacions que l'empresa us ofereix: documentació particular, correu intern, accés a Internet, ús del programari, maquinari, etc.

5.3 L'accés a Internet és restringit. S'ha de sol·licitar al Servei d'Informàtica amb autorització expressa dels responsables del servei o oficina on esteu adscrits.

5.4 Cada lloc de treball únicament ha de tenir accés als recursos als quals hi està autoritzat (aplicacions, espais compartits de disc, bústies de correu, impressores i altres dispositius o llocs). Qualsevol altra circumstància s'ha de notificar immediatament al Servei d'Informàtica.

5.5 Tota la informació que feu servir en el vostre àmbit de treball, inclosa la que té format digital, és responsabilitat exclusiva de la societat i, per tant, no se'n pot fer un ús privat. L' utilització d' aquesta informació i dades – tinguin o no la consideració de caràcter personal- al marge de les tasques professionals encomanades significarà el trencament de la confiança empresarial amb l' usuari; i fins i tot la comissió d' un delicte penal de revelació de secrets; podent l'entitat exercitar quantes accions judicials consideri oportunes per protegir la seva informació i la que tracta en el seu marc professional.

5.6 S'està obligat a guardar el secret professional del coneixement que se'n tingui, fins i tot després del canvi del lloc de treball o de l'extinció de la relació laboral.

6.- Els treballadors i col·laboradors de l'empresa entitat som responsables dels recursos informàtics i de telecomunicacions que ens han encomanat com a ajut per facilitar la nostra tasca professional a la societat.

6.1 Tota persona al servei de la societat que té autorització d'accés als recursos telemàtics té assignat un nom d'usuari (Username) i una bústia de correu personal que l'identifica individualment. No utilitzeu les identificacions d'altres persones per accedir a les xarxes i no deixeu que els altres ho facin. Tramitar una alta o una baixa d'usuari és tan senzill com omplir i enviar els formularis adequats.

6.2 Us heu de responsabilitzar de la contrasenya (Password) que teniu assignada personalment per accedir als Sistemes d'Informació de l'empresa entitat . No s'ha de donar difusió de la contrasenya associada al vostre codi d'usuari i és responsabilitat de cadascú de mantenir-ne el secret, ja que aquesta és l'única manera de garantir la seguretat i confidencialitat del sistema i protegir d'actuació informàtica i/o telemàtica del personal usuari.

6.3 Assegureu-vos que ningú pugui suplantar la vostra personalitat a l'entorn dels mitjans informàtics o de telecomunicacions. No deixeu l'ordinador sense vigilància abans de sortir

de la sessió en la qual us heu identificat mitjançant la contrasenya. Una bona opció és l'ús del protector de pantalla amb una contrasenya.

6.4 Utilitzeu únicament els recursos informàtics i de telecomunicacions als quals esteu autoritzats pels vostres responsables. Assegureu-vos de fer servir les unitats d'emmagatzematge adequades a cada necessitat.

6.5 Responsabilitzeu-vos dels documents digitals que elaboreu. Els documents que resideixen en mitjans informàtics o de telecomunicacions són responsabilitat dels seus autors, els quals han de tenir cura de fer-los servir de forma ètica, d'acord amb el seu responsable i en l'àmbit estricte del seu lloc de treball.

6.6 Procureu emmagatzemar tota la informació en els espais destinats a l'efecte a les xarxes informàtiques i de telecomunicacions de la societat on s'hi garanteix l'adequada confidencialitat i integritat. Malgrat tot, si per alguna raó heu de guardar informació en unitats locals, és a dir, en el disc del PC (C:\), assegureu-vos de disposar de còpies de seguretat de la vostra informació.

6.7 No és recomanable protegir els documents amb contrasenya. Només pot ser-ho quan ho aconsellin necessitats molt específiques d'una alta confidencialitat que no pugui estar garantida per un altre mitjà (com xifrar-lo amb les claus de la signatura electrònica). En tal cas i sempre que sigui possible, es recomana compartir la contrasenya del document amb alguna altra persona ja que l'oblit d'aquesta contrasenya representa la pèrdua del document.

6.8 Si actualment a l'empresa entitat es pot treballar amb correu segur i fer connexions Internet a pàgines segures amb un certificat digital. Convé tenir instal·lat aquest certificat amb un nivell de seguretat alt amb contrasenya. És responsabilitat de l'usuari tenir cura d'aquesta contrasenya i no oblidar-la així com de fer una còpia de seguretat del seu certificat.

7.- Utilitzeu el correu electrònic de forma digna i responsable. L'ús del correu electrònic d'Internet ens representa personalment però també com a membres de l'empresa entitat i per allà on passem estem deixant una targeta de visita.

El sistema informàtic, la xarxa interna, el software i els terminals utilitzats pels treballadors són propietat de la Societat. És per això que cap correu electrònic enviat o rebut des dels sistemes informàtics de l'empresa entitat pot tenir la consideració de personal.

7.1 El correu electrònic no podrà ser utilitzat per a propòsits personals; i per tant en cap cas es podrà considerar que tenen la condició de privat; atès que el principi d' eficàcia de les tasques a desenvolupar, en cas d' absència d' un treballador per qualsevol motiu, la seva adreça de correu electrònic serà redirigida a un altre usuari; per tal de poder realitzar les tasques professional. Per tant, s' informa que totes les adreces de correu electrònic de la entidad son de la seva exclusiva propietat, sense que en cap cas, incloses les adreces nominatives, es pugui considerar que pertany a l' usuari en concret que l'utilitza.

7.2 No es podrà fer ús de l'e-mail per transmetre continguts:

a) Que infringeixin les normes de Copyright o de la propietat intel·lectual.
b) Que atemptin contra els drets a terceres persones, o de la mateixa organització.
c) Difamats, obscens, fraudulents, amenaçadors o de qualsevol altra natura que incorri en conductes il·legals o il·lícites.

7.3 En tot cas, tots els correus que hagin de ser enviats a diversos destinataris sempre s' hauran d' enviar amb còpia oculta (CCO.), atès que l' adreça de correu electrònic és una dada de caràcter personal i per tant subjecte a aquesta normativa. L' enviament d' un correu a diversos destinataris amb les adreces a la vista (CC) es considerada una cessió de dades, i per tant pot ser objecte d' una sanció per l' autoritat de protecció de dades competent.

7.4 L'empresa podrà controlar els missatges de correu electrònic quan hi hagi indicis que s'ha vulnerat la present política d'utilització del correu electrònic o per causa d'alguna obligació legal.

8. Els treballadors i col·laboradors de l'empresa entitat han de tenir una especial cura quan hagin de tractar dades de caràcter personal.

8.1 La normativa de Protecció de Dades de Caràcter Personal, té com objecte principal garantir i protegir els drets fonamentals de les persones físiques, i especialment, el seu honor i intimitat personal i familiar.

8.2 En el seu compliment, l'empresa entitat aprova i declara tots els fitxers informàtics que contenen dades personals tractades per les aplicacions o programes gestionats pel Servei d'Informàtica.

8.3 Aquesta entitat estableix les mesures de seguretat tècniques i organitzatives que s'han d'aplicar per garantir la confidencialitat i integritat de les dades de caràcter personal.

8.4 Per aquest fet, l'emmagatzematge i tractament de dades de caràcter personal en els PC's dels usuaris fa impossible l'aplicació d'aquestes mesures, per la qual cosa serà responsabilitat del propi usuari l'aplicació de les mesures de seguretat i protecció exigides per la normativa.

8.5 Pel mateix motiu, qui creï bases de dades que continguin dades de caràcter personal o desenvolupi aplicacions o programes que les tractin al marge del Servei d'Informàtica, serà el responsable del Fitxer o Tractament amb les conseqüències legals que se'n derivin.

8.6 Les dades de caràcter personal només han de ser objecte dels tractaments pels quals varen ser recollides. Heu de tenir en compte que les dades han de ser exactes, mantenir-se actualitzades i ser cancel·lades (no necessàriament eliminades) quan hagin deixat de ser necessàries. Malgrat tot, es considera admissible el tractament posterior amb finalitats històriques, estadístiques o científiques.

8.7 En recollir dades de caràcter personal heu de tenir present que ningú podrà ser obligat a declarar sobre la seva ideologia, religió o creences. En el cas que la persona afectada decideixi lliurement facilitar la informació que se li sol·licita en relació amb les dades indicades o la relativa a la seva afiliació sindical, caldrà disposar de manera indispensable de la seva autorització PER ESCRIT per l'emmagatzematge i tractament de qualsevol d'aquestes dades.

8.8 Les dades de caràcter personal objecte de tractament, únicament podran ser comunicades a un tercer, amb el previ consentiment de l'interessat i sempre que la finalitat de la comunicació respongui al compliment de les funcions legítimes del receptor de les dades. En cas que sigui necessària una cessió/comunicació de dades a un tercer, consulteu amb els vostres responsables. Si la comunicació s'efectua previ procediment de dissociació (l'interessat deixa de ser identificat o identificable) no serà necessari el seu consentiment.

8.9 Si en un fitxer hi ha un camp d'observacions no es permet d'incloure-hi qüestions relatives a la vida privada i/o l'honorabilitat de les persones, especialment si fa referència a dades considerades sensibles (raça, religió, creences, vida sexual, salut, afiliació sindical) o que puguin resultar despectives per a la persona).

8.10 S'han de respectar totes aquelles mesures de seguretat, que adopti l'empresa entitat per tal de garantir la confidencialitat i integritat de la informació.

8.11 En el supòsit de que tenir assignat un dispositiu mòbil amb accés al correu professional, l' usuari haurà de protegir el dispositiu amb una contrasenya o codi d' accés que limiti que un tercer pugui visionar dades en cas de pèrdua o robatori del aparell. Així mateix, el propi usuari

reconeix que és l' única persona a utilitzar el dispositiu mòbil entregat, fent-se responsable de qualsevol ús que es pugui realitzar del dispositiu.

8.12 En tots aquells documents (llistats, documents impresos, cd, zips i altres suports magnètics o de qualsevol altre tipus) que continguin dades de caràcter personal s'hauran d'observar una sèrie de mesures addicional, com:

a) Han de ser tractades i conservades amb la màxima confidencialitat i, per tant, s'han de guardar en llocs on només hi tingui accés el personal autoritzat. Els suports (cds, zip, dat…) han de tenir una identificació amb el detall de la informació que conté i la data en què es van fer.
b) Els documents han de ser destruïts quan deixin de ser necessaris, no s'han d'utilitzar com a paper reciclat.
c) Els suports magnètics s'han de fomatejar abans de reutilitzar-los i destruir-los físicament abans de llançar-los.

8.13 Si un usuari ha de realitzar proves amb dades de caràcter personal, haurà de demanar autorització al departament informàtic per tal de poder assegurar-se que aquestes es realitzin d' acord amb les mesures de seguretat establertes pel fitxer del qual es tracta.

9. Queda totalment prohibit l' ús de qualsevol xarxa social per tots els treballadors de l'entitat ; a excepció dels usuaris que es trobin per escrit i expressament autoritzats al tractar-se del Comunity Manager de l' entitat.

2.2 NORMES DE BON ÚS DELS SUPORTS MANUALS

a. La normativa de protecció de dades de caràcter personal també es aplicable a tots els fitxers manuals, és a dir, a tots aquells tractament que es realitza en paper; havent de tenir molta cura d' aquests al ser molt més senzill, si no s' apliquen de forma correcta les mesures de seguretat, que un tercer no autoritzat pugui tenir accés.

a.1 Per aquest motiu, l' usuari serà sempre el responsable de que un tercer no pugui tenir accés al fitxer manual que estigui tractant. Serà l' encarregat d' emmagatzemar la informació de tal manera que no pugui ser visionat per tercers que es trobin en les instal·lacions de l'entitat.

a.2 Els expedients que es trobin en les seves taules es guardaran en carpetes, sense que en la portada s'identifiqui clarament l' assumpte i la persona de qui es tracta nominativament, utilitzant números de referència o codis anonimitzats i només identificables pel personal de l' entitat. La persona que té l' expedient al seu càrrec, ha de tenir la diligència suficient per la seva custòdia, evitant accessos no autoritzats.

a.3 En el trasllat d' aquest expedients s' utilitzaran sistemes que garanteixi la integritat de les dades que es tracten, evitant la pèrdua d' aquests per accidents. Es recomana la utilització de carteres amb cremalleres; i en cap cas carpetes obertes i sense cap sistema de tancament.

b. Qualsevol document on poden constar dades de caràcter personal i que hagi deixat de ser necessari, i no hagi de ser conservat legalment, haurà de ser destruït de forma confidencial i de tal manera que no es pugui visionar cap tipus de dada. Per això es recomana la utilització de destructora de paper que es disposen per aquesta finalitat o el sistema de destrucció confidencial per tal de que un tercer mai pugui tenir accés.

c. Els suports utilitzats per arxivar la documentació en paper hauran de trobar-se en espais només accessible pel personal expressament autoritzat per l'entitat i amb dispositius que garanteixin que un tercer no pugui tenir accés. Serà obligació de l' usuari mantenir l' ordre i les pautes marcades per l' arxiu.

d. Tota la informació que consta a la documentació és responsabilitat de l'empresa, que ha implementat las mesures de seguretat legal determinades, entre altres, en aquest document; per la qual cosa, l' usuari es compromet a guardar el més alt secret professional sobre totes les dades i informació que pot tenir accés, fins i tot una vegada finalitzada la prestació de serveis que el vincula amb l'entitat.

e. L' usuari té l' obligació de posar en coneixement del responsable qualsevol petició dels exercicis dels drets previstos a la normativa, de forma immediata, per tal de poder donar contestació en el plaç legal establert.

I essent coneixedor que en moltes ocasions, la lectura de les funcions i obligacions de forma completa pot significar la seva no comprensió de forma correcta atesa la seva extensió, a continuació s'inclou un model de notificació on es detallen els punts més importants a tenir en compte per un usuari:

FUNCIONS I OBLIGACIONS DE L'EMPLEAT

PROTECCIÓ DE DADES

-10 punts bàsics-

1. *S'ha d'accedir amb el nom d'usuari i contrasenya facilitat i que l' identifica de forma personal, sense que es permeti la seva compartició o anotació que permeti l'accés d'una altra persona.*

2. *Qualsevol sistema o suport de telecomunicacions, informàtic o sistema posat a la seva disposició per l'empresa és per a la realització de les tasques professionals encarregades sense que pugui ser utilitzat amb cap altra finalitat personal o particular.*

3. *No es permet la descàrrega, instal·lació o incorporació de cap programa o servei informàtic per part de l'usuari, per a evitar vulnerar la normativa de protecció de dades així com els drets de propietat intel·lectual inherents a ells.*

4. *S'ha de garantir que només les persones expressament autoritzades puguin accedir a la informació. Cada empleat és responsable de no deixar documents en taules, prestatgeries o espais que puguin ser visionats per tercers. Les taules han de romandre sempre netes de papers visibles.*

5. *Qualsevol document que sigui rebutjat ha de ser prèviament destruït de forma confidencial amb una destructora de paper o amb el servei de destrucció confidencial que es disposa.*

6. *No es permet la gravació, custòdia de dades o informació en suports externs sense disposar de l'autorització expressa del responsable del departament o informàtic; i sense disposar de les mesures de seguretat que permeti el no accés de tercers.*

7. *Tots els correus electrònics han de ser enviats mitjançant còpia oculta si es realitza a diversos destinataris, tret que aquests tinguin relació prèvia entre ells i ja disposin dels correus electrònics que figuren en el correu.*

8. *Ha de tenir-se en compte que la imatge és una dada de caràcter personal i per tant és aplicable aquesta normativa, que ens requereix el seu consentiment exprés i poder demostrar-ho. S'ha de ser prudent amb les xarxes socials, disposant de les corresponents autoritzacions per a publicacions d'imatges, de dades o per al seu ús en nom de l'empresa.*

9. *S'ha de guardar el més alt secret professional sobre qualsevol dada o informació responsabilitat de l'empresa, fins i tot una vegada extingida la relació jurídica entre totes dues parts. S'ha de comprometre amb el compliment respectuós de la normativa de protecció de dades així com la confidencialitat respecte a tota la informació de*

l'empresa, podent aquesta exigir les responsabilitats que es puguin derivar per la vulneració del secret professional per part de l'empleat.

10. *L'empleat haurà de llegir atentament el text complet de funcions i obligacions que l'afecta com a empleat, així com qualsevol altre comunicat, instrucció o nota informativa que es rebi; i complir amb les pautes exposades.*

L'empresa