



**GUIA D'ÚS DE LES ESTACIONS
DE TREBALL**

Índex

3 . . . Qui fem aquesta guia?

5 . . . Introducció

5 . . . Audiència

6 . . . Aspectes legals i normatius

7 . . . Pas a pas

7 . . . Què és una estació de treball?

7 . . . Finalitat de l'estació de treball

8 . . . Casos d'estudi

**Per què hem de fer un bon ús
de l'estació de treball?**

9 . . . La condició física del treballador

9 . . . Amenaces

9 . . . Denegació del servei

9 . . . Pèrdua de confidencialitat, integritat i
disponibilitat de la informació

9 . . . Indisponibilitat dels treballadors

9 . . . Instal·lació de programari no autoritzat

10 . . . Amenaces

10 . . . Infecció de l'equip informàtic per virus o

10 . . . codi maliciós

10 . . . Incompliment legal

**11 . . . Divulgació no intencionada
d'informació confidencial**

11 . . . Amenaces

11 . . . Divulgació no autoritzada d'informació

11 . . . Pèrdua d'informació

11 . . . Incompliment legal

**11 . . . Robatori d'equips portàtils o
dispositius mòbils**

11 . . . Amenaces

11 . . . Accés no autoritzat

11 . . . Pèrdua d'informació

12 . . . Incompliment legal

12 . . . Indisponibilitat de l'equip

13 . . . Recomanacions

13 . . . Recomanacions per fer un bon ús
de l'estació de treball

14 . . . Recomanacions a l'hora d'instal·lar
nou programari

14 . . . Recomanacions per protegir la
informació electrònica

15 . . . Recomanacions per protegir la informació
en paper

16 . . . Recomanacions per protegir els ordinadors
portàtils i dispositius mòbils en cas de
robatori o pèrdua

17 . . . Conclusions

19 . . . Glossari de termes

19 . . . Referències i enllaços web

19 . . . Eines

19 . . . Eines per realitzar còpies de seguretat

20 . . . Antivirus i tallafocs locals

20 Eines pel xifratge

20 Eines per gestionar contrasenyes

20 Recursos de suport en línia

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

El contingut de la present guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà mitjançant la inclusió de la següent menció:



Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.


Llicenciada sota la llicència CC BY-NC-ND.

La present guia es publica sense cap garantia específica sobre el contingut.





L'esmentada llicència té les següents particularitats:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament la obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de la obra de la manera especificada per l'autor o el llicenciador (en tot cas no de manera que suggereixi que gaudeix del seu suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Respecte d'aquesta llicència caldrà tenir en compte el següent:

■ **Modificació:** Qualsevol de les condicions de la present llicència podrà ser modificada si vostè disposa de permisos del titular dels drets.

■ **Altres drets:** En cap cas els següents drets restaran afectats per la present llicència:.

■ Els drets del titular sobre els logots, marques o qualsevol altre element de propietat intel·lectual o industrial inclòs a les guies. Es permet tan sols l'ús d'aquests elements per a exercir els drets reconeguts a la llicència.

■ Els drets morals de l'autor.

■ Els drets que altres persones poden tenir sobre el contingut o respecte de com s'empra la obra, tals com drets de publicitat o de privacitat.

Avis: En reutilitzar o distribuir la obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complet de la llicència pot ser consultat a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Introducció

Audiència

Aquesta guia està adreçada als usuaris d'estacions de treball d'universitats i centres de recerca, administracions públiques catalanes i PIME que en fan ús dins del seu entorn professional.

El següent document també està pensat per a:

- Administradors de sistemes
- Encarregats de configurar les polítiques de seguretat per a les estacions de treball
- Membres dels departaments de microinformàtica
- Encarregats d'atendre les peticions i incidències dels usuaris respecte a les seves estacions de treball

Als responsables de seguretat, en canvi, la guia els pot resultar útil a l'hora de conscienciar en les seves tasques els diferents actors que participen del procés dins de l'organització.

Les organitzacions que vulguin implantar un Sistema de Gestió per a la Seguretat de la Informació (SGSI) en un futur pròxim, hauran de tenir en compte les recomanacions d'aquesta guia durant la implantació prèvia a la superació del procés de certificació.

Abast

Aquesta guia permet aconseguir un seguit de bones pràctiques i recomanacions de seguretat, necessàries per realitzar i gestionar un bon ús de les estacions de treball.

Els usuaris d'una empresa o entitat utilitzen les estacions de treball a diari. Els administradors són els encarregats d'aplicar les

polítiques corporatives en les estacions de treball i microinformàtica i de solucionar els problemes i les necessitats dels usuaris respecte de les seves estacions de treball. Tots, doncs, impacten en com es poden utilitzar aquestes estacions de treball.

Per aconseguir que aquestes estacions de treball funcionin correctament i no es converteixin en un maldecap per a l'usuari i la pròpia organització a la qual pertanyen, en aquesta guia es tracten els punts següents:

- Correcta manipulació de les estacions de treball
- Com protegir la informació emmagatzemada
- Com implantar mesures de seguretat física a l'equip
- Configuració i instal·lació de programari
- Dret de propietat intel·lectual
- Protecció de dades de caràcter personal
- Gestió d'incidències
- Assistència remota

Aspectes legals i normatius

La present guia s'ha elaborat tenint en compte les recomanacions provinents de l'estàndard internacional ISO 27002, que queden recollides als següents controls:

- 10.4.1 Controls contra codi maliciós
- 11.3.2 Equips d'usuari desatesos
- 11.3.3 Política de taules i pantalles netes

- 11.7.1 Informàtica mòbil i comunicacions
- 13.1.1 Notificació dels esdeveniments de seguretat
- 15.1.2 Drets de la propietat intel·lectual
- 15.1.4 Protecció de les dades de caràcter personal

Pas a pas

Què és una estació de treball?

L'estació de treball és l'eina que ens permet desenvolupar les nostres tasques laborals dins del context de les noves tecnologies. Com a equip informàtic connectat a una xarxa, l'ordinador permet la interacció entre usuaris, l'accés a la informació, a les aplicacions i als sistemes d'informació necessaris per al desenvolupament habitual de les nostres funcions dins de l'organització.

Hi ha molts elements que poden afectar la seguretat d'una estació de treball. Alguns dels factors més comuns són la connexió a Internet, la pràctica d'emmagatzemar informació de manera local (és a dir, dins del disc dur de l'ordinador), el fet de compartir l'equip amb tercers usuaris o instal·lar-hi noves aplicacions regularment. Per tal de minimitzar els riscos, cal adoptar un conjunt de mesures de seguretat detallades en aquesta guia.

Finalitat de l'estació de treball

L'equip de treball amb el programari instal·lat és una eina que l'organització posa a disposició dels usuaris per al desenvolupament de les seves funcions professionals. Modificar la configuració d'aquesta eina de treball, utilitzar-la per a finalitats no previstes, permetre'n l'accés indiscriminat de tercers o emmagatzemar-hi informació important, no només pot comprometre la màquina, sinó que també pot afectar el funcionament operatiu habitual de l'organització a la qual pertany l'usuari.

Per què hem de fer un bon ús de l'estació de treball?

Un dels actius més importants de tota organització és la informació. Els usuaris tracten aquesta informació, majoritàriament, a través de les estacions de treball.

Si bé és molt pràctic disposar dels permisos adients per fer qualsevol tipus d'actuació a la màquina que tenim assignada, aquest excés de permisos pot convertir-se em un problema. Pensem en alguns exemples concrets:

- Poder deshabilitar l'antivirus de l'equip perquè aquest funcioni més ràpid ens pot solucionar una necessitat puntual, però si aquesta acció comporta la infecció del nostre equip, el temps que s'haurà d'invertir per desinfectar-lo i el risc que més equips de l'organització es vegin afectats superarà amb escreix l'inconvenient puntual que existia per a un usuari concret.
- Tenir la capacitat de configurar connexions cap a l'exterior mitjançant connexions Wi-Fi ens proporciona una gran mobilitat, però si el dispositiu al qual ens connectem per disposar d'aquesta connexió no és de confiança, podem perdre el control del nostre equip i posar en risc la informació que conté.
- També podem donar accés remot al nostre equip a un tècnic perquè ens ajudi a resoldre els problemes que puguem tenir amb la nostra eina de treball, però en fer-ho, si no anem amb compte, correm el risc que un tercer accedeixi a informació confidencial, en pugui fer una còpia, modificar-la i, fins i tot, esborrar-la.

Veiem, doncs, que és important i necessari que tots els usuaris siguin conscients de la necessitat que existeixin uns procediments i unes recomanacions de seguretat interns corporatius. També és important que l'usuari s'abstingui de realitzar accions amb l'estació de treball que puguin interferir en el funcionament ordinari de les instal·lacions informàtiques. En cas contrari, l'usuari s'arrisca a què es produeixi un incident que l'afecti puntualment o que, fins i tot, afecti a l'operativa diària de l'organització.

La condició física del treballador

Les persones i la seva condició física són també aspectes molt importants que cal tenir en compte. Segons el Reial decret 488/1997[3] sobre disposicions mínimes de seguretat i salut relatives al treball amb equips que inclouen pantalles de visualització, el criteri que determina la condició de treballador que utilitza pantalles de visualització de dades és el següent:

- Qualsevol treballador que habitualment i durant una gran part del seu temps laboral utilitzi un equip amb pantalla de visualització.

L'organització haurà d'adoptar les mesures adients perquè l'ús d'aquests equips no suposi riscos per a la seguretat física i la salut dels treballadors.

Amenaces

Denegació del servei

Una infecció d'un equip pot comportar que es quedi totalment inoperatiu. A més, també podria implicar la infecció d'altres actius més crítics dins de l'organització afectada, que també podrien quedar inactius.

Pèrdua de confidencialitat, integritat i disponibilitat de la informació

Si un equip resulta compromès, també es veurà afectada la informació que emmagatzema. Així, si un tercer pot accedir a l'estació de treball (ja sigui mitjançant una connexió remota que pot semblar lícita o com a conseqüència de la infecció per codi maliciós de l'equip), tindrà accés a la informació. Es podria donar el cas que també pogués modificar aquesta informació i, fins i tot, eliminar-la.

Indisponibilitat dels treballadors

Si no s'observen les recomanacions bàsiques de seguretat i salut dins de l'organització, els treballadors podrien arribar a patir problemes de salut que els impedisin exercir la seva activitat laboral amb normalitat.

Instal·lació de programari no autoritzat

L'equip de treball i el programari instal·lat són eines que l'organització posa a disposició del personal per al desenvolupament de les funcions encomanades. Tot i que l'equip ja té el programari necessari per cobrir aquestes funcions, en algunes ocasions cal programari addicional.

Si un usuari té els permisos suficients per instal·lar noves aplicacions al seu equip de treball, l'organització pot incórrer en riscos de diversa gravetat. Els perills més habituals són:

- La violació de drets de propietat intel·lectual, en cas que no es disposi d'una llicència d'ús del programari adequada.
- La utilització de programari descarregat d'entorns que no són de confiança i que podria tenir associat algun tipus de codi maliciós.

Per evitar aquesta mena de situacions, les organitzacions limiten el tipus d'accés dels usuaris a les màquines i deleguen la responsabilitat d'instal·lar nou programari al personal de sistemes i microinformàtica, que gestiona tot el programari adquirit per l'organització i les seves llicències d'ús.

Amenaces

Infecció de l'equip informàtic per virus o codi maliciós

Instal·lar aplicacions de fonts que no són de confiança pot repercutir en la infecció de l'equip per codi maliciós. Si aquest equip forma part de la xarxa corporativa, la infecció es podria arribar a estendre internament a la resta d'equips de l'organització i, depenent de la gravetat de l'incident, l'equip humà encarregat de la seva resolució es podria veure col·lapsat a l'hora de contenir l'atac.

Incompliment legal

Tot programari té associada una llicència d'ús, es tracti de programari comercial o de programari lliure. En alguns casos, la llicència del producte canvia en funció de l'ús que se'n fa (personal o corporatiu).

L'ús de programari sense la llicència corresponent contravé la llei de propietat intel·lectual.

Divulgació no intencionada d'informació confidencial

Avui en dia es tracten i s'intercanvien grans volums de dades, tant de manera electrònica com en paper. La informació d'una organització és un valor que cal protegir en funció de la seva importància.

Si l'usuari de l'equip de treball no té cura de la informació que tracta amb aquesta eina, poden arribar a produir-se situacions com aquestes:

- No bloquejar un equip quan es deixa desatès facilita que un tercer pugui consultar informació per a la qual no està autoritzat.
- Imprimir un document confidencial en una impressora a la qual tenen accés directe altres persones pot ser l'origen d'una divulgació no intencionada d'informació cap a tercers, amb l'afegit que pugui estar-se divulgant també informació personal (per exemple, dades de contacte que formaven part d'un currículum vitae), fets que contravenen la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD[1]).
- Emmagatzemar informació no xifrada en dispositius mòbils (portàtils, memòries USB, DVD, etc.) desatesos en permet la còpia no autoritzada del contingut. Si el dispositiu es perd o ha estat sostret, no només existeix el risc que es produeixi una divulgació no intencionada d'informació, sinó que també hi ha la possibilitat de perdre la informació de l'organització de manera permanent en cas que no existís cap còpia de seguretat.

Aquestes situacions són exemples de per què una organització considera important establir internament recomanacions de seguretat amb l'objectiu d'evitar el risc que suposen.

Amenaces

Divulgació no autoritzada d'informació

No bloquejar l'accés de tercers a informació que no els correspon saber, ja sigui per mitjans electrònics o bloquejant l'accés a un equip o xifrant el contingut d'un suport electrònic com una memòria USB, pot acabar en una fuga d'informació. El mateix passa si s'imprimeix documentació en paper i no se supervisa ni es vigila la impressora o si s'emmagatzema documentació en paper en espais no tancats amb clau.

Depenent de la informació divulgada, l'incident pot arribar a afectar la imatge corporativa.

Pèrdua d'informació

Si es perden equips o suports d'informació, ja siguin suports electrònics o en paper, dels quals no es conserva una còpia interna, l'organització perd permanentment la informació que contenien. Aquesta pèrdua pot impactar en el funcionament habitual dels processos de l'ens i, en funció de la informació, l'incident pot arribar a afectar-ne la imatge corporativa.

Incompliment legal

La pèrdua i divulgació de dades de caràcter personal és punible d'acord amb la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD[1]) en forma de greu sanció econòmica per a organitzacions privades. La gravetat de la sanció varia en funció del tipus d'informació perduda i les condicions que han propiciat la pèrdua.

Robatori d'equips portàtils o dispositius mòbils

La sostracció de portàtils o dispositius mòbils és un fet molt freqüent a l'actualitat. Si es perd l'equip i no s'han adoptat mesures de seguretat específiques, el lladre no només disposarà d'un equip nou, sinó que també podrà aconseguir les configuracions presents a l'equip, com poden ser l'usuari i la contrasenya per accedir a l'ordinador, al domini, a una VPN corporativa o a una xarxa Wi-Fi corporativa. A més, tindrà accés a tota la informació emmagatzemada dins de l'equip.

Amenaces

Accés no autoritzat

Si se sostrau un equip on la informació del disc no està xifrada, es pot aconseguir el compte d'accés a l'equip i, si aquest compte s'utilitza dins d'un domini corporatiu, es disposarà d'unes credencials vàlides per accedir a la xarxa de l'organització des d'alguna de les seves oficines.

Si l'equip també disposa d'una connexió VPN configurada, l'atacant podrà utilitzar-la per intentar accedir remotament a la xarxa de l'organització. El mateix succeeix si l'equip té configurades connexions sense fil (connexions Wi-Fi).

Pèrdua d'informació

En cas de robatori de l'equip, perdrem tota la informació emmagatzemada al disc dur local de la qual no s'hagi fet còpia de seguretat.

Si la informació emmagatzemada al dispositiu no estava xifrada, a més del robatori de l'equip, es pot produir

un robatori d'informació que, depenent de la seva confidencialitat, impactarà en major o menor mesura en l'organització.

Incompliment legal

Si entre la informació perduda hi havia dades de caràcter personal i no s'havien adoptat les mesures de seguretat pertinents, en funció del tipus de dades de què es tractés, si se'n fa un mal ús, l'organització s'enfronta a una situació d'incompliment legal respecte la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD[1]).

Indisponibilitat de l'equip

Si l'usuari afectat no disposa d'un equip equivalent al perdut, no podrà prosseguir normalment amb les seves tasques mentre no disposi d'un equip nou, fet que pot impactar en l'operativa en què participa dins de l'organització.

Recomanacions

Cadascun dels escenaris plantejats en aquesta guia exposa un seguit d'amenaques que, si es materialitzen al llarg del temps, en major o menor mesura, tindran efectes perjudicials per a l'organització a la qual pertanyen. Per tal d'evitar que això succeeixi o minimitzar-ne l'efecte, si l'amenaça no pot evitar-se totalment, a continuació es proporcionen tot un conjunt de recomanacions dirigides als responsables i usuaris de les estacions de treball.

Recomanacions per fer un bon ús de l'estació de treball

Els usuaris han de tenir presents aquestes recomanacions a l'hora d'utilitzar l'estació de treball:

- Abstenir-se de realitzar qualsevol ús que interfereixi en el correcte funcionament de les instal·lacions informàtiques.
- No utilitzar l'equip de treball amb finalitats no autoritzades per l'organització.
- Per tal de protegir la xarxa interna de l'organització, no utilitzar ordinadors propietat de l'usuari si no compleixen els requeriments mínims de seguretat establerts per als equips corporatius.
- Disposar de programari antivirus instal·lat i actiu a l'estació de treball i no modificar-ne la configuració.
- No configurar dispositius de comunicació (Bluetooth, Wi-Fi, etc.). Utilitzar només els que proporciona l'organització i que ja es troben configurats a l'estació de treball.

- Notificar qualsevol incidència amb l'estació de treball a través dels canals establerts, ja que pot ser símptoma d'infeccions o de mal funcionament d'algun component.
- No obrir mai les estacions de treball per intentar reparar-les. El que cal fer és contactar amb el departament de l'organització encarregat d'aquestes tasques.
- Un usuari no hauria d'atendre cap petició d'assistència remota a l'estació de treball si no ha estat informat prèviament de l'acció d'assistència per part del servei de suport.
- No autoritzar l'assistència remota si l'estació de treball conté informació classificada com a confidencial.
- Cal estar present davant de l'estació de treball durant la sessió d'assistència remota.
- Les estacions de treball s'han de situar a sobre de les taules o en suports específics. Les màquines no s'han de situar al terra ni se n'ha de canviar l'orientació inicial (per exemple, col·locar en vertical màquines instal·lades en posició horitzontal).
- Cal prestar especial atenció a la posició de les estacions de treball respecte de l'usuari: l'alçada de la pantalla, la posició del teclat i la posició corporal que s'adopta en seure davant de l'ordinador. Si no es fa correctament, podria ocasionar molèsties corporals.

Recomanacions a l'hora d'instal·lar nou programari

Els usuaris han de tenir presents aquestes recomanacions sempre que necessitin disposar de nou programari a les estacions de treball:

- Les estacions de treball es configuren per optimitzar la productivitat i el manteniment del parc informàtic corporatiu. És per aquest motiu que és important que un usuari no pugui alterar la configuració predefinida.
- L'usuari d'una d'estació de treball no necessita tenir accés a la configuració d'arrencada de l'ordinador.
- No s'ha de permetre la instal·lació de programari no autoritzat per l'organització. Això evita una disminució del rendiment de la infraestructura interna, possibles funcionaments anòmals o infeccions de les màquines.
- L'usuari no necessita tenir accés a còpies del programari, ja que la instal·lació la durà a terme el personal que té atribuïdes aquestes funcions i que també gestiona el parc de llicències.

Recomanacions per protegir la informació electrònica

La informació és un actiu important per a tota organització. Per aquest motiu, cal garantir que aquesta informació estigui protegida i es pugui recuperar en cas de pèrdua.

Així, les recomanacions que cal que tinguin presents els usuaris de les estacions de treball són les següents:

- Quan s'utilitzin ordinadors portàtils o dispositius mòbils en llocs públics, sales de reunions o altres àrees fora del lloc de treball habitual, cal prendre les mesures adients per evitar que persones alienes puguin visualitzar o accedir a la informació de l'ordinador sense autorització.
- Configurar l'estalvi de pantalla perquè sol·liciti contrasenya i s'activi després d'un temps d'inactivitat d'entre 5 i 10 minuts.
- Quan l'estació de treball estigui connectada a la xarxa directament per cable, desactivar l'enllaç a la xarxa Wi-Fi, si existeix i està activa.
- Si es necessita compartir un recurs (com pot ser una carpeta o un dispositiu), es realitzarà aplicant les mesures de seguretat fixades per l'organització.
- En el cas que la informació emmagatzemada a l'estació de treball sigui de caràcter personal, s'aplicaran les mesures de seguretat adients per complir amb la normativa vigent de protecció de dades[1].
- Apagar l'estació de treball quan finalitza la jornada laboral.
- Per evitar accessos indeguts i duplicitats d'informació, cal facilitar la compartició d'informació i garantir-ne la continuïtat. Així, sempre que sigui possible, s'evitarà emmagatzemar informació al disc local i en suports externs i la xarxa de l'organització es convertirà en el principal recurs d'emmagatzematge.
- Quan sigui indispensable emmagatzemar informació al disc local o en suports externs, caldrà aplicar les mesures adequades per protegir la informació segons el nivell de confidencialitat o cri-

titat d'aquesta, protegint-la sempre d'accessos il·legítics.

- És responsabilitat de l'usuari i no de l'organització garantir la continuïtat d'aquesta informació mitjançant la realització de còpies de seguretat periòdiques a la xarxa[2]. Com que la informació és propietat de l'organització, sempre haurà d'existir una còpia de seguretat no xifrada emmagatzemada de manera segura als recursos de l'Organització i no al disc local.

Recomanacions per protegir la informació en paper

La informació que tractem mitjançant la nostra estació de treball es troba en format electrònic, però en nombroses ocasions és necessari imprimir-ne una còpia en format paper. Si cal preservar i protegir la informació en format electrònic, també s'ha de fer amb la informació en paper. La importància de la informació no depèn del suport on es troba, sinó del seu valor, de la seva criticitat. Les recomanacions que han de tenir presents els usuaris de les estacions de treball que realitzen còpies en paper en algun moment són les següents:

- Emmagatzemar i arxivar la informació en suport paper de manera segura per tal d'impedir l'accés a persones no autoritzades.
- Cal tenir la màxima cura en el tractament de la informació impresa en paper i recollir sempre la documentació en finalitzar la jornada laboral.

- Si es tracta de dades especialment sensibles, bé pel grau de confidencialitat, bé per tractar-se de dades de caràcter personal especialment protegides per la LOPD[1], caldrà guardar la documentació en paper en un lloc segur i amb accés restringit únicament a aquelles persones que disposin de l'autorització pertinent.
- No deixar impressions sense recollir a les impressores.
- Realitzar la impressió de dades confidencials mitjançant impressores amb accés restringit i controlat.
- Utilitzar les destructores de paper per eliminar la documentació impresa obsoleta, especialment si conté informació confidencial o protegida per la llei de protecció de dades personals[1].

Recomanacions per protegir els ordinadors portàtils i dispositius mòbils en cas de robatori o pèrdua

Els dispositius mòbils són susceptibles de ser robats o perduts. És per aquest motiu que els usuaris han de tenir en compte les recomanacions següents:

- Quan s'utilitzin ordinadors portàtils o dispositius mòbils en llocs públics, sales de reunions, o altres àrees fora del lloc de treball habitual, no s'han de deixar mai desatesos. Sempre que sigui possible, cal dotar-los de dispositius antirobatori que permetin lligar-los a elements fixos.
- Si s'ha de viatjar és millor no facturar l'equip o el dispositiu com a equipatge. S'ha de portar sempre a mà.

- En absències prolongades (vacances, permisos, etc.) de l'usuari, durant les quals no s'hagi d'usar el dispositiu, es recomana guardar-lo de manera segura.
- En cas de robatori o pèrdua de l'equip portàtil o dispositiu mòbil fora de les instal·lacions de l'organització, s'ha de presentar denúncia davant dels cossos de seguretat per tal de formalitzar el que ha succeït.

Conclusions

La primera vegada que un ordinador va ser qualificat com a estació de treball va ser l'any 1959. Es tractava de l'estació de treball IBM 1620, una petita computadora científica preparada per ser utilitzada per una única persona.

Avui en dia, l'estació de treball ha evolucionat de la mateixa manera que la tecnologia i les seves aplicacions. Una estació de treball pot ser des d'un simple ordinador de taula, fins a un portàtil, un dispositiu mòbil o un Assistent Digital Personal (PDA).

Les xarxes de comunicacions també han evolucionat. Actualment podem fer ús de xarxes de comunicació sense fils que ens faciliten la mobilitat. Ara és possible realitzar les nostres funcions des d'una ubicació remota. Si bé aquesta evolució té molts avantatges, tal com s'ha pogut veure al llarg d'aquesta guia, també suposa l'aparició de noves amenaces a causa de l'existència d'estacions de treball fora de les instal·lacions de l'organització. Per això, cal vigilar la seguretat física d'aquests dispositius per impedir que tercers hi accedeixin fàcilment, que els robin o que es perdin.

Hem de tenir present que la informació emmagatzemada en una estació de treball pot ser extremament important per a l'organització, ja sigui perquè permet esbrinar configuracions internes o comptes d'accés vàlids o bé perquè es tracta d'informació estratègica, personal[1], organitzativa, comptable o similar.

Com a conclusió, cal remarcar que el fet de normalitzar les pautes de funcionament de les estacions de treball és

un punt molt important per a les organitzacions. S'han d'establir normes i mesures de seguretat internes, en especial, les associades a un bon ús de les estacions de treball. I, és clar, cal transmetre-les als treballadors perquè les tinguin presents i les compleixin en tot moment.

Glossari de termes

Estalvi de pantalla: imatge que s'activa de manera automàtica a la pantalla de l'estació de treball després d'un cert temps d'inactivitat. Sovint, els estalvis de pantalla sol·liciten una contrasenya per poder accedir novament a l'estació de treball.

PDA (Assistent Digital Personal): dispositiu electrònic mòbil, inicialment dissenyat com a agenda electrònica amb funcionalitats bàsiques com calendari, llista de contactes, bloc de notes, etc. Avui en dia, aquests dispositius poden realitzar moltes altres funcions, com ara crear documents, jugar, fer ús del correu electrònic o navegar per la xarxa. Es tracta d'un dispositiu mòbil.

Sistema d'Alimentació Ininterrompuda (SAI): equip amb alimentació elèctrica que disposa d'una bateria de gran capacitat i que permet proporcionar energia elèctrica a tots els equips que hi estiguin connectats en cas de caiguda del subministrament elèctric general. El SAI actua també com a regulador de pics de tensió de la xarxa elèctrica.

Tallafocs: maquinari o programari utilitzat a les xarxes de comunicacions per prevenir alguns tipus de comunicacions prohibides o indesitjades.

Xarxa Privada Virtual (VPN): és una tecnologia que permet estendre la xarxa local a la xarxa pública.

Referències i enllaços web

En l'elaboració de l'actual guia s'ha utilitzat com a referència:

GE-GUI25-01 ÚS DE L'ESTACIÓ DE TREBALL, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

A la xarxa s'hi pot trobar informació rellevant relacionada amb la matèria desenvolupada en aquesta guia:

- [1] Agència Espanyola de Protecció de Dades.
<https://www.agpd.es>
- [2] CESICAT, Guia de còpies de seguretat.
[PDF] <http://www.cesicat.cat/fitxers/publicacions/Guia%20copies%20de%20seguretat.pdf>
- [3] Reial decret 488/1997, del 14 d'abril, sobre les disposicions mínimes de seguretat i salut relatives al treball amb equips que incloquin pantalles de visualització (BOE núm. 97 23-04-1997).
[PDF] http://www.oect.es/InshtWeb/Contenidos/Normativa/TextosLegales/RD/1997/488_97/PDFs/realdecreto-4881997de14deabrilsobredisposicionesminimasd.pdf

Eines

Eines per realitzar còpies de seguretat

Amanda

<http://www.amanda.org/>

Cobian

<http://www.educ.umu.se/~cobian/cobianbackup.htm>

CopiaDATA

<http://www.copiadata.com/clientes/copiadata/>

eSaveData

<http://www.esabe.com>

SeCoFi

<http://www.thephoenixprod.com/programas/secofi/>

Antivirus i tallafocs locals

Avast

<http://www.avast.com/>

Comodo

<http://www.comodo.com/>

Eines pel xifratge

GNUpg

Implementació lliure de l'estàndard OpenPGP definit al RFC4880

<http://www.gnupg.org/>

TrueCrypt

Aplicació de codi obert que xifra dispositius d'emmagatzematge

<http://www.truecrypt.org/>

Eines per gestionar contrasenyes

Password Manager

Eina de pagament que permet guardar i gestionar contrasenyes de manera segura

<http://www.cp-lab.com>

Password Safe

Eina lliure que permet guardar i generar contrasenyes de manera segura

<http://passwordsafe.sourceforge.net/>

Recursos de suport en línia

Com seure davant l'ordinador

(audiovisual)

Televisió de Catalunya

<http://www.tv3.cat/videos/193077910/Com-seure-davant-lordinador#>

Prevenió de riscos a l'oficina

(document escrit en format PDF)

Pla de prevenció de riscos laborals UPC 1998-2001

https://www.upc.edu/prevencio/fes_prevencio/arxius/manuals/riscos_oficina.pdf

Treball amb pantalles de visualització de dades: usuaris d'ordinadors

(document escrit en format PDF)

Generalitat de Catalunya

http://www20.gencat.cat/docs/governacio/Funcio%20Publica/Documents/Empleats%20publics/Arxius/pantalla_ordinador.pdf

Altres guies publicades a www.cesicat.cat

Guia per a l'ús segur de les xarxes socials

Aquesta guia està dirigida a totes les persones que són usuàries habituals de les xarxes socials virtuals.

Aquesta guia també està pensada per a les persones que, tot i no pertànyer a cap xarxa social virtual, hi estan interessades i volen conèixer quines precaucions haurien d'adoptar si, finalment, decidissin provar d'utilitzar-ne alguna.

Guia per gestionar les contrasenyes

Aquesta guia està adreçada als usuaris d'universitats i centres de recerca, administracions públiques catalanes i PIME que utilitzen serveis telemàtics dins de l'entorn professional que requereixen la utilització de contrasenyes d'accés.

Aquesta guia també està pensada per als administradors de sistemes, encarregats de configurar els perfils d'accés i les polítiques de seguretat dels sistemes d'informació. Els responsables de seguretat la trobaran útil a l'hora de conscienciar els usuaris de l'organització quant a l'ús de les contrasenyes i el seu manteniment.

Les organitzacions que en un futur pròxim vulguin implantar un Sistema de Gestió per a la Seguretat de la Informació (SGSI) hauran de tenir en compte les recomanacions d'aquesta guia durant la implantació prèvia a la superació del procés de certificació.



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat