



GUIA DE CÒPIES DE SEGURETAT

Índex

5.....	Introducció	13.....	Recomanacions per recuperar la informació
5.....	Audiència	14.....	Recomanacions per guardar, localitzar i verificar la validesa de les còpies de seguretat
5.....	Abast	15.....	Recomanacions per minimitzar l'amenaça en cas d'un desastre que afecti greument a les instal·lacions on es desenvolupa l'activitat
6.....	Aspectes legals i normatius	15.....	Recomanacions en cas de la necessitat de compliment legal
7.....	Descripció general	16.....	Conclusions
7.....	Què és i en què consisteix?	17.....	Glossari de termes
8.....	Finalitat	17.....	Referències i enllaços web
9.....	Casos d'estudi	18.....	Eines
9.....	Per què cal una còpia de seguretat		Eines per a realitzar còpies de seguretat
	Descripció		Eines per recuperació de dades.
	Amenaces		
10.....	Còpia corrupte amb dades de caràcter personal		
	Descripció		
	Amenaces		
10.....	Importància d'una bona gestió dels suports físics de còpia		
	Descripció		
	Amenaces		
11.....	Continuïtat en cas de desastre que afecti a les instal·lacions		
	Descripció		
	Amenaces		
12.....	Recomanacions		
12.....	Recomanacions a l'hora de definir i realitzar les còpies de seguretat corporatives		

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 logotips, 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 responsables i operadors de còpia d'Universitats i Centres de Recerca, Administracions públiques catalanes i PIME que realitzen còpies de seguretat a l'entorn professional. Indirectament, aquesta guia també pot resultar d'interès per als responsables dels serveis i/o aplicacions.

Als responsables de seguretat d'aquestes comunitats els pot resultar útil a l'hora de conscienciar als actors que participen del procés dins de l'organització en les seves tasques.

Aquesta guia també s'ha pensat per als responsables de seguretat que pertanyin a organitzacions que en un futur pròxim vulguin implantar un Sistema de Gestió per a la Seguretat de la Informació (SGSI). Si bé aquesta guia no es podria incorporar directament dins del cos normatiu de gestió, sí que inclou tots els aspectes i les recomanacions que l'organització hauria de tenir presents i implantar per superar el procés de certificació.

Abast

Aquest document permet assolir un seguit de bones pràctiques i recomanacions de seguretat, necessàries per realitzar i gestionar de manera correcta les còpies de seguretat. Es cobreixen els punts d'interès següents: la realització de còpies, la recuperació de la informació, procediments, proves, gestió de suports, seguretat física, continuïtat, traçabilitat, incidències i compliment legal.

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 controls següents:

- 9.1.2 Controls d'accés físic.
- 9.1.4 Protecció contra amenaces externes i ambientals.
- 9.2.7 Sortida de propietats.
- 10.5.1 Còpies de seguretat de la informació.
- 10.7.2 Retirada dels suports.
- 10.7.3 Procediments de maneig de la informació.
- 10.8.3 Transport de suports.
- 10.10.3 Protecció de la informació dels registres.
- 15.1.1 Identificació de la legislació aplicable.
- 15.1.4 Protecció de les dades de caràcter personal i de la privacitat de les persones.

Cal tenir en compte el compliment de la legislació vigent pel que fa al tractament de la informació. Cal donar compliment a les mesures requerides per la Llei de Protecció de Dades de Caràcter Personal (LOPD[1]) i, més concretament, al reglament que la desenvolupa, on s'especifiquen els requeriments per a la gestió de les còpies de seguretat. Així mateix, caldrà tenir en compte altres requeriments legals que puguin afectar les dades i la seva conservació. retat de la informació prescrits per la legislació d'adminis-

tració electrònica i s'ha d'entendre sense perjudici d'altres normes aplicables que estableixen obligacions de seguretat de la informació, en particular la legislació de protecció de les dades de caràcter personal.

És important notar que els subjectes obligats a donar compliment a ambdues normatives hauran de coordinar-ne el compliment mitjançant documentació conjunta o la implementació de les mesures de seguretat tècniques i/o organitzatives necessàries.

Descripció general

Què és i en què consisteix?

La informació és un actiu important per a tota organització. Imaginem-nos, sinó, què passaria si un bon dia ens adonem que hem perdut tota la comptabilitat o que el nostre sistema de facturació, de sobte, no disposa de cap dada. Per evitar situacions d'aquest tipus, cal garantir que aquesta informació es pugui recuperar en cas de pèrdua, ja sigui totalment o parcial.

Un dels mecanismes de protecció de la informació consisteix a realitzar una còpia de seguretat que serà utilitzada en cas de necessitat, per restaurar la informació al punt que permeti que un servei o sistema pugui tornar a estar operatiu. En funció de com es realitza la còpia, existeixen diferents tipus de còpies de seguretat:

- **Totals:** es realitza una còpia de seguretat completa de tota la informació d'un servei o sistema.
- **Diferencials:** es realitza una còpia de seguretat de totes les dades que s'hagin modificat des de l'última còpia total.
- **Incrementals:** es realitza una còpia de seguretat de la informació que s'ha modificat respecte de l'última còpia.

A l'hora de realitzar les còpies de seguretat, cal realitzar una còpia tant de la informació corporativa com de les dades pròpies del sistema que les sustenta. El fet de disposar d'una còpia només amb la informació corporativa, sense possibilitat de recuperar un sistema a partir d'una imatge, alenteix el procés de tornar a disposar de la informació.

És important analitzar els requeriments que presenta un servei i/o aplicació, abans de determinar quin és el sistema de còpia i recuperació adient per a l'organització.

Finalitat

La finalitat de les còpies de seguretat consisteix a poder disposar d'una còpia de les dades el més actualitzada possible que ens permeti recuperar-nos davant d'alguna pèrdua o caiguda del sistema.

Aquest procés, per tant, ens permet tenir emmagatzemades, en format digital, còpies de la informació corporativa que ens permetran restaurar un sistema a un estat similar o igual al que teníem just abans de l'incident, o bé recuperar informació puntual en forma de fitxers individuals que hagin pogut resultar malmesos o que han estat modificats erròniament pels usuaris. En resum, les còpies de seguretat permeten mantenir una certa capacitat de recuperació de la informació en cas de possibles pèrdues. Aquesta capacitat pot ser molt important i, en determinats casos, es pot convertir en crítica.

Casos d'estudi **Per què cal una còpia de seguretat**

Descripció

Hem passat de generar un gran volum de documentació en paper a utilitzar-ho gairebé tot en suports digitals. La informació és un valor crític que cal protegir, ja que és necessària per mantenir la capacitat de prestar servei o de distribuir i vendre productes manufacturats de l'empresa.

Depenent de la importància de l'incident que hagi pogut patir la informació corporativa, si el responsable del sistema no ha generat una còpia de seguretat adequada, aquest fet podria interferir negativament en l'operativa diària de l'organització afectada o en aspectes encara més greus que podrien causar un impacte econòmic i en la imatge corporativa.

Amenaces

Pèrdua d'informació

Si no es disposa de còpies de seguretat en bon estat, si es produeix qualsevol tipus d'incident que malmeti informació, l'organització no podrà recuperar el sistema en un estat similar al que existia just abans del moment de l'incident. Aquest fet pot repercutir negativament en l'organització de diferents maneres. Tot dependrà de la cripticitat de la informació que ha resultat afectada.

Denegació de servei

Si l'incident ha afectat directament el sistema, es produeix una denegació de servei, ja que el sistema ha deixat de funcionar. Aquesta situació perdurarà mentre no es pugui restaurar de nou i, si no es disposa d'una còpia de seguretat en condicions del sistema, el temps que caldrà inver-

tir per tal de recuperar-lo serà molt superior al que caldria emprar si existís una còpia de seguretat vigent.

Còpia corrupta amb dades de caràcter personal

Descripció

És important aplicar una política de còpies de seguretat coherent amb el nivell d'actualització de la informació dins de l'organització. Si bé la informació del sistema canvia poc al llarg del temps, la informació corporativa s'actualitza, modifica i esborra cada dia i els usuaris que gestionen i tracten aquesta informació n'introdueixen de nova a diari. Per tant, en funció de la seva cripticitat, caldrà determinar quina és la política de seguretat aplicable més adient.

Una còpia de seguretat per si mateixa, però, no constitueix una garantia si no se'n comprova el correcte funcionament i no es disposa dels procediments necessaris per tal de recuperar la informació que conté. No només pot fallar el sistema de còpia, també pot fallar el suport, bé per algun defecte, bé perquè no s'ha emmagatzemat en les condicions adients.

Si perdre còpies de seguretat pot tenir un impacte considerable per a l'organització, sempre en funció de la importància de la informació que s'ha perdut, si existeixen dades de caràcter personal que formen part d'aquesta pèrdua, podem incórrer en incompliments legals (RD 1720/2007) i, per tant, l'organització es troba sotmesa al risc d'haver de pagar multes que podrien tenir un fort impacte addicional per a l'entitat afectada.

Amenaces

Pèrdua d'informació

Quan una organització no disposa de còpies de seguretat en bon estat, si es produeix qualsevol tipus d'incident que malmeti informació, aquesta no podrà recuperar el sistema a un estat similar al que existia just abans del moment de l'incident. Aquest fet pot repercutir negativament en l'organització de diferents maneres, depenent de la cripticitat de la informació que ha resultat afectada.

Incompliment legal

No dur a terme còpies de seguretat d'aquelles dades de caràcter personal en possessió de l'entitat, no verificar la idoneïtat d'aquestes còpies de seguretat o no ser capaç de restaurar el teu sistema a un estat similar al del moment de l'incident són incompliments de la Llei Orgànica de Dades de Caràcter Personal, concretament del Reial decret 1720/2007, del 21 de desembre, i poden suposar fortes multes per a l'organització.

Importància d'una bona gestió dels suports físics de còpia

Descripció

L'aplicació d'una política i d'uns procediments adequats per realitzar còpies de seguretat s'ha de complementar amb un seguit de regles i recomanacions aplicables a l'emmagatzemament i etiquetatge dels suports digitals utilitzats. Això ens permetrà reduir els temps de recuperació en cas de desastre i/o pèrdua de la informació.

Si no podem localitzar en un temps de resposta prudential les còpies de seguretat adients a cada situació, l'ex-

cés de temps invertit repercutirà negativament en la recuperació de l'activitat corporativa i podria convertir-se en una situació crítica a l'hora de prestar servei als clients.

CPD amb les úniques còpies de seguretat a dins, l'organització no podrà recuperar els seus sistemes d'informació ja que les còpies de seguretat s'hauran perdut juntament amb els equips. Per tant, l'entitat no podrà tornar a prestar servei als seus clients i es veurà forçada a tancar.

Amenaces

Denegació de servei

Si l'incident ha afectat el sistema de manera directa, es produeix una denegació de servei perquè el sistema ha deixat de funcionar. Aquesta situació perdurarà mentre el servei no es pugui restaurar de nou i, si no es disposa d'una còpia de seguretat del sistema en condicions, el temps que caldrà invertit per tal de recuperar-lo serà molt superior a sí existís una còpia de seguretat vigent.

Continuïtat en cas de desastre que afecti les instal·lacions

Descripció

Poder disposar d'un seguit de còpies de seguretat que ens permetin recuperar la nostra activitat en cas de desastre i/o pèrdua de la informació és prioritari per assegurar la continuïtat de la nostra activitat.

Si es produeix un desastre que afecti greument les instal·lacions on es realitza l'activitat i el responsable de les còpies de seguretat no ha contemplat aquest supòsit i les còpies de seguretat no estaven en una ubicació remota, ho haurem perdut tot.

Amenaces

Pèrdua d'informació

Si no es disposa de còpies de seguretat en bon estat i es produeix un desastre, com per exemple un incendi del

Recomanacions

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

Recomanacions a l'hora de definir i realitzar les còpies de seguretat corporatives

Els responsables i operadors de còpia hauran de tenir en compte les recomanacions següents quan calgui definir els requeriments per dur a terme les còpies de seguretat:

- És recomanable que l'extensió, la periodicitat, el tipus (total, parcial o incremental) i la retenció de les còpies de seguretat estiguin alineats amb els requeriments del servei i/o l'aplicació dels quals es realitza la còpia de la informació.
- De manera conjunta amb el responsable del servei i/o l'aplicació, caldrà analitzar si el servei conté dades de caràcter personal i, en aquest cas, avaluar-ne el nivell. També caldrà determinar si les dades estan sotmeses a alguna altra legislació vigent, per tal de garantir-ne el compliment.
- El responsable del servei i/o l'aplicació hauria de determinar el temps màxim de restauració de les còpies.

- Sempre que sigui possible, l'anàlisi s'hauria de realitzar per als diferents entorns (producció, preproducció, integració, etc.) del servei i/o l'aplicació. Per a nous serveis i/o aplicacions, aquesta anàlisi s'hauria de fer en la fase de definició inicial.
- És recomanable realitzar còpies de seguretat de les dades, les aplicacions i el sistema operatiu de tots els actius que formen el servei i/o l'aplicació, inclosos els entorns tant productius com no productius.

Si en un entorn existeixen diferents actius amb una configuració idèntica, inclòs el maquinari, serà suficient realitzar la còpia de les aplicacions i la de sistema operatiu d'un sol actiu.

- Per al cas dels entorns no productius, podran existir diferents plans de còpies de seguretat amb un període de retenció menor que les dels entorns productius, prèvia aprovació del responsable del servei i/o les aplicacions.
- Per a entorns on no es disposi de xarxes dedicades, caldrà analitzar la necessitat de desenvolupar un pla d'acció per implementar una xarxa dedicada a la realització de les còpies.
- S'aconsella que les còpies de seguretat es realitzin dins d'una finestra de temps que serà aprovada pel responsable del servei i/o l'aplicació. El responsable analitzarà la franja de temps on l'entorn té menys càrrega per poder determinar la finestra temporal, preferiblement fora de l'horari laboral.
- Per als entorns productius, i sempre que tècnicament sigui possible, les còpies s'haurien de poder realitzar sense necessitat d'aturar el servei i/o l'aplicació (cò-

pia en calent). Es recomana realitzar almenys una còpia un cop l'any amb el servei aturat.

- Per als entorns no productius es podran consensuar amb el responsable del servei i/o l'aplicació finestres d'aturada per a permetre la realització de les còpies de seguretat.
- Si la informació que s'ha de copiar ha d'estar xifrada, caldria que el xifrat utilitzat fos un estàndard reconegut i no un xifrat propietari de cap programari. Es recomana l'ús de l'estàndard AES amb claus de 256 bits.

Recomanacions per recuperar la informació

Els responsables i operadors de còpia hauran de tenir en compte les recomanacions següents quan defineixin els procediments necessaris, tant per a la realització de còpies de seguretat com per a la recuperació de la informació:

- Caldrà definir procediments de còpia i recuperació de dades que contemplin les accions i els passos necessaris per a l'execució dels processos.
- Els procediments de recuperació hauran de garantir la reconstrucció en l'estat en què estaven les dades al moment de produir-se'n la pèrdua. Caldrà que contemplin la recuperació de les dades tant a nivell de fitxer com de sistema.
- Sempre que sigui possible es durà a terme una revisió regular dels procediments per assegurar-ne l'efectivitat, vigència i completesa.
- S'han de definir procediments per a la gestió de suports amb còpies de seguretat que en contemplin el tractament i l'emmagatzemament.

- Només les persones autoritzades pel responsable del servei i/o l'aplicació podran sol·licitar operacions de restauració de les còpies. Caldrà implantar mecanismes d'autenticació i no repudi en la verificació dels peticionaris de restauracions de còpies.
- Caldrà que la informació es pugui recuperar en el temps establert pel responsable del servei i/o l'aplicació. El temps serà el que s'hagi determinat en la fase d'anàlisi de requeriments del servei i/o l'aplicació.

D'altra banda, el responsable haurà de tenir en compte les recomanacions següents en cas d'eliminació o destrucció de les còpies de seguretat:

- Caldrà disposar d'un procediment d'eliminació d'informació dels suports, en cas que siguin reutilitzats.
- És recomanable tenir un procediment de destrucció de suports, en cas que siguin rebutjats (baixa del servei i/o l'aplicació, funcionament incorrecte d'un suport, etc.).

Recomanacions per guardar, localitzar i verificar la validesa de les còpies de seguretat

Els responsables i operadors de còpia hauran de tenir en compte les recomanacions següents:

- Caldria garantir que els suports utilitzats per emmagatzemar les còpies de seguretat són d'ús exclusiu de l'organització.
- Mantenir un inventari detallat de tots els suports que continguin còpies de seguretat.
- Utilitzar una nomenclatura comuna per a la identi-

ficació de tots els suports que possibiliti la identificació de la informació que conté el suport.

- S'evitarà que la identificació sigui directa, especialment si hi ha dades crítiques quant a confidencialitat o privadesa.
- Quan la gestió dels suports es confiï a una tercera empresa, caldrà que es formalitzin els contractes legals que permetin garantir la disponibilitat, confidencialitat i integritat de les còpies, així com els procediments d'entrega i recepció de còpies i el protocol d'emergència. D'altra banda, és necessari implementar un registre d'entrada i sortida de suports.
- És important respectar el temps de vida dels suports indicat pel fabricant i definir-ne un pla de rotació que en garanteixi la fiabilitat i el bon funcionament.
- Cal realitzar proves periòdiques de recuperació de dades de cada servei i/o aplicació com a mínim un cop l'any (aconsellable dos cops l'any) i sempre que es produeixi un canvi en la infraestructura del servei i/o l'aplicació.
- Les proves hauran de permetre tant la comprovació dels suports que contenen les còpies com la restauració d'un sistema per complet o de manera parcial. Per considerar vàlides les proves és necessari que s'alternin de manera aleatòria els jocs de suports, sistemes sobre els quals realitzar la restauració i dades parcials o totals restaurades.
- En cas de recuperació per causa d'un incident real, es podrà considerar com a prova de recuperació.
- És recomanable disposar d'un registre de les activitats de còpia, restauració i destrucció, que reculli com a mínim la data, l'hora, la persona que l'executa

i el resultat de l'operació. És important guardar un registre de les proves de recuperació que es realitzin i del seu resultat.

- Com a norma general, si es produeix alguna incidència en la gestió de les còpies de seguretat, caldrà notificar-ho al responsable del servei i/o l'aplicació.
- Les accions portades a terme per a la seva resolució s'hauran de documentar.

Recomanacions per minimitzar l'amenaça en cas d'un desastre que afecti greument les instal·lacions on es desenvolupa l'activitat

El responsable de la gestió de les còpies de seguretat haurà de tenir en compte les recomanacions següents per tal de garantir la continuïtat de l'activitat en cas d'un desastre extrem que afecti les instal·lacions i si queden malmeses les còpies de seguretat locals:

- Per tal que sigui possible la continuïtat, hi ha d'haver una còpia de seguretat disponible en una ubicació que no estigui sotmesa als mateixos riscos que l'edifici on s'ubiquen els sistemes d'informació.
- Quan els temps de restauració establerts siguin molt curts, pot ser recomanable disposar addicionalment de còpies en una ubicació propera a la ubicació dels sistemes.
- Per a serveis i/o aplicacions molt crítics pot ser recomanable disposar d'una segona còpia en una ubicació diferent a la ubicació habitual dels suports.
- Caldrà definir un pla de continuïtat per al sistema de gestió de còpies de seguretat, que garanteixi l'opera-

tivitat del servei de còpies per a sistemes considerats com a crítics.

Recomanacions en cas de necessitat de compliment legal

En el cas que les còpies de seguretat emmagatzemin dades que necessitin d'un compliment legal, recomanem al responsable del servei i al responsable de còpia que tinguin en compte les recomanacions següents:

- Quan la informació a copiar contingui dades de caràcter personal, caldrà donar compliment als requeriments de seguretat indicats al Reglament de la LOPD[1].
- Per als serveis i/o aplicacions que gestionin informació subjecta a compliment legal (judicial, financera, sanitària, etc.), serà el responsable del servei i/o aplicació qui especifiqui el període de retenció i les mesures de seguretat aplicables a les còpies.

Conclusions

Avui en dia, el més important per a les empreses és la informació. En aquesta nova era tecnològica hem passat de generar un gran volum de documentació en paper a utilitzar suports digitals constantment.

Imagina't arribar un dia a l'oficina i comprovar que has perdut totes les dades del teu ordinador personal o servidor. Existeix una còpia de seguretat que et permeti continuar amb la teva activitat? Quin temps has de dedicar a recuperar els sistemes fins que assoleixin una operativa normalitzada? T'hi pots dedicar? Les màquines no són infalibles i en qualsevol moment poden fallar. Cal estar preparats per a quan això passi i així minimitzar la possible amenaça de pèrdua de la nostra activitat.

Un estudi realitzat per Ontrack [2] als Estats Units denota que el 76% de les empreses d'aquest país té la sensació que està en risc la supervivència de la seva empresa en cas de fallida amb un interval de 24 a 72 hores, el 20% pensa que amb 8 hores el perjudici pot ser important i el 8% de les empreses creu que amb 1 hora és suficient per afectar greument la seva continuïtat de negoci.

A Espanya, segons un estudi realitzat per l'Associació Espanyola per a la Direcció Informàtica (AEDI)[3] sobre la situació actual i les tendències a les empreses consumidores de tecnologia de la informació l'any 2005, en cas de catàstrofe es podria arribar a recuperar un 88,5% de la informació. El temps mig de recuperació de la informació és de 51 hores. Dades d'un altre estudi realitzat l'any 2002 indiquen que el 74% de les empre-

ses espanyoles creuen que no podrien superar més de 4 dies sense informació.

Sense una còpia de seguretat amb garanties, una organització és molt vulnerable. Què passaria si juntament amb els sistemes perdem les còpies de seguretat? El fet de tenir un sistema de seguretat no significa que les dades es guardin de manera efectiva. Si es perd la còpia de seguretat amb la màquina que havia d'estar protegida, s'haurà perdut tot.

Glossari de termes

Còpia en calent: mecanisme que permet la realització de la còpia de seguretat sense necessitat d'aturar el servei.

CPD (Centre de Processament de Dades): ubicació on es concentren tots els recursos necessaris per al processament de la informació d'una organització.

Entorn: diferents àmbits (desenvolupament, integració, consolidació, preproducció, producció) corresponents a un servei.

Responsable del servei i/o l'aplicació: persona designada com a responsable d'un servei o aplicació.

Suport: dispositiu (cinta, disc, CD, DVD, etc.) on s'emmagatzema informació, ja sigui en format electrònic o en paper.

Referències i enllaços web

S'ha utilitzat com a referència en l'elaboració de l'actual guia:

GE-GUI40-01 Guia de còpies de seguretat, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

A la web 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] OnTrack Data Recovery

<http://www.ontrackdatarecovery.es>

[3] Associació Espanyola per a la direcció informàtica

<http://www.aedi.es>

Guia com fer backup del teu Mac, Appleismo mundo apple, divendres 29 d'Agost del 2008.

<http://www.appleismo.com/guia-como-hacer-backup-de-tu-mac/>

Guia pas a pas per la creació de còpies de seguretat i restauració de Serveis de directori lleuger d'Active Directory, Microsoft Technet, Agost del 2007.

<http://technet.microsoft.com/es-es/library/cc725665%28WS.10%29.aspx>

Desmuntant el mite: La recuperació remota i la recuperació de laboratori son iguals de fiables, OnTrack, Setembre del 2005.

[PDF]<http://www.ontrackdatarecovery.es/biblioteca/articulos/Ontrack%20Red%20Seguridad%20sept%2005.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/>

Eines per recuperació de dades

Advanced File Recovery

<http://advanced-file-recovery.com/>

Disk Doctors

<http://www.diskdoctors.net>

Recupera Data

<http://www.recuperadata.com>

Stellar

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



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat