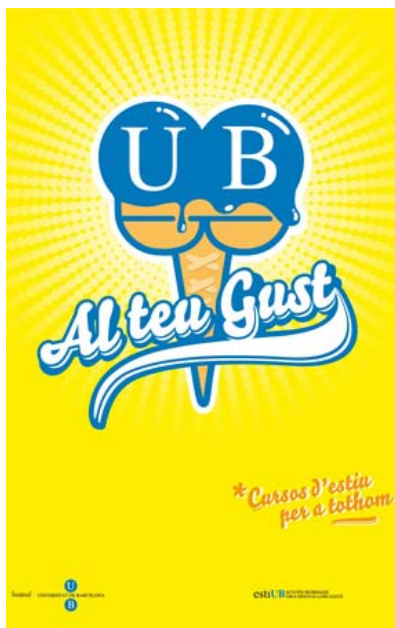


Destaquem... Xarxes socials. Autocontrol o descontrol de la privacitat a Internet?



Amb aquest títol i en el context dels cursos "Els Juliols Linguae", de la Universitat de Barcelona, l'Agència Catalana de Protecció de Dades dóna suport i coordina un curs que es celebrarà del 6 al 10 de juliol, a la UB. L'objecte d'aquesta activitat és tractar el fenomen de les xarxes socials, des de diferents punts de vista.

Els aspectes legals relacionats amb la protecció de les dades de caràcter personal i la intimitat s'abordaran en algunes de les sessions previstes, però també s'hi debatran aspectes de tipus sociològic, de globalització, de gestió de les identitats, sobre el màrqueting i la comunicació o la qüestió dels menors com a usuaris de les xarxes socials.

Els ponents de les diferents sessions provenen tant de l'àmbit acadèmic i de la recerca com del sector professional, amb perfils tècnics i jurídics, i analitzaran l'explosió de les xarxes socials des de diferents perspectives. Una eclosió que les autoritats de control de protecció de dades estan observant, per valorar quines poden ser les conseqüències de l'activitat que es desenvolupa en aquestes xarxes i aconsellar els usuaris la millor manera de preservar la seva privacitat.

Per a més informació:

<http://www.ub.edu/juliols/linguae/programacurs.php?CodiCurs=80>

Continguts

Destaquem...	1
Parlem de...	1
Vulnerabilitats de seguretat	2
Tecnologia i protecció de dades	3
Incidents de seguretat	4
Responsables de seguretat	5
Enllacem amb...	6
On anar...	6
Destrucció de documents en suport paper: preservar la confidencialitat fins al final de vida útil de la informació	8

Parlem de... la destrucció de paper

1. Alguns plantejaments inicials

En relació a la protecció de dades de caràcter personal, i amb caràcter general, la destrucció de documentació en suport paper té com a objectiu principal cancel·lar la informació que conté el paper i que ja no és necessària per a la finalitat per a la qual va ser recollida o tractada, de manera que resulti impossible tornar-ne a reproduir el contingut.

Dit això, cal matisar que la destrucció de paper també s'aplica quan el que en realitat ha esdevingut innecessari és el suport paper mateix (i no la informació). És a dir, quan el document ha estat generat com a còpia, aquesta ha deixat de ser necessària i la destrucció persegueix preservar la confidencialitat del contingut del document còpia que ja no és necessari.

+info



Revisió de vulnerabilitats de seguretat

El phishing s'estén per Twitter

En els darrers dies, molts usuaris de Twitter han rebut un missatge que els informa de nous seguidors dels seus comptes, en alguns casos fins a 1.000 seguidors. En realitat, es tracta d'un atac de pesca informàtica, un mètode habitual de frau a Internet que s'estrena així en el servei de microblogs.

Si l'usuari desitja visitar el perfil dels seus suposats seguidors clicant la direcció inclosa en el missatge, se l'envia a un fals Twitter, amb l'adreça *tvviter.com* (dues "v" en lloc de "w" i una "t" menys), on se li demanen les contrasenyes d'accés al servei veritable. Per augmentar les possibilitats d'engany, molts dels perfils dels suposats seguidors són dones atractives. Si el seguidor sent curiositat per saber-ne més, clica els enllaços en els seus perfils i llavors és enviat a una web de contactes, que podria ser l'origen de tot l'engany.

Les empreses espanyoles, entre les que gasten menys en seguretat informàtica

L'estudi anual de Panda Security situa les companyies espanyoles entre les més afectades pels virus informàtics (64%), només superades per la Xina. Espanya és un dels països del món on les empreses inverteixen menys en seguretat informàtica.

La companyia especialitzada en solucions de seguretat informàtica Panda Security ha presentat la primera edició del baròmetre internacional de seguretat a les PIME. L'estudi, que tindrà caràcter anual, pretén conèixer l'estat de la seguretat a les pimes de diferents països del món i avaluar l'impacte que té en l'economia l'allau de virus informàtics, enfocats al robatori econòmic i al frau en línia.

L'estudi s'ha fet entre el desembre de 2008 i l'abril de 2009, entre 7.000 empreses amb fins a 400 ordinadors, en diferents països del món.

Segons el director general de Panda Security Espanya, els ha sorprès gratament que el grau de conscienciació en seguretat de les companyies espanyoles estigui al nivell d'altres països tan tecnològicament madurs com els Estats Units. Tanmateix, el nivell d'infecció és molt alt, cosa que implica que no totes les companyies es protegeixen amb les solucions adequades i, com a conseqüència, es veuen afectades per la gran allau de nous virus que cada dia es generen.

Les cerques més perilloses

Els programadors de programari maliciós utilitzen cada vegada més els resultats d'alguns termes molt populars de cerca, per amagar els seus programes maliciosos. El *malware* adopta moltes formes i una de les més perilloses és ocultar-se darrere d'alguns termes de cerca molt populars.

La companyia de seguretat McAfee ha elaborat un estudi en què identifica les cerques més perilloses a la Xarxa, per al qual es van escollir 2.600 termes extrets de Google Zeitgeist, Yahoo! Buzz i altres fonts.

Segons l'estudi, la majoria de les recerques enverinades estan relacionades amb productes gratuïts, com música, lletres de cançons o fons d'escriptori. Altres cerques perilloses estan relacionades amb notícies de famosos, ofertes d'autoocupació o consells per estalviar diners.

A partir d'aquí, van establir un índex de perillositat de cada terme, d'acord amb la quantitat d'enllaços maliciosos relacionats amb cadascun. Segons el resultat, el major perill és darrere dels salvapantalles, ja que el 60% conté *malware*. Després apareixen les lletres de cançons, amb un 50% d'enllaços infectats. El podi de les cerques amb foc es completa amb les ofertes per treballar des de casa, amb un 40% d'enllaços que contenen programari maliciós.

A l'altre extrem, l'estudi descobreix alguns termes aparentment sospitosos, però amb índexs de perillositat baixos. Per exemple, la recerca de Viagra, un producte abundant en el correu brossa, és poc arriscada. Els sectors on les consultes són menys perilloses són els de salut i finances.



Tecnologia i protecció de dades

ASIMELEC edita una guia pràctica sobre protecció de dades per a persones grans

L'obtenció de dades personals de les persones grans és, actualment, una pràctica que va en augment en l'àmbit de la ciberdelinqüència. Mitjançant diversos procediments, com trucades enganyoses, pesca informàtica (*phishing*) o correus brossa. En molts casos, l'aïllament i la soledat del col·lectiu de gent gran, combinat amb altres factors propis de l'edat avançada, pot fer relativament fàcil la consecució del delictes.

La guia editada per ASIMELEC, titulada "*Aprenda a proteger sus datos*" i desenvolupada en col·laboració amb l'Agència Espanyola de Protecció de Dades, pretén prevenir i informar aquest col·lectiu, de forma senzilla i resumida, sobre els riscos que s'assumeixen en proporcionar dades sense prendre les precaucions necessàries. També vol informar-los dels seus drets, a l'hora de protegir les seves dades davant qualsevol entitat o organització que en faci un ús indegut.

ASIMELEC considera aquesta iniciativa realment innovadora i útil, sobretot per dues raons: la primera, que el col·lectiu de gent gran és un focus d'interès creixent per a cert tipus de delinqüència; la segona, que es tendeix a oblidar que cal fer accessibles, quan a la comprensió, normes i lleis que afecten directament els drets individuals de les persones. En aquest sentit, la guia pot ser perfectament vàlida per a la ciutadania en general.

La publicació està dividida en cinc parts fonamentals: un decàleg pràctic sobre la necessitat de ser caut a l'hora de proporcionar dades; un resum sobre els drets que assisteixen la persona afectada, si es fa un ús indegut de les dades; els drets relatius a la imatge; els riscos inherents en l'àmbit d'Internet i, finalment, una sèrie d'exemples pràctics de les situacions de risc més habituals.

https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_mayores_05_2009.pdf

LUMENSION reforça la protecció de les dades i la gestió de les vulnerabilitats

Lumension ha llançat la nova versió del seu paquet ofimàtic per a la protecció de dades i la gestió de vulnerabilitats, que incorpora les solucions de control d'aplicacions i dispositius, inventariat de vulnerabilitats i aplicació de pedaços informàtics.

Les principals aportacions són les capacitats de xifrat, l'expansió de la plataforma OS, capacitats d'informes més àmplies, major optimització de les bases de dades i suport a la virtualització.

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

El Defensor del Menor alerta a la televisió dels riscos de penjar imatges a Internet

El Defensor del Menor ha impulsat, en col·laboració amb l'Obra Social CajaMadrid, Telefónica i Telemadrid, un anunci a la televisió per fomentar la responsabilitat dels adolescents a l'hora de penjar imatges a Internet i a les xarxes socials, ja que, una vegada a la xarxa, tothom pot accedir-hi.

L'espot, que té com a lema "*Antes de colgar tu imagen en la red, piénsalo*", pretén conscienciar els més joves que publicar a Internet determinades fotografies o vídeos pot conduir a efectes no desitjats, ja que a la xarxa les imatges són de tothom i qualsevol pot utilitzar-les amb la finalitat que desitgi.

L'anunci s'emetrà de manera gratuïta durant un mes, en totes les franges horàries i en totes les seves durades diferents, de 30, 40 i 50 segons, de manera que hi haurà cinc anuncis diaris.

<http://www.europapress.es/epsocial/rsc/noticia-defensor-menor-madrid-alerta-riesgos-colgar-imagenes-internet-anuncio-television-20090609130144.html>



Incidents de seguretat relacionats amb dades personals

L'empresa T-Mobile nega haver estat víctima d'un atac informàtic (juny 2009)

Un pirata informàtic va publicar una llista de dades de clients de l'empresa T-Mobile en el lloc web *insecure.com*, on informava que havia entrat a la xarxa de l'empresa i havia robat les dades dels seus clients. També informava que havia intentat vendre la informació a d'altres empreses, que havien descartat l'adquisició. Arran d'aquesta negativa, publicava una mostra de les dades a Internet per si hi havia algú interessat a comprar-les.

T-Mobile ha volgut tranquil·litzar els seus clients i ha informat que les dades publicades pertanyien a un document intern de l'empresa, però que els sistemes que contenen les dades dels seus clients no han estat atacats.

De tota manera, l'empresa ha pres mesures per reforçar la seguretat dels seus sistemes i ha informat que, en cas que trobessin evidències que hi hagut informació de clients compromesa, n'informarien immediatament les persones afectades.

1 de cada 3 internautes admet que utilitza la mateixa contrasenya per a tots els llocs web (juny 2009)

Segons una enquesta feta per l'empresa de seguretat TI Sophos, el 33% dels internautes utilitza la mateixa contrasenya per a tots els seus accessos a diferents serveis web.

La companyia recomana la utilització de diferents contrasenyes per a cadascun dels accessos web que es tingui i, a més, que no siguin paraules que es puguin trobar en un diccionari, ni contrasenyes força comunes com ara "admin" o "1234".

Accés a la base de dades IBM DB2 sense autenticació (juny 2009)

Segons informa el web d'Hispacec Sistemas (www.hispasec.com), s'ha anunciat una vulnerabilitat a IBM DB2 segons la qual, en determinades circumstàncies, un usuari remot podrà connectar amb la base de dades sense autenticació.

Aquestes circumstàncies són que el sistema estigui configurat amb autenticació basada en LDAP, que el servidor LDAP permeti vincles (*binds*) anònims i que tingui la funcionalitat de cerca de grups mitjançant mòduls auxiliars LDAP de seguretat.

IBM ja ha corregit aquesta vulnerabilitat, a la versió 9.5 fixpak 4.



Secció responsables de seguretat

Nom i cognoms
Miguel Ángel Murillo Viñuales

Lloc que ocupa
Subdirector de Planificació i Serveis Informàtics

Des de quan
Juny de 1996

Entitat
Diputació de Barcelona

En quin àmbit desenvolupes la teva activitat com a responsable de seguretat?

La Diputació de Barcelona és una institució de govern local que actua directament prestant serveis i, sobretot, en cooperació amb els 311 ajuntaments de la província de Barcelona.

Aquesta característica fa que en l'àmbit del sistema d'informació, i en concret de la protecció de les dades, es presentin casos de fitxers que són cent per cent de la Diputació, com a organisme, i d'altres que són el vehicle per prestar serveis als ajuntaments, en els quals la Diputació actua com a encarregat del tractament. Efectivament, se'ns dona una casuística molt variada en aquest àmbit, que hem de resoldre tant des del punt de vista legal com tècnic.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

No. L'equip de persones que formem la Subdirecció som responsables tant de la planificació de les arquitectures dels sistemes d'informació de la Diputació com de la prestació dels serveis bàsics de sistemes, operació, xarxes i seguretat. I ens ocupem, també, de l'atenció als usuaris i del seu suport tècnic.

Quina és la principal dificultat que trobes per desenvolupar les funcions de responsable de seguretat?

Deixant de banda els aspectes més estàndard de seguretat informàtica en el sentit clàssic, relacionats amb la tècnica de sistemes i de l'operació ordinària, des del punt de vista de la Diputació de Barcelona el punt més delicat i complex és la varietat de casuístiques abans esmentades.

Tot i que els aspectes de seguretat informàtica poden ser semblants, des del punt de vista dels sistemes en explotació i de la gestió de les bases de dades, la formalització dels tractaments i l'assegurament de l'acompliment de la llei requereixen actuacions diferents, en el cas de gestió pròpia i en el de gestió per compte d'un tercer. Així mateix, la problemàtica se'ns complica encara més en el cas que s'incorpori una empresa externa per desenvolupar alguna tasca en aquest projecte comú.

Un altre aspecte a modular consisteix a trobar el punt d'equilibri entre el pànic que pot produir en els clients dels sistemes d'informació el seu primer contacte amb la llei, a causa dels requisits no sempre coneguts que exigeix, i l'excés de deixadesa en matèria de seguretat que, de vegades, et pots trobar en els plantejament dels projectes. Hem de treballar en els sistemes d'informació i hem de complir la llei. Totes dues coses són perfectament compatibles i imprescindibles.

En relació a la protecció de dades, quina responsabilitat et requereix més dedicació?

El fet d'articular mesures de seguretat en els sistemes d'informació ha estat una feina clàssica dins dels departaments d'informàtica. Per tant, l'acompliment de la llei no implica més que una formalització que pot ser una mica diferent, però que no modifica substancialment aquesta funció.

En aquest sentit, el suport i la difusió de les obligacions que marca la llei als usuaris promotors de nous projectes és la part que requereix més dedicació, tant del responsable de seguretat com de les persones que actuen com a suport tècnic o jurídic en la nostra organització.

Per tal d'articular aquest suport, la Diputació de Barcelona va crear, ja fa uns anys, el Comitè Directiu de Protecció de Dades, format per directius de l'àmbit tècnic, organitzatiu i



jurídica. Recentment, la capacitat de suport s'ha reforçat notablement amb la creació de la figura del responsable corporatiu de Protecció de Dades, que és la persona que coordina totes les tasques derivades de suport, difusió de polítiques corporatives i interlocució entre els diferents serveis de la nostra organització i que, a més, és la secretària del Comitè.

Mantens contacte amb l'APDCAT per resoldre qüestions o plantejar dubtes que et puguin sorgir en el dia a dia?

Per descomptat, encara que no sigui amb un contacte directe. Actualment, tota la relació amb l'APDCAT la vehiculem a través de la responsable corporativa de Protecció de Dades, que és qui s'encarrega de plantejar totes les nostres qüestions o dubtes amb l'APDCAT.

Per a nosaltres és fonamental mantenir un contacte fluid i continu amb l'Agència, per aclarir dubtes i col·laborar-hi no només en els problemes del dia a dia, sinó també en aspectes de caire més estratègic i general.

Enllacem amb...

<http://www.iso27000.es/>

Aquest enllaç proporciona informació d'utilitat, especialment per als qui s'hagin d'enfrontar per primera vegada a qüestions relacionades amb la ISO27000 i, en general, amb els processos d'implantació de sistemes de gestió de la seguretat de la informació (SGSI). Però és, alhora, un recurs útil per als qui ja tenen coneixements en aquesta matèria i busquen informació especialitzada i de detall.

De forma senzilla, en aquest lloc web s'aborden aspectes relacionats amb els SGSI, les ISO27000, altres estàndards vinculats a la seguretat de la informació i qüestions relacionades amb la certificació en normes. Hi ha, també, una llista útil d'enllaços a altres pàgines d'interès, o a pàgines que contenen eines que convé conèixer quan es treballa en aquest àmbit.

Finalment, s'hi pot consultar la secció de novetats i l'apartat de preguntes més freqüents, juntament amb un glossari.

6

On anar...

Congressos i esdeveniments

Workshop on RFID Security 2009 (RFIDsec09)

De l'1 al 3 de juliol de 2009. Leuven (Bèlgica)
<http://www.cosic.esat.kuleuven.be/rfidsec09/>

14th IEEE Symposium on Computers and Communications

Del 5 al 8 de juliol de 2009. Sousse (Tunísia)
<http://www.comsoc.org/iscc/2009/>

Redes sociales. Autoncontrol o descontrol de la privacidad en Internet?

Del 6 al 10 de juliol de 2009. *Els juliols linguae*. Universitat de Barcelona (UB)
<http://www.ub.edu/juliols/linguae>

XV Jornadas de Enseñanza Universitaria de la Informática JENUI 2009

Del 8 al 10 de juliol de 2009. Barcelona
<http://jenui2009.fib.upc.edu/>

Curs sobre seguretat de la informació

Del 8 al 10 de juliol de 2009. Universitat de Salamanca
<http://www.informatica64.com/CursoDeVeranoSalamanca/>

Conferència "Defensa de reputació a Internet"

9 de juliol de 2009. Il·lustre Col·legi d'Advocats de Barcelona
<http://www.icab.es/?go=d7f092babe5a485eb8cdde0eba01701dc3fc17faa049c5d0a2d14facb22f06a88a6bef22e382a2d792b22b52fe6f1dd1a15ac3fd225914b1>

23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security

Del 12 al 15 de juliol de 2009. Montreal (Canadà)
<http://www.ciise.concordia.ca/newsandevents/2009/dbsec09/>

International Conference on Security and Management SAM '09

Del 13 al 16 de juliol de 2009. Las Vegas (EUA)
<http://www.world-academy-of-science.org/worldcomp09/ws/conferences/sam09>

International Conference on Information Security and Privacy (ISP-09)

Del 13 al 16 de juliol de 2009. Orlando (EUA)
<http://www.promotersearch.org/>

The fifth Symposium on Usable Privacy and Security

Del 15 al 17 de juliol de 2009. Mountain View, Califòrnia (EUA)
<http://cups.cs.cmu.edu/soups/2009/>

**Summer school on Cryptography**

Del 3 al 7 d'agost de 2009. Bonn (Alemanya)

<http://cosec.bit.uni-bonn.de/students/events/cryptabit2009/>**Joint Workshop on Information Security (JWIS2009)**

6 i 7 d'agost de 2009. Kaohsiung (Taiwan)

<http://jwis2009.nsysu.edu.tw/index.php/jwis/jwis2009>**11th Annual NEbraskaCERT Conference**

18 i 19 d'agost de 2009. Omaha, Nebraska (EUA)

<http://www.certconf.org/>**2009 IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT'09)**

Del 29 al 31 d'agost de 2009. Vancouver (Canadà)

<http://cse.stfx.ca/~passat09/>**Workshop in Information Security Theory and Practices**

De l'1 al 4 de setembre de 2009. Brussel·les (Bèlgica)

<http://www.wistp.org/index.php>**International Symposium: Recent Developments in Cryptography and Information Sec (CryptoBG*2009)**

Del 3 al 5 de setembre de 2009. Oriahovitza (Bulgària)

<http://www.cryptobg.org/>**Curs de Protecció de Dades a les Administracions Públiques**

Del 14 al 16 de setembre de 2009. Universitat Internacional Menéndez Pelayo (UIMP). València

http://www.uimp.es/uimp/home/homeUIMPdina.php?jci=AC_ADEMICAS_FICHA&juj=2003&jpi=IdActividad=7970306&pq=1&orden=6**VI Conference on Broadband Communications, Networks and Systems**

Del 14 al 17 de setembre de 2009. Madrid

<http://www.broadnets.org/>**Workshop on Computational Intelligence for Security in Information Systems CISIS 09**

Del 23 al 26 de setembre de 2009. Burgos

<http://qicap.ubu.es/cisis2009/>**Fourth International Workshop on Data Privacy Management DPM 2009**

24 i 25 de setembre de 2009. Saint Malo (França)

<http://dpm09.dyndns.org/>**IEEE 9th International Conference on Computer and Information Technology**

De l'11 al 14 d'octubre de 2009

<http://grid.hust.edu.cn/CIT2009/>**Cursos seguretat TIC 2009**

Centre Criptològic Nacional (CCN-Cert)

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2140&Itemid=188&lang=es

Neix l'Associació Professional Espanyola de Privacitat

El dia 4 de juny de 2009, es va celebrar a la Facultat de Dret de la Universitat Complutense de Madrid l'Assemblea Constituent de l'Associació Professional Espanyola de Privacitat (APEP).

Aquesta Associació integra els professionals de la privacitat i la protecció de dades de caràcter personal i pretén, entre d'altres objectius, fomentar i difondre els drets fonamentals a la intimitat personal i a la pròpia imatge, amb l'organització d'activitats de conscienciació sobre la privacitat dels ciutadans.



Destrucció de documents en suport paper: preservar la confidencialitat fins al final de vida útil de la informació

«...la transformació del paper ha d'impedir que la informació pugui ser recuperada amb posterioritat.»

Del que parlem, però, és més aviat de transformació. La clau és que la manipulació que dona lloc a la transformació del paper ha d'impedir que la informació es pugui recuperar posteriorment. Aquí podríem fer referència al que es coneix com a *lleï de Lomonosov-Lavoisier*, principi químic pel qual «la matèria ni es crea ni es destrueix, només es transforma».

En relació a la destrucció/transformació del paper, podem distingir dues tipologies d'ús: d'una banda, el que podríem anomenar «*paper original*», quan el document en paper és l'origen de la informació; i d'altra banda, el que anomenarem «*paper còpia*», que és la reproducció d'un «*paper original*» (fotocòpia o transmissió per fax), o bé la impressió d'un document en suport paper (impressió de llistats o documents).

La introducció de les tecnologies de la informació i la comunicació en els processos de gestió de la informació certament ha reduït, i seguirà reduint considerablement, l'ús del «*paper original*». Però, al mateix temps, la facilitat i la reducció de costos dels sistemes tècnics de reproducció i impressió (fotocòpies i impressores) han provocat un considerable augment del «*paper còpia*». Per tant, paradoxalment i malgrat la tendència cap a un model *paperless*, en l'actualitat la gestió de la informació en suport paper és una realitat que genera problemes i que reclama atenció i la dedicació de molts recursos materials i humans.

Segons les conclusions d'un estudi de Landwell i PricewaterhouseCoopers, que durant el 2006 va plantejar a 610 empreses un qüestionari amb preguntes relacionades amb la gestió del paper («*Datos en Papel* Tratamiento de datos personales e información confidencial en soporte papel en la empresa española*»):

- Només el 37% de les empreses disposen de normes de seguretat específiques per protegir les dades de caràcter personal en suport paper.
- La majoria no classifiquen la informació, de manera que no poden conèixer de forma detallada quins dels documents que gestionen contenen dades personals. Només un 27% disposa de metodologies de classificació i emmagatzemament dels documents en paper.
- En relació a la destrucció del paper, només el 33% considera el paper com a informació confidencial i ho té en compte a l'hora de definir o executar els processos de destrucció.

«...mesures de seguretat aplicables als fitxers i tractaments no automatitzats...»

El Reial decret 1720/2007, que aprova el Reglament de desenvolupament de la LOPD, regula els objectius de control a què han de donar resposta les mesures de seguretat aplicables als fitxers i tractaments no automatitzats, i que en definitiva han d'evitar l'alteració, pèrdua, tractament i accés no autoritzat als documents en suport paper. En el títol VIII, regula de forma directa aspectes relacionats amb els controls de destrucció de documents en suport paper (art. 83, 87.2, 92.4 i 112.2).

2. Un problema real

La primera conseqüència d'una mala aplicació o de la inexistència d'una política de destrucció de la documentació en suport paper és que afecta la confidencialitat de la informació. Habitualment, el



« ... llencen a les papereres documents amb dades personals i sense destruir o dipositen documents confidencials en contenidors destinats al reciclatge de paper ...»

« ... prendre consciència dels incidents que es produeixen al voltant de la mala gestió del paper ...»

problema és que volums més o menys importants de documents queden a disposició de tercers, no legítimats per accedir a les informacions que contenen. Sovint, es tracta de negligències d'empleats, que llencen a les papereres documents amb dades personals i sense destruir o dipositen documents confidencials en contenidors destinats al reciclatge de paper, sense cap destrucció prèvia.

En el cas Enron, l'FBI va recuperar milers de documents que es van intentar fer desaparèixer mitjançant destructores de paper, però que posteriorment es van recuperar i processar per ser analitzats. És més complex el cas de la recuperació de documentació de l'ambaixada dels Estats Units a Teheran (després de la revolució d'Iran de 1979), en què es van utilitzar teixidors iranians locals de la catifa per recuperar documentació prèviament destruïda.

Fins i tot si es volen aplicar procediments segurs de destrucció del paper, poden sorgir problemes logístics i de manipulació, especialment quan es tracta de grans volums de paper, com el cas de la NSA (Agència de Seguretat Nacional, EUA). A mitjans dels noranta, aquesta agència havia de destruir una mitjana de quasi 30 tones de documents secrets cada dia; aquest volum no es podia gestionar amb destructores tradicionals, ni tan sols amb empreses especialitzades, així que la NSA va encarregar una destructora a mida.

Es tractava d'una incineradora que podia destruir fins a 6 tones de paper per hora, però a l'hora de fer-la servir va resultar que la pasta generada per la incineració impedia que la màquina treballés amb normalitat (menys de 60 dies de funcionament, durant el quasi any i mig que es va intentar utilitzar-la). Al final, la solució va ser un sistema basat en aigua, vapor i productes químics, que generava una polpa de paper reciclable per fabricar caixes de pizzes, cosa que fins i tot va reportar beneficis econòmics a la NSA.

Però no cal recórrer a situacions tan extremes per prendre consciència dels incidents que es produeixen al voltant de la mala gestió del paper. Alguns titulars de premsa com aquests són habituals:

Un mendigo encuentra en la basura planos confidenciales de la 'zona cero'
Font: ELPAÍS.com - Madrid - 18/04/2008

Coalición Canaria halla documentos oficiales en la basura
Font: El dia.es - 02/06/2007

Investigan la aparición en contenedores de documentación privada de las reclusas de la cárcel de Wad-Ras de Barcelona
Font: Europa Press - 02/02/2006

Firmas de policías y direcciones particulares acaban en plena calle en Palma de Mallorca
Font: Europa Press - Palma de Mallorca - 02/01/2005

Aparecen en la vía pública cientos de partes médicos de niños asistidos en el Hospital Materno-Infantil de Málaga
Font: Diario de Navarra - 17/12/2004

Hallados entre la basura mapas y documentos del Ejército de EEUU
Font: El Mundo - 13/07/2004

Hallan tirados documentos confidenciales del Inem sobre miles de parados
Font: El Mundo - 14/12/2003

Encontrados en la basura 7.000 partes médicos confidenciales de un centro de salud de Málaga
Font: El Mundo - 29/06/2002



Relacionats amb l'aparició de documents a les escombraries hi ha els conceptes de *dumpster diving* (bussejar a les escombraries) o *garbology* (analitzar la brossa).

Les conseqüències no tenen a veure únicament amb la pèrdua de confidencialitat de les dades. A l'hora d'abordar la problemàtica de la destrucció del paper, també s'han de considerar qüestions com l'espionatge industrial o empresarial o el robatori d'identitats.

«... solucions
tècniques i
organitzatives i,
en el cas que ens
ocupa, amb
especial
incidència en la
sensibilització
de les persones
de
l'organització.»

3. Com abordar el problema

Com sempre, les qüestions vinculades a la seguretat de la informació s'han d'enfocar amb solucions tècniques i organitzatives i, en el cas que ens ocupa, amb especial incidència en la sensibilització de les persones de l'organització. Per descomptat, sempre des d'una anàlisi global i integrada de totes les normes i mecanismes de seguretat que s'apliquen a la gestió de la informació i, de manera destacada, amb un rol clau dels perfils professionals dedicats a la gestió documental i l'arxivística.

a) Classificació dels documents: aquest és el primer pas

Per a una classificació eficaç de la documentació, cal tenir en compte 4 dimensions:

1. La sensibilitat de les dades: aquí hi entrarien la confidencialitat, la disponibilitat, l'accés, etc.
2. La determinació dels períodes legals o procedimentals de retenció de la informació.
3. Els tipus d'arxius pels quals passa la documentació al llarg del seu cicle de vida.
4. I el volum de documents i l'espai físic que ocupen, i la previsió de creixement del volum de documentació arxivada.

b) Anàlisi dels documents: una vegada agrupats els documents segons els criteris de classificació utilitzats, cal analitzar-ne amb detall les característiques, quins estan afectats per normes i de quina manera ho estan:

1. Identificació dels documents i de les sèries de documents: continguts i dades contextuals
2. Normes legals de tipus general, sectorial o corporatives que puguin afectar cada document
3. Identificació de bones pràctiques o estàndards de destrucció que puguin ser d'aplicació

c) Disseny de la política de destrucció de paper, que en tot cas ha d'incloure:

1. Quadres de classificació
2. Calendaris de retenció
3. Política global de destrucció del paper

d) Implantació del que preveu la política de destrucció:

1. Elaborar les normes d'aplicació a la destrucció de paper, tenint en compte si es tracta de «*paper original*» o «*paper còpia*» i si són susceptibles de reciclatge o no.
2. Donar a conèixer al personal implicat les seves obligacions respecte de la destrucció del paper.
3. Implantar els elements tècnics interns: fonamentalment les destructores de paper, ja sigui en zones comunes o de tipus individual. Aquí caldrà tenir en compte el nivell de destrucció de paper requerit i, per tant, verificar quin nivell compleixen les destructores, d'acord amb la norma DIN 32757 (estableix 5 nivells de destrucció de la documentació, en què cada nivell superior implica una transformació del paper en partícules més petites).
4. La destrucció de grans volums de documents requerirà la col·laboració de terceres empreses. Cal definir perfectament les obligacions i els mecanismes de verificació de la destrucció que



s'encarregui externament. Igualment, quan es tracti de serveis de reciclatge les mesures han d'incloure tant el procés de destrucció com les qüestions relacionades amb el transport i emmagatzemament dels documents a reciclar, fins a la seva destrucció.

- e) Auditoria: per últim, cal articular mecanismes de verificació del compliment del que preveuen els procediments i normes de destrucció, tant si són interns com externs. Això ha d'incloure verificar, amb una certa periodicitat, el contingut de les papereres personals i dels contenidors de paper comuns.

4. Legislació, normes i referències

- a) **Legislació:** a banda de la legislació estatal vigent en matèria de protecció de dades de caràcter personal, hi ha la següent.

- *Decret 914/1969, de creació de l'Arxiu General de l'Administració Civil*
- *Llei 16/1985, de 25 de juny, del patrimoni històric espanyol*
- *Llei 10/2001, de 13 de juliol, d'arxius i documents*
- *Reial decret 937/2003, de 18 de juliol, de modernització dels arxius judicials*
- *Reial decret 2598/1998, de 4 de desembre, pel qual s'aprova el reglament d'arxius militars*
- *Decisió núm.1600/2002/CE del Parlament Europeu i del Consell, de 22 de juliol de 2002, per la qual s'estableix el sisè Programa d'acció comunitari en matèria de medi ambient*
- *Llei 10/1998, de 21 de abril, de residus*
- *Reial decret 1164/2002, de 8 de novembre, pel qual es regula la conservació del patrimoni documental amb valor històric, el control de l'eliminació d'altres documents de l'Administració General de l'Estat i els seus organismes públics i la conservació dels documents administratius en suport diferent a l'original*
- *El Health Insurance Portability and Accountability Act (HIPAA), de 1996, que requereix que totes les entitats de salut i assistencials siguin responsables de l'emmagatzemament i rebuig de la informació dels pacients*
- *El Gramm-Leach-Bliley Act, de 2000, que requereix que les institucions bancàries i financeres protegeixin la seguretat i confidencialitat dels documents i de la informació del consumidor*
- *El US Economic and Espionage Act, de 1996, diu que les organitzacions han de prendre les mesures necessàries per mantenir segura la informació comercial secreta.*
- *FACTA (2005): és una llei federal per reduir el risc de frau i robatori de la identitat causada pel rebuig incorrecte d'informacions dels consumidors. La FACTA obliga a destruir la informació dels clients abans de llençar-la*

- b) **Algunes normes, estàndards, guies i bones pràctiques**

- *Norma DIN 32757 de 1985 (Deutsches Institut für Normung – Institut Alemany de Normalització).*

Aquesta norma, aplicable a maquinària de destrucció de paper, defineix 5 nivells de seguretat per a la destrucció d'arxius. El nivell de seguretat el defineix la mida de la partícula triturada.

- *Physicians & Security of Personal Information. June 2006*
Comissonat per a Informació i Privacitat de la Colúmbia Britànica
<http://www.oipc.bc.ca>.



- *Faxing and emailing personal information. February 2005*
Comissonat per a Informació i Privacitat de la Colúmbia Britànica
[http://www.oipc.bc.ca/pdfs/public/fax-emailguidelines\(Feb2005\).pdf](http://www.oipc.bc.ca/pdfs/public/fax-emailguidelines(Feb2005).pdf)
 - *Criterios generales para la valoración de documentos de la Administración General del Estado.*
Document aprovat per la Comissió Superior Qualificadora de Documents Administratius, en sessió de 27 de novembre de 2003
 - *National Archives and Records Administration's approved changes to information and life cycle management manual, COMDTINST M5212.12A*
Les normatives NARA (Arxius Nacionals i Administració de Documents dels Estats Units) requereixen que les agències implementin i actualitzin els programes aprovats per l'Arxiu Nacional dels Estats Units
 - *Guide Privacy Requirements and Policies for Health Practitioners*
Publicada pel Col·legi de Quiropràctics d'Ontàrio, novembre 2003
 - *Acuerdo del Consejo General del Instituto Federal Electoral, por el que se emiten criterios para la destrucción de los paquetes electorales que contienen la documentación electoral de las elecciones federales extraordinarias, celebradas en los distritos electorales federales uninominales 06 del Estado de Coahuila i 06 del Estado de Michoacán*
Estados Unidos Mexicanos.- Instituto Federal Electoral.- Consejo General - CG149/2004
 - *Criterios de seguridad, normalización y conservación, 24 de junio de 2004*
Consell Superior d'Informàtica i per a l'Impuls de l'Administració Electrònica
 - *Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas*
 - *Aclaración sobre la aplicación del Reglamento de Seguridad a los ficheros en soporte no automatizado*
Agència Espanyola de Protecció de Dades
<https://www.agpd.es/index.php?idSeccion=162>
 - *Manual de tratamiento de archivos administrativos*
Ministeri de Cultura, 1992
Normes tècniques de la Direcció d'Arxius Estatals
- c) Articles i altres referències**
- Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*
James Bamford, 2002
- Tome control: Defiéndase contra el robo de identidad*
Federal Trade Commission, FTC
- Los riesgos de la basura informática*
M^a Goretti López Deltell. Consultora de l'Agència de Protecció de Dades de la Comunitat de Madrid



Battling Big Business: Countering Greenwash, Front Groups and Other Forms of Corporate Deception

Eveline Lubbers, 2002

La importancia de destruir correctamente la documentación en papel

Isidro Gómez-Juárez Sidera. Doctor en Dret de les Noves Tecnologies de la Informació i les Comunicacions i membre del Servei Jurídic de la Comissió de Llibertats i Informàtica (CLI)

Datos en Papel Tratamiento de datos personales e información confidencial en soporte papel en la empresa española*

Landwell i PricewaterhouseCoopers, 2006

Ramon Miralles.
Coordinador
d'Auditoria i
Seguretat de la
Informació.
APDCAT

<http://www.arxivers.com/cat/default.asp>

<http://www.paper-shredder-info.com/>

<http://www.safetydoc.es/>

<http://www.consumer.gov/idtheft>

<http://www.identitytheft.org>

<http://www.theshreddingplace.com>