

Destaquem... Ultimàtum a Facebook

Per Esther Mitjans, directora de l'APDCAT. Publicat v. castellà a *La Vanguardia* de 13 d'agost de 2009



El Canadà és el primer país que amenaça Facebook de portar-lo als tribunals per violació de la seva llei de protecció de dades personals.

Segons la comissària de Privacitat del Canadà, Jennifer Stoddart, Facebook ha de resoldre en 30 dies aspectes que fan referència a com es recullen, es distribueixen i es guarden les dades personals dels seus usuaris. També demana més transparència sobre què passa quan un usuari es dona de baixa. Quant de temps ha de passar abans que la seva informació personal no desaparegui de les bases de dades de Facebook? D'altra banda, vol que s'aclareixin els motius pels quals es mantenen els perfils dels usuaris difunts i censura que les persones que demanen la baixa puguin ser identificades indefinidament, cosa que també passa amb les adreces electròniques de les persones que només són convidades a registrar-s'hi.

L'autoritat canadenca creu que aquesta xarxa social ha de conscienciar els usuaris dels riscos d'etiquetar terceres persones, i insta les persones que es registrin a llegir les condicions d'ús i a activar les opcions de màxima privacitat. Segons la comissària, falten mecanismes que evitin l'accés no autoritzat a dades personals de tercers pels qui, sense ser Facebook, desenvolupen aplicacions en la seva plataforma, com els creadors de jocs, horòscops i qüestionaris.

Les xarxes socials poden assumir el risc jurídic de no complir totes les legislacions nacionals, però han de tenir en compte les dels països que, com el Canadà, poden portar-los als tribunals. La ferma posició canadenca ha estat el detonant perquè autoritats de protecció de dades d'altres països, com Espanya, reforcin la seva pressió sobre Facebook per tal que els usuaris determinin el grau de privacitat de les seves dades. Facebook al·lega que altres companyies no s'han preocupat tant per la privacitat, tot i que està disposada a treballar-hi. L'Agència Catalana de Protecció de Dades insisteix que la privacitat ha d'estar prevista en el disseny de tot servei o aplicació, i que no pot ser només un afegitó en la presentació final. L'agència ha difós uns manuals perquè els joves sàpiguen gestionar els seus propis riscos en les xarxes socials. És hora que Facebook ordeni que aplicacions, com ara jocs i tests, que s'ofereixen en la seva plataforma, introdueixin elements de privacitat des del moment del seu disseny.

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...	7
Control de la destrucció dels documents a Catalunya	8

Parlem... del control de la destrucció dels documents a Catalunya

Per al número d'aquest mes, comptem amb una col·laboració externa a l'Agència, que complementa l'article publicat al butlletí núm. 4 del passat mes de juny que, des d'un vessant tecnològic i amb una orientació divulgativa, parlava de la problemàtica de la destrucció del paper. Aquest nou article tracta de manera profunda i concreta del control de la destrucció dels documents a Catalunya, centrada en el sector públic. Aprofitem l'ocasió per animar els nostres lectors a fer-nos arribar les seves col·laboracions, ja que el +Kdades vol generar debat i visions complementàries en el context de la protecció de dades i la tecnologia.

+info



Revisió de vulnerabilitats de seguretat

Microsoft confirma un zero day a IIS

Microsoft ha advertit d'un nou "zero, vulnerabilitat de dia" en els seus serveis d'Internet Information Server (IIS), que podria permetre als pirates informàtics l'execució remota de codi. D'acord amb les últimes xifres, IIS és el segon servidor web més popular del món, després d'Apache.

La companyia ha emès un avís de seguretat per a la vulnerabilitat, que és en el File Transfer Protocol (FTP) a IIS 5.0, 5.1 i 6.0 i ha dit que, tot i que el codi s'ha publicat àmpliament a Internet, l'empresa no està al corrent d'atacs actius que utilitzin aquest codi d'explotació o que, en aquest moment, hi hagi hagut impacte sobre els usuaris.

Segons Microsoft, "la vulnerabilitat és un desbordament de pila en el servei FTP en enumerar una llarga llista de directoris especialment dissenyats". Si un atac arribés a explotar correctament aquesta vulnerabilitat, podria executar codi en el context de LocalSystem, en el procés en què s'executa el servei FTP.

Microsoft aconsella les empreses d'evitar que els usuaris que no són de confiança tinguin accés d'escriptura al servei de FTP, fins que estigui disponible una actualització de seguretat totalment provada. Això es pot aconseguir sense aturar el servei FTP, si no és necessari, o evitar l'escriptura als usuaris anònims a través de la configuració de l'IIS.

Els troians segueixen dominant les deteccions d'amenaces

Un virus de categoria "troia de descàrrega" segueix dominant les estadístiques de programari maliciós, amb l'explotació de l'autorun.inf i funcions de Delphi.

Les estadístiques del proveïdor de programari global de programari de seguretat ESET mostren que, a l'agost, el cuc "Conficker" era l'amenaça més generalitzada a nivell mundial, amb una quota del 8,56%. Respecte de les estadístiques del mes de juliol, però, això suposa un lleuger descens del 2% de mitjana. Tot i això, l'estudi ha detectat que hi ha una barreja d'amenaces que ha assolit una posició forta a nivell mundial, sobretot els troians de jocs en línia i l'explotació de la funció d'autorun.inf.

Les estadístiques del laboratori SunbeltLabs van informar que l'amenaça per robar contrasenyes fent servir "Trojan-Spy.Win32.Zbot.gen" s'han mantingut el primer lloc en la llista. El segon més detectat va ser "Trojan.Win32.Generic!BT", un descarregador de programes de seguretat falsos, que no apareixia a la llista al mes de juliol però que va ser la segona amenaça més alta.

SunbeltLabs també va indicar la incidència del virus de "Win32.induc", que va ser molt publicitada a l'agost, per la seva propagació a través d'aplicacions de desenvolupament de Delphi.

Michael St Neitzel, vicepresident de recerca d'amenaces i de tecnologies de Sunbelt Software, va dir: "El fet que Zbot sigui l'índex de detecció superior dels dos últims mesos no és sorprenent. És una peça molt versàtil de codi maliciós, que injecta el seu codi des d'un lloc remot per robar la informació de les seves víctimes, incloses les contrasenyes en memòria cau, les credencials d'inici de sessió per a llocs web (principalment bancs), així com les dades en els certificats i les galetes."

El troia té algunes funcionalitats de porta del darrere i pot registrar pulsacions de tecles.

En primer lloc, es va notar un augment d'aquest virus a mitjans de maig, quan es va distribuir a través d'una sèrie de campanyes de correu brossa.

En un dels casos, el missatge de correu brossa pretenia ser una línia aèria e-ticket, i en d'altres una suposada notificació per al pagament electrònic d'una comanda a Amazon.com. Sunbelt ha documentat més de 2.700 arxius relacionats amb "Trojan-Spy.Win32.Zbot.gen", des que es va detectar per primera vegada.



Tecnologia i protecció de dades

Nova eina de Google per recuperar informació personal

Google acaba d'incloure en els seus serveis web una eina perquè els usuaris recuperin la seva informació personal penjada a Internet i en puguin esborrar la part en línia, si ho volen. La funció és a cadascun dels serveis de la companyia del buscador, com ara el correu, l'editor de fotos, el Google Docs o les aplicacions de publicitat.

Aquesta funcionalitat és simple en els casos en què es permet la descàrrega de documents i fotografies, però no en eines com ara el Gmail o el Blogger. En aquests casos, la nova funcionalitat descarrega els correus en un altre compte o, en el cas dels blocs, els trasllada a una altra plataforma.

http://www.elperiodico.com/default.asp?idpublicacio_PK=46&idioma=CAS&idtipusrecurs_PK=7&idnoticia_PK=644885

Facebook canvia les seves polítiques de privacitat a petició del Canadà

Com a resultat de les seves negociacions amb la comissària canadenca de privacitat, Jennifer Stoddart, Facebook ha acceptat fer canvis en la seva plataforma per protegir millor la informació personal dels seus usuaris de tot el món.

La xarxa social ha accedit a modificar els processos de baixa del compte i gestionar la informació dels seus membres d'una forma més transparent, després que la comissària declarés que la política de Facebook de mantenir la informació personal de les persones que havien tancat el seu compte violava les lleis canadenques de privacitat.

Els canvis donaran als usuaris més transparència i control sobre la informació que ofereixen als creadors d'aplicacions, com ara jocs i qüestionaris. Per la seva banda, Facebook també aclarirà als usuaris que tenen l'opció d'eliminar el seu compte, i no només de desactivar-lo. A més, la informació dels no usuaris estarà més ben protegida.

La comissària canadenca considera que la resposta de la

companyia és acceptable, ja que permet als usuaris prendre decisions i estar informats sobre com es tracta la seva informació personal.

http://www.lanacion.com.ar/nota.asp?nota_id=1167591

La Comissió Europea fixa els requisits de privacitat per a les etiquetes RFID

La Comissió Europea (CE) ha establert un codi de conducta per a les empreses que utilitzen etiquetes d'identificació per radiofreqüència (RFID), a fi de salvaguardar la privacitat dels ciutadans i promoure el ràpid desplegament d'aquesta tecnologia.

Aquest codi de conducta, que adopta la forma de recomanació formal per als governs nacionals i que ha estat molt ben rebut per la indústria, està dissenyat per alliberar els usuaris del temor que les noves etiquetes es puguin utilitzar per rastrejar els moviments dels ciutadans o comprometre la seguretat de les seves dades. Bàsicament, els principis d'aquest codi són quatre:

1. En primer lloc, el xip dins el producte RFID s'ha de desactivar automàticament en el punt de venda, tret que el comprador manifesti expressament que vol que romangui actiu. El text no especifica què s'ha de fer amb les etiquetes RFID, un cop desactivades.
2. En segon lloc, el document estableix que seria desitjable que les empreses o autoritats públiques que utilitzin xips intel·ligents proporcionessin als consumidors informació simple i clara, per tal que entenguin que les seves dades personals poden ser utilitzades, quin és el tipus de dades recopilades (nom, adreça o data de naixement) i amb quin propòsit.
3. En aquest punt, la CE aconsella a les associacions i organitzacions de distribuïdors que avisin els usuaris sobre els productes que tenen targetes intel·ligents, mitjançant un símbol comú que indiqui quan un article utilitza aquesta tecnologia.
4. Per últim, el codi suggereix a les empreses i administracions públiques que avaluin l'impacte sobre la protecció de dades i la privacitat abans d'utilitzar els xips RFID.

Revista SIC, núm. 86, setembre 2009



Incidents de seguretat relacionats amb dades personals

Detenen a Alacant un pirata que va robar vídeos i fotos íntimes de 200 dones (agost 2009)

La Policia Nacional ha detingut a Alacant un presumpte *hacker* i el seu còmplice. Se'ls acusa de tenir en els seus ordinadors més de 200 comptes de correu electrònic de dones i unes 300 carpetes amb arxius de fotografia i vídeo íntims, sense que les seves víctimes estiguessin al corrent de la captació d'aquestes imatges i dades personals.

La Brigada Provincial de la Policia Judicial, Grup de Delictes Tecnològics, va iniciar les investigacions a partir d'una denúncia que va presentar una persona que assegurava que uns desconeguts havien accedit al seu ordinador, mitjançant un troià. Després, utilitzant la seva identitat i la seva adreça de correu electrònic, havien enviat missatges de correu electrònic molestos i desagradables a la seva parella, amb la intenció de fer-li pensar que l'havia enganyat amb una altra dona.

Als detinguts se'ls acusa de delictes contra l'honor, la intimitat personal i la pròpia imatge, així com de delictes d'usurpació de l'estat civil.

Font: www.laflecha.net

Es troben informes de pacients en els edificis en ruïnes de l'Hospital Psiquiàtric de Toén (Galícia) (setembre 2009)

Durant la recerca d'una noia desapareguda a les muntanyes de Toén, es van descobrir als soterranis de l'antic edifici administratiu de l'Hospital Psiquiàtric milers de documents abandonats referents a expedients de pacients, factures i llibres de comptes. En els informes psiquiàtrics trobats hi apareixen dades de pacients dels anys 70.

Xategen amb les seves víctimes per recol·lectar les seves dades (setembre 2009)

Fent-se passar per un banc legítim, aquests delinqüents envien missatges de correu electrònic als usuaris demanant que visitin el lloc web del banc per confirmar les seves dades.

Quan els usuaris entren a la pàgina web del banc i escriuen les seves dades d'accés al seu compte bancari, o bé cliquen qualsevol enllaç del lloc, s'obre una finestra de xat i l'estafador comença a xatejar amb la víctima, per obtenir-ne més informació personal. L'estafador diu ser un funcionari del departament de frau del banc i ofereix a l'usuari assistència en el procés de validació del seu compte. Llavors comença a demanar-li dades personals, com el seu nom i cognoms, el número de telèfon i la seva adreça de correu electrònic.

Es creu que aquesta informació s'utilitzarà en un futur per a estafes més elaborades, per telèfon o correu electrònic.

L'empresa que va descobrir l'atac, RSA Security, va afirmar que els delinqüents utilitzen un protocol lliure de missatgeria instantània, que no té cap relació amb els programes de missatgeria instantània que l'usuari té instal·lats en el seu ordinador.

Font: www.viruslist.com



Secció responsables de seguretat

Nom i cognoms

Francesc P. Borguny Graullera

Lloc que ocupa

Cap de Seguretat Informàtica
(amb destinació al Servei d'Informàtica)

Des de quan

Març de 2002

Entitat

Universitat Autònoma de Barcelona

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

Al Servei d'Informàtica (SI) de la Universitat Autònoma de Barcelona (UAB).

La missió i l'estructura del Servei d'Informàtica estan definides per reglament propi. Es configura com un servei tècnic general de suport a la docència, a la recerca i a la gestió universitària i s'estructura en un àmbit central i en unitats distribuïdes (serveis d'Informàtica Distribuïda, SID), vinculades a cada àmbit territorial (centres, departaments, unitats departamentals, instituts, centres especials de recerca, de serveis i de centres d'estudis).

Les seves funcions més rellevants estan vinculades a les metodologies i els procediments de seguretat en tots els àmbits de les TIC: la supervisió de la seguretat en els processos del SI, l'auditoria interna de seguretat informàtica de la UAB i la gestió dels incidents contra la seguretat informàtica de la universitat, així com els plans de seguretat del SI.

Adicionalment, s'han definit funcions de col·laboració per impulsar diferents iniciatives en relació a la protecció de dades personals i el desenvolupament normatiu intern, i darrerament, també funcions d'impuls a la revisió, adequació i alineació de les polítiques de seguretat existents.

5

Per completar el mapa, cal dir que per a l'administració de sistemes i comunicacions (Administració i Explotació de

Sistemes i Comunicacions, AESC) i per a l'atenció personal en l'àmbit informàtic (Centre d'Assistència i Suport, CAS) disposem d'una contractació de serveis d'externalització, amb recursos presencials a les instal·lacions informàtiques del CPD del Servei d'Informàtica de la UAB. La cobertura horària és de disponibilitat total 24x7, mitjançant prestació presencial o de disponibilitat de personal quan sigui necessari.

La prestació d'aquests serveis d'externalització està orientada a permetre a la Universitat augmentar la focalització en els aspectes més estratègics dels seus sistemes d'informació, reduint la dedicació a tasques de manteniment i operatives.

Alhora, es disposa d'una organització flexible que facilita l'adaptació a l'evolució de l'organització i a la càrrega de treball i creixement dels diferents sistemes.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

Sí, amb l'ajuda d'un equip de dues persones, una de la mateixa Universitat i l'altra de l'empresa contractada. El rol i l'abast institucional són amplis i no podria desenvolupar plenament l'activitat sense la col·laboració de tots els professionals vinculats a les TIC.

Fins ara, l'objectiu principal ha estat créixer i millorar en la configuració dels processos de seguretat, des de les posicions més baixes i fins aconseguir construir un sistema de gestió de la seguretat dels sistemes d'informació. Això, mantenint una permanent atenció als riscos que poden fer incórrer la Universitat en responsabilitat.

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

Les dificultats que trobo no són gens diferents de les típiques del sector de la seguretat informàtica. Formen part del procés de maduració interna de les organitzacions, que progressivament les superen i les incorporen al seu funcionament normal.



La dificultat principal és trobar l'equilibri entre els avantatges que suposa l'ús de les TIC i els avantatges que aporta la seguretat com a valor afegit, com a generador de confiança, juntament amb el repte del compliment legal.

Altres dificultats estan vinculades amb la singularitat que en molts aspectes té una institució universitària. A la universitat cal cercar l'excel·lència en la prestació de serveis a professors, investigadors, estudiants i personal no docent. Tots ells tenen diferents necessitats, però també comparteixen la necessitat comuna de disposar de serveis ubics, és a dir, disposar d'accessos a la xarxa i a serveis, en qualsevol moment, des de qualsevol lloc i amb diversitat de dispositius, la qual cosa ens presenta un escenari amb un elevat grau d'exposició.

En aquest escenari, cal afegir les dificultats típiques del sector de la seguretat informàtica, que no per ser comunes entre les organitzacions són menys importants. Cal destacar: l'alta consolidació organitzativa interna dels diferents àmbits amb els quals es treballa habitualment, àrees, unitats, equips, etc.; la manca de conscienciació en matèria de seguretat informàtica; la resistència al canvi i les actituds poc respectuoses vers la comunitat universitària i la mateixa institució. El propi rol i la seva ubicació no estan exempts de dificultats vinculades a les diferents funcions.

Aquestes dificultats formen part de l'atractiu d'aquest rol, del repte que suposa, intentar-ho i aconseguir-ho poc a poc amb il·lusió, automotivació, paciència i, sobretot, amb la col·laboració i ajuda dels professionals implicats.

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

Hi ha hagut diferents responsabilitats en el temps que han requerit un elevat grau de dedicació, des de col·laborar a impulsar la iniciativa per al compliment legal juntament amb el Gabinet Jurídic, el CESCA i la resta d'universitats públiques catalanes. També amb el concurs públic, el desenvolupament del document de seguretat, la seva adequació a la nostra Universitat, la col·laboració en el desenvolupament de la normativa interna i el suport a les àrees afectades.

Actualment, respecte de la protecció de dades, les responsabilitats que requereixen més dedicació se centren en

aspectes relacionats amb les mesures tècniques de seguretat requerides al Reglament, el suport als diferents responsables tècnics dels serveis amb fixers afectats i la col·laboració i coordinació amb aquests responsables en l'execució d'auditories..

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

Sí, encara que no de forma directa. La relació amb l'APDCAT es formalitza institucionalment a través del responsable corporatiu de protecció de dades, que és qui planteja totes les qüestions que puguin sorgir.

Actualment, el comissionat de la Rectora per la Societat de la Informació d'aquesta Universitat, a proposta del Consell Interuniversitari de Catalunya, és membre del Consell Assessor de l'Agència.

Aprofito per felicitar l'APDCAT per aquesta iniciativa de donar l'oportunitat als responsables de seguretat de posar en comú experiències que ens ajuden a tots i compartir molts aspectes de millora.

Enllacem amb...

<http://www.priv.gc.ca/>

En els últims mesos, les xarxes socials han estat un focus d'atenció de les autoritats de control en matèria de protecció d'àmbit internacional. Una de les últimes a analitzar i pronunciar-se respecte d'aquest fenomen ha estat l'Oficina del Comissari de Privacitat del Canadà, que en aquest moments dirigeix la Sra. Jennifer Stoddart. Per aquest motiu i pels continguts que incorpora la pàgina, ens ha semblat oportú enllaçar amb aquest lloc web.

Es tracta d'una pàgina molt completa, amb els continguts en anglès i francès, de la qual destacaríem especialment la secció de recursos, on es pot trobar documentació de tot tipus relacionada amb les més diverses problemàtiques de privacitat. La web, amb un accés senzill i àgil, inclou tant publicacions com material audiovisual.



Cal destacar els documents que tracten qüestions com el procés d'avaluació de la privacitat (PIA) i les directrius o recomanacions, que, tot i que s'han d'analitzar des de la perspectiva d'aplicació de la legislació vigent al Canadà, aporten elements innovadors que podrien ser d'aplicació al nostre context.

El contingut de la pàgina es completen amb les seccions habituals d'organigrama, contacte, notícies, activitat parlamentària, reculls legislatius, etc.

On anar...

Congressos i esdeveniments

Net-ID 2009 - Identity, Trust, Privacy and Security in Europe

1 i 2 d'octubre de 2009. Berlín (Alemanya)
<http://www.computas.de/html/net-id09.html>

The 27th ACM International Conference on Design of Communication

Del 5 al 7 d'octubre de 2009. Bloomington, IN (EUA)
<http://www.sigdoc.org/2009/index.html>

2nd International Conference on Security of Information and Networks (SIN 2009)

Del 6 al 10 d'octubre de 2009. Gazimagusa (Xipre)
<http://www.sinconf.org/>

5th Annual INFORMATICS-Europe Meeting

8 i 9 d'octubre de 2009. París (França)
<http://www.informatics-europe.org/ECSS09/>

6th International Workshop on Visualization for Cyber Security

11 d'octubre de 2009. Atlantic City (EUA)
<http://vizsec.org/vizsec2009/>

The 2009 IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-09)

Del 12 al 14 d'octubre de 2009. Macau SAR (Xina)
<http://trust.csu.edu.cn/conference/tsp2009/>

4th International Conference on Malicious and Unwanted Software (Malware 2009)

13 i 14 d'octubre de 2009. Montreal, Quebec (Canadà)
<http://www.ieee-security.org/Calendar/cfps/cfp-MALWARE2009.html>

3rd International Conference on Network and System Security (NSS 2009)

Del 19 al 21 d'octubre de 2009. Gold Coast (Austràlia)
<http://nss2007.cqu.edu.au/FCWViewer/view.do?site=104>

International Conference on Risks and Security of Internet and Systems (CRiSIS)

Del 19 al 22 d'octubre de 2009. Toulouse (França)
<http://www.crisis2009.org/>

e-Privacy Directive Workshop

19 d'octubre de 2009. Londres (Gran Bretanya)
<http://www.e-comlaw.com/eprivacydirective/>

Workshop on Quantum and Classical Information Security

Del 26 al 30 d'octubre de 2009. Nàpols (Itàlia)
<http://www.quantumcomm.org/workshop.shtml>

4th International Workshop on Security (IWSEC2009)

Del 28 al 30 d'octubre de 2009. Toyama (Japó)
<http://www.iwsec.org/>

31a Conferència Internacional de Protecció de Dades i Privacitat

Del 4 al 6 de novembre de 2009. Agència Espanyola de Protecció de Dades, Madrid
<http://www.privacyconference2009.org/privacyconf2009/home/index-ides-idweb.html>

9th ACM Digital Rights Management Workshop 2009 (ACM DRM 2009)

9 de novembre de 2009. Chicago (EUA)
<http://www.almaden.ibm.com/cs/people/hongxia-jin/DRM2009/>

The Third Provable Security Conference (ProvSec 2009)

De l'11 al 13 de novembre de 2009. Guangzhou (Xina)
<http://ist.sysu.edu.cn/ProvSec2009/>

V Congreso Iberoamericano de Seguridad Informática (CIBSI '09)

Del 16 al 18 de novembre de 2009. Montevideo (Uruguai)
<http://www.fing.edu.uy/inco/eventos/cibsi09/>

International Conference on Information Security and Cryptology (ICISC '09)

Del 2 al 4 de desembre de 2009. Seul (Corea)
<http://www.icisc.org/>

Iberic Web Application Security conference (IBWAS09)

10 i 11 de desembre de 2009. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, UPM, Madrid
<http://www.ibwas.com/>

International Conference on Information Systems Security (ICISS 2009)

Del 14 al 18 de desembre de 2009. Kolkata (Índia)
<http://www.eecs.umich.edu/iciss09/>

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



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

Lluís Cermeno Martorell

Secretari de la Comissió Nacional d'Accés, Avaluació i Tria Documental

En el número 4 del Butlletí +Kdades de l'Agència Catalana de Protecció de Dades s'ha publicat l'article "Destrucció de documents en suport paper: preservar la confidencialitat fins al final de la vida útil de la informació"¹.

La lectura d'aquest article fa palès que s'ha omès una part important de la tasca de control que fan les persones professionals dels arxius de Catalunya. Al mateix temps, es fa una descripció de la situació que podríem sintetitzar en els següents punts:

- La destrucció dels documents en paper en les organitzacions públiques i privades estaria pràcticament descontrolada.
- La situació en el sector públic i privat és equivalent.
- El no control de la destrucció de documents produeix casos amb forta repercussió en els mitjans de comunicació i, consegüentment, hem de suposar que creen alarma social.
- En el sector públic:
 - La situació seria igual a Catalunya que a Espanya.
 - A Espanya (Catalunya inclosa), l'únic organisme que hauria emès criteri hauria estat el Ministeri de Cultura, per mitjà de la Comissió Superior Qualificadora de Documents Administratius.
 - A Catalunya no hi ha normativa específica sobre destrucció dels documents.

Atès que, pel que fa al sector públic català, no estem d'acord amb la situació descrita, hem elaborat un article que se centra en la normativa i els processos de destrucció de documents en el sector públic català². D'aquesta manera, els lectors i les lectores d'aquest Butlletí disposen d'una visió alternativa i de major informació sobre el sistema d'avaluació de documents i sobre els controls de la destrucció de documents que se'n deriven. No entrarem en cap cas en la situació que es produeix en el sector privat, del qual no tenim informació fidedigna, de forma que qualsevulla opinió emesa no deixaria de ser pura especulació.

1.- Què és l'avaluació de documents

El Decret 13/2008, de 22 de gener, sobre accés, avaluació i tria de documents³ (D13/2008) defineix en el seu article 2.b) l'avaluació de documents com: "la funció destinada a determinar el valor cultural, informatiu o jurídic dels documents, per tal de decidir-ne la conservació o l'eliminació". Com tota norma jurídica, la definició està feta en relació o en dependència d'altres disposicions normatives. Signifiquem aquí que l'objecte principal de la definició és el concepte *document*.

La Llei 9/1993, del patrimoni cultural català (LPCC), defineix *document* com "tota expressió en llenguatge oral, escrit, d'imatges o de sons, natural o codificat, recollida en qualsevol mena de suport material, i qualsevol altra expressió gràfica que constitueixi un testimoni de les funcions i les activitats socials de l'home i dels grups humans, amb exclusió de les obres d'investigació o de creació"⁴.

La Llei 10/2001 d'arxius i documents⁵ (LAD) indica, en el seu article 6, que són documents públics els produïts i rebuts en l'exercici de les seves funcions pel president, el Govern i l'Administració de la Generalitat; el Parlament de Catalunya, el Síndic de Greuges, la Sindicatura de Comptes i el Consell Consultiu; les administracions locals; els òrgans amb seu a Catalunya de l'Administració General i dels poders de l'Estat i el dels òrgans amb seu a Catalunya de la Unió Europea i d'institucions públiques internacionals.



La mateixa LAD estableix que cap document no pot ser eliminat si no s'ha seguit abans el procés d'avaluació corresponent (art. 9). Esmentarem com un altre element destacat de la LAD que, en el seu article 12, concreta les característiques dels documents públics: inalienabilitat, inembargabilitat i imprescriptibilitat.

Amb aquesta breu introducció al règim jurídic dels documents públics a Catalunya, us hem volgut conduir a un dels punts conceptualment importants de l'avaluació de documents. Per poder eliminar els documents, cal transformar-los⁶; i aquesta transformació es fa mitjançant un procés reglat d'avaluació documental, en el qual la Comissió Nacional d'Accés, Avaluació i Tria Documental (CNAATD) és l'òrgan competent per determinar-ne el termini de retenció, mitjançant les Taules d'Avaluació i Accés Documental (TAAD). Just en el moment en el qual ha vençut el termini de vigència administrativa, jurídica o fiscal d'un document i ja no té cap valor de caire informatiu o històric que en justifiqui la conservació, aquest document s'ha d'eliminar.

En el moment que s'elimina el document, podríem dir que ja no es considera un "document públic", atès que no té cap valor per a l'Administració i és per això que, per exemple, els podríem alienar. En aquest cas, el seu valor econòmic no estaria en la informació continguda com a document, sinó en la seva condició de mer "paper usat". En aquest punt, ja hem transformat els documents. Evidentment, aquests "papers" contenen informació que alguna persona pot llegir (una informació que no només es refereix a dades personals, sinó també dades financeres, tècniques, socials, etc.). És per aquest motiu que els organismes públics i controlats per la CNAATD segueixen uns protocols d'eliminació⁷.

2.- Procediments d'avaluació i eliminació de documents

La funció d'avaluació de documents en el marc del Sistema Arxivístic Català ja es va regular l'any 1990, quan el Govern aprovà el Decret 117/1990, de 3 de maig, sobre avaluació i tria de documents de l'Administració Pública. L'Administració Pública catalana es convertia en la pionera a l'Estat espanyol en aquesta matèria i creava la CNAATD, 10 anys abans que la Comissió Superior Qualificadora de Documents Administratius de l'Administració de l'Estat.

El Decret 117/1990 és l'antecedent directe de l'actual D13/2008 i és el que en el seu moment va establir els principals processos d'avaluació i eliminació de documents; processos que, essencialment, es mantenen amb l'actual regulació i que comentarem tot seguit.

Destaquem breument les principals característiques del sistema d'avaluació i eliminació de documents vigent⁸.

L'avaluació:

- a) Determina el temps de retenció dels documents d'una sèrie documental.
- b) És independent del suport o format en què s'han produït o gestionat els documents.
- c) Les propostes d'avaluació documental les elaboren les persones responsables de l'arxiu, però han d'obtenir l'autorització de l'òrgan que disposi de la màxima autoritat administrativa de l'organisme (secretari municipal, secretari general...).
- d) La CNAATD revisa les propostes d'avaluació documental i en determina el termini de vigència.
- e) Les eleva al conseller o consellera competent en matèria de Cultura, per a la seva aprovació.
- f) El resultat són les denominades Taules d'Avaluació i Accés Documental (TAAD), que es publiquen en forma d'Ordre del conseller o consellera competent en matèria de Cultura.
- g) Les TAAD són norma jurídica.



Eliminació:

- a) Per poder eliminar documentació, cal disposar sempre d'una TAAD a la qual es pugui fer referència. Si no es té, no es pot eliminar la documentació.
- b) Quan la persona responsable d'un arxiu vol aplicar una TAAD, prèviament ha fer el següent:
 - a. Obtenir el vistiplau de la persona responsable de la unitat administrativa productora de la documentació.
 - b. Assegurar-se que cap circumstància (bàsicament de tipus judicial) hagi pogut alterar el termini de retenció dels documents.
 - c. Disposar d'un inventari dels documents / expedients a eliminar.
 - d. En cas de terminis de retenció establerts en cinc anys o més, obtenir el vistiplau previ de la CNAATD.
- c) Un cop la persona responsable de l'arxiu ha complert els punts anteriors, pot procedir a la destrucció de la documentació. L'eliminació es pot fer per mitjans propis o aliens. En el segon cas, si per dur a terme la destrucció es requereix la participació d'empreses externes, s'exigeix un certificat de l'empresa conforme s'han eliminat totalment els documents.
- d) La normativa preveu que tota eliminació de documents es registri en un Registre de Destrucció de Documents, el qual ha d'estar a disposició de la inspecció d'arxius i de la CNAATD.

Tot seguit, destaquem unes característiques comunes entre els procediments d'avaluació i destrucció de documents en el sistema arxivístic català.

1.- Els procediments d'avaluació de documents i destrucció estan concebuts des d'una perspectiva en què la responsabilitat és corporativa. Així, el protagonisme en la gestió i l'execució de les propostes d'avaluació documental i l'aplicació de TAAD recau en les persones responsables de l'arxiu (o millor, responsables del sistema de gestió de documents de l'organització), però no de forma exclusiva. D'aquesta manera, les propostes d'avaluació documental han de ser validades per les persones responsables de l'Administració de l'organisme o bé, prèviament a l'eliminació, s'ha d'obtenir l'autorització de les persones responsables de les unitats productores.

2.- La CNAATD és un òrgan de referència per als centres del Sistema d'Arxius de Catalunya de forma que, a més de vetllar per l'aplicació correcta de les TAAD, dóna suport tècnic als arxius.

3.- Tots els processos d'avaluació i eliminació per norma estan documentats, de forma que se'n pot fer la traçabilitat.

4.- Les funcions d'avaluació i, si escau, eliminació de documents es consideren de forma integrada als sistemes de gestió documental que duen a terme les organitzacions. En aquest sentit, el sistema català segueix els principis que en aquesta matèria fixa la norma ISO 15489:2001 Informació i Documentació. Gestió Documental⁹. Aquesta norma, publicada l'any 2001, s'ha erigit en un referent internacional en aquesta matèria, tant per a organitzacions públiques com privades. La norma¹⁰ detalla els processos de gestió documental, que són: Incorporació, Registre, Classificació, Assignació de categories d'accés i seguretat, Identificació del tipus de disposició¹¹, Emmagatzematge, Ús i traçabilitat i Disposició. Cadascun d'aquests processos és una part que conforma un tot.

3.- Resultats

L'acció de la CNAATD va començar a obtenir resultats tangibles a partir de l'any 1995 i, fins l'any 2008, s'han destruït més de 33.480 metres lineals de documents de les diverses administracions públiques¹²; així mateix, remarcuem que l'any 2008 i 66 centres d'arxiu van aplicar TAAD¹³.



Finalment, anem a fer un seguit de reflexions finals:

- 1.- Podem considerar que els processos de destrucció de documents s'estan duent a terme a Catalunya de forma molt correcta, amb una bona implicació del conjunt de professionals d'arxius de les diverses administracions públiques.
- 2.- Progressivament es va incrementant el nombre d'organismes públics que constitueixen sistemes de gestió de documents i, per tant, apliquen cada cop un major nombre de TAAD.
- 3.- En el sector privat català, en general no s'han desenvolupat encara sistemes de gestió de documents similars als del sector públic. Tot i així, la legislació tendirà a anar obligant a disposar d'aquests sistemes de forma similar al que succeeix a d'altres estats occidentals.
- 4.- S'ha fet una destacada normativització en matèria d'avaluació de documents i aplicació de resolucions. Així, en el període 1995 - 2008 s'han aprovat i publicat al Diari Oficial de la Generalitat 20 ordres del conseller o la consellera de Cultura, cosa que ha permès l'aprovació d'un total de 635 taules d'avaluació documental¹⁴.

Esperem haver pogut transmetre al lector que, si més no a Catalunya i en el seu sector públic, existeix una clara política de destrucció de documents, que és efectiva i que està permetent processar milers de documents de forma totalment segura i amb el grau de confidencialitat escaient. També esperem que s'hagi pogut copsar que aquest resultat positiu ho són gràcies que les organitzacions estan prenent clara consciència de la importància de la correcta gestió dels seus documents i, sobretot, perquè hi ha un conjunt de professionals dels arxius que, de forma discreta i eficient, impulsen i dirigeixen sistemes de gestió de documents.

Notes:

- ¹ Miralles, Ramon: "Destrucció de documents en suport paper: preservar la confidencialitat fins al final de la vida útil de la informació". +Kdades núm. 4/juny 2009. Agència Catalana de Protecció de Dades.
- ² Àmbit competencial de la Comissió Nacional d'Accés, Avaluació i Tria Documental, òrgan col·legiat que l'autor no ha citat.
- ³ Decret 13/2008, de 22 de gener, sobre accés, avaluació i tria de documents. DOGC 5056 de 25.1.2008.
- ⁴ Art. 19.1 de la Llei 9/1993, de 30 de setembre, del patrimoni cultural català. DOGC 1807 d'11.10.1993.
- ⁵ Llei 10/2001, de 13 de juliol, d'arxius i documents. DOGC 3437 de 24.7.2001).
- ⁶ En aquest punt, estem d'acord amb la introducció que planteja R. Miralles; el problema és en el fet que en el seu article no ha explicat com es transformen.
- ⁷ *Eliminació* es defineix a l'art. 2d) del D13/2008 com "la destrucció o supressió **d'informació o documents** per qualsevol sistema que n'impossibiliti la recuperació o posterior accés i utilització".
- ⁸ Disposeu de tota la informació sobre aquests processos a la pàgina web del Departament de Cultura i Mitjans de Comunicació de la Generalitat de Catalunya <http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.03f78855c746589fda97dc86b0c0e1a0/?vgnextoid=b0595cacff59f010VgnVCM100008d0c1e0aRCD&vgnnextchannel=b0595cacff59f010VgnVCM100008d0c1e0aRCD&vgnnextfmt=default>
- ⁹ Aquesta norma es divideix en dues parts: la primera són consideracions generals i la segona, directrius. Des de l'any 2009, AENOR disposa d'una traducció catalana de la corresponent versió UNE-ISO 15489 Informació i Documentació. Gestió Documental.
- ¹⁰ Vegeu apartat 4 Processos i controls de la gestió documental, de la Norma UNE-ISO 15489-2:2001 Informació i Documentació. Gestió Documental. Directrius.
- ¹¹ En el marc de la norma ISO 15489, el terme *disposició* engloba el període de temps de conservació de documents i el moment i condicions per a la seva destrucció o bé transferència cap als arxius històrics.
- ¹² Correspon a documentació amb un termini de retenció de cinc anys o més, que és el que els centres d'arxiu tenen l'obligació de comunicar. D'acord amb un estudi fet per la CNAATD, si comptem l'eliminació de documents amb uns terminis de retenció inferiors caldria incrementar aquesta xifra en un 20%.
- ¹³ Les dades aquí comentades s'han extret de la memòria d'activitats de la CNAATD de l'any 2008. <http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Comissio%20Nacional%20d%20Acces/Actes/arxius/Memoria%202008%20CNAATD.pdf>
- ¹⁴ Podeu consultar tota la normativa a la pàgina web del Departament de Cultura i Mitjans de Comunicació: <http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.d81d04123ceb3b8fda97dc86b0c0e1a0/?vgnextoid=95c9adf74e99f010VgnVCM100008d0c1e0aRCD&vgnnextchannel=95c9adf74e99f010VgnVCM100008d0c1e0aRCD&vgnnextfmt=default>