



A l'Agència Catalana de Protecció de Dades, sempre hem prestat especial atenció als aspectes tecnològics relacionats amb la salvaguarda del dret a la protecció de dades de caràcter personal. Les mesures de seguretat tècniques i organitzatives són un element clau per a una efectiva protecció de la informació de caràcter personal i som conscients que, sovint, sincronitzar els requeriments legals de protecció de la informació amb les solucions tècniques resulta una tasca complicada.

La publicació electrònica de l'APDCAT que us presento pretén ser un instrument útil i complementari d'altres actuacions de l'Agència, una eina que ajudi a fer menys complicada la tasca de protegir la informació. Va adreçada, especialment, a les persones de perfil tècnic i de gestió tècnica que tenen responsabilitats relacionades amb l'auditoria i la seguretat de la informació, tot i que procurem que els seus continguts també siguin d'interès per a d'altres perfils professionals relacionats amb els tractaments de dades personals.

El +Kdades és una iniciativa que situem en l'àmbit de la prevenció, una línia de treball a la qual donem molta importància al l'Agència, perquè la considerem una de les millors maneres d'avançar cap a una gestió responsable de la informació de caràcter personal. Espero que, mes a mes, aquesta publicació resulti d'utilitat en el vostre dia a dia.

Esther Mitjans

Directora de l'Agència Catalana de Protecció de Dades

Continguts

Incidents de seguretat relacionats amb dades personals	2
Tecnologia i protecció de dades	2
Parlem amb els responsables de seguretat	3
Enllacem amb...	4
On anar...	4
L'ús de metadades sobre dades personals orientat a l'interoperabilitat	5

Parlem de... l'ús de metadades sobre dades personals orientat a la interoperabilitat

El concepte *metadades* fa referència a l'ús de dades que descriuen altres dades, en definitiva *dades sobre dades*. A la pràctica, aquest ús es relaciona amb dos àmbits d'actuació: la web semàntica i la recuperació d'informació.

En el context dels projectes d'administració electrònica, l'ús de metadades té com a punt de partida la iniciativa coneguda com a Dublin Core Metadata Standard (convertida en la ISO 15836:2003) que, adaptada a les necessitats de l'intercanvi de dades i documents relacionats amb el sector públic, ha donat lloc a perfils d'aplicació específics (*application profiles*). Un dels més coneguts és l'e-GMS3 (e-Government Metadata Standard del Regne Unit, 2001), que proposa l'ús generalitzat de metadades en el sector públic per a la gestió dels recursos d'informació i la seva localització.

Aquí, el que proposem és una aplicació innovadora de les metadades: usar-les per descriure la informació de caràcter personal objecte d'intercanvi; una descripció centrada en les característiques de la informació en relació a la protecció de dades de caràcter personal.

+Info



Incidents de seguretat relacionats amb dades personals

Caiguda de Gmail (febrer de 2009)

La darrera setmana de febrer de 2009, el servei de correu electrònic de Google (Gmail) va deixar de funcionar durant 4 hores. En un comunicat, Google informava que la caiguda del servei es va produir per un error en les tasques de manteniment d'un centre de procés de dades europeu de la companyia, desmentint així que hagués estat degut a un atac extern.

Per altra banda, Sophos ha advertit els usuaris del servei d'una possible amenaça de pesca (*phishing*) en el servei de missatgeria instantània de Gmail (Google Talk).

Un fallada de seguretat de Twitter permet a un pirata informàtic (*cracker*) suplantar el compte d'Obama (gener de 2009)

El sistema de microblogging Twitter ha sofert un incident de seguretat, que va permetre que un pirata (*cracker*) segrestés els comptes d'usuari de 33 personatges famosos i es fes passar pels seus propietaris, per llançar missatges difamatoris. Entre els comptes segrestats hi havia els de Barack Obama i Britney Spears

FACUA denuncia Microsoft, Yahoo i Google per la baixa seguretat en l'accés al correu electrònic (gener de 2009)

L'Associació de Consumidors i Usuaris en Acció (Facua) ha denunciat Microsoft, Yahoo i Google davant l'Agència Espanyola de Protecció de Dades, per "un greu problema de seguretat" en els seus serveis de correu electrònic. Aquest error permet que qualsevol persona accedeixi al compte de correu d'un altre usuari, si coneix on viu i la resposta a una pregunta de seguretat, que en molts casos es fàcil d'esbrinar.

L'associació ha posat com a exemple l'intent d'extorsió a un conegut cantant, on unes persones li demanaven diners a canvi de no divulgar informació obtinguda dels seus missatges de correu electrònic.

Tecnologia i protecció de dades

INTECO I PANDA PROTEGIRAN ELS MENORS A INTERNET

INTECO i Panda han donat a conèixer les iniciatives que han acordat conjuntament, per a la millora de la seguretat dels adolescents quan naveguen per la xarxa. La principal iniciativa es refereix a l'educació en matèria de seguretat.

FUJITSU SIEMENS BLINDA LA INFORMACIÓ DELS PORTÀTILS

Es proposen dues solucions, la primera per localitzar els portàtils, en el moment que es connectin a Internet, i l'altra per poder-ne esborrar de forma remota el contingut.

AUDEMA AVANÇA EN AUTENTICACIÓ

S'anuncia el llançament i comercialització de la família aXs Guard, per protegir els accessos a aplicacions en mode remot.

SYMANTEC MILLORA LA PROTECCIÓ CONTRA LA PÈRDUA DE DADES EN ELS PUNTS FINALS

Symantec ha llançat el producte Data Loss Prevention 9.0, que ofereix a les organitzacions més capacitat per localitzar, controlar i protegir la informació confidencial, en qualsevol lloc on s'emmagatzemi o s'utilitzi.

[més informació](#)

JUNIPER PRESENTA NOVES SOLUCIONS DE SEGURETAT

Juniper Networks va anunciar les solucions adaptatives d'administració d'amenaçes. És un conjunt obert de solucions que ofereix defensa en temps real, amb visibilitat de la xarxa i control a escala, per reduir el risc i augmentar la productivitat.

[més informació](#)



Parlem amb els responsables de seguretat

Nom i cognoms
Anna Garcia Martínez

Lloc que ocupa
Responsable Programa de Seguretat de la Informació

Des de quan
Novembre 2006

Entitat
Departament de Salut

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

En el Departament de Salut, pel tipus de dades que es tracten, s'està treballant des de fa anys en temes de confidencialitat de la informació i protecció de dades personals. En els últims temps, la preocupació s'ha ampliat a conceptes com integritat i disponibilitat dels sistemes.

Els qui treballem en la definició d'estratègies i de polítiques de Sistemes d'Informació en Salut fa temps que pensem a donar resposta a un àmbit que comprèn el Departament de Salut, el Servei Català de la Salut i, en els casos en què els sistemes s'intercomuniqueu, també som referents per als centres sanitaris (per exemple, en temes de seguretat: marcs de regulació legislativa, polítiques de seguretat i definició de criteris).

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

Sí, el meu àmbit d'activitat és ampli però sempre des de la perspectiva de Seguretat de la Informació.

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

La necessitat del treball conjunt amb àrees amb formes de treball molt diverses. Constantment ens relacionem amb responsables de negoci, de recursos humans, de tecnologia i d'assessories jurídiques. Qualsevol petit canvi en la forma de treballar a l'Administració requereix il·lusió i dosis de resistència a la frustració.

No obstant això, també considero que aquesta dificultat és el gran atractiu d'aquesta feina.

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

Donar suport a les àrees. Vam iniciar les activitats del Programa de Seguretat organitzant sessions de formació sobre la normativa de seguretat, i en l'actualitat el nostre esforç fonamental es basa en la implantació de procediments de seguretat. En organitzacions tan extenses com Salut, sempre hi ha nous projectes que ens consulten sobre les mesures de seguretat a implantar.

Les activitats més recents en què estem treballant es centren en temes d'auditoria, pensant en aquest instrument com una eina que ens permeti, també, continuar en la línia anterior de suport a través d'identificar com podem millorar.

Finalment, un últim aspecte interessant és la participació en projectes d'innovació tecnològica.

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

Sí, i sempre que hem demanat suport, el nivell de resposta ha estat excel·lent. Bàsicament, hem validat amb l'APDCAT propostes que volíem fer arribar a tot el sector o projectes que hem considerat innovadors a nivell de tecnologia i impacte en la ciutadania (recepta electrònica o història clínica compartida, per exemple). Les seves aportacions ens han facilitat una perspectiva sempre interessant.

El meu cap, responsable de la Secretaria d'Estratègia i Coordinació, és membre del Consell Assessor de l'Agència i participa amb interès en aquest organisme.

El suport que he rebut de l'Agència, i hi incloc les diverses inspeccions i l'auditoria, ha estat fonamental per poder assumir les responsabilitats diàries. Sempre he rebut una resposta professional i col·laboradora.



Enllacem amb...

<http://www.enisa.eu>

L'Agència Europea de Seguretat de les Xarxes i de la Informació és un organisme de la Unió Europea. La seva principal funció és assessorar i fer recomanacions relacionades amb l'anàlisi de dades i l'organització de campanyes de sensibilització promogudes pels òrgans de la UE i els Estats membres, en relació a la seguretat de les xarxes i la informació.

ENISA es considera un centre de coneixement especialitzat en relació a qüestions de seguretat de productes i solucions, tant de maquinari com de programari. Promou iniciatives relacionades amb l'anàlisi i la gestió de riscos i elabora estudis sobre aquesta matèria, adreçats tant al sector públic com privat.

De la seva pàgina a Internet, són d'especial interès les seccions "ENISA Library", on podem trobar publicacions, tant periòdiques (trimestrals) com de caràcter puntual, així com interessants estudis relacionats, per exemple, amb els menors i Internet, la societat de la informació segura, l'ús del correu electrònic, l'administració electrònica, etc. S'hi pot trobar també la secció "Country Reports", amb informes detallats sobre la seguretat de les xarxes i la informació de cada estat membre de la Unió Europea, i de l'espai europeu.

On anar...

Cursos de postgrau i especialitat en seguretat de la informació

Programes de Seguretat Informàtica (2009)
Institut Internacional de Postgrau de la Universitat Oberta de Catalunya UOC
http://www.uoc.edu/masters/cat/web/informatica_multimedia_telecomunicacio/seguretat_informatica/

Edició 2009 del Màster en Auditoria i Protecció de dades Departament de Ciència Política i Dret Públic de la Universitat Autònoma de Barcelona (UAB)
http://www.cdpd.uab.cat/postgraus/master_auditoria_proteccio_dades/cat/index.htm

Congressos i esdeveniments

18th International World Wide Web Conference WWW
Del 20 al 24 d'abril de 2009. Madrid
<http://www2009.org/>

Cuarto Congreso Colombiano de Computación 4CCC
Del 23 al 25 d'abril de 2009. Bucaramanga (Colòmbia)
<http://serverlab.unab.edu.co/4ccc>

7th International Workshop on Security In Information Systems
Del 6 al 10 de maig de 2009. Milà (Itàlia)
<http://www.iceis.org/Workshops/wosis/wosis2009-cfp.htm>

V Congreso Iberoamericano de Telemática CITA 2009
11 i 12 de maig de 2009. Gijón
<http://www.cita2009.com/>

Tercer Counter-eCrime Operations Summit CeCOS III
Del 12 al 14 de maig de 2009. Barcelona
http://www.antiphishing.org/events/2009_opSummit.html

2nd International Symposium on Distributed Computing and Artificial Intelligence DCAI 09
Del 10 al 12 de juny de 2009. Salamanca
<http://dcai.usal.es/>

Third IFIP WG 11.11 International Conference on Trust Management
Del 15 al 19 de juny de 2009. West Lafayette (EUA)
<http://projects.cerias.purdue.edu/IFIPTM/>

IX Jornada Nacional de Seguridad Informática ACIS 2009
Del 17 al 19 de juny de 2009. Bogotà (Colòmbia)
<http://www.acis.org.co/index.php?id=1246>

Cuarta Conferencia Ibérica de Sistemas y Tecnologías de la Información
Del 17 al 20 de juny de 2009. Póvoa de Varzim (Portugal)
<http://www.aisti.eu/cisti2009/>

IADIS Multi Conference on Computer Science and Information Systems 2009
Del 17 al 23 de juny de 2009. Algarve (Portugal)
<http://www.mccsis.org/>

E-Activity and Leading Technologies E-ALT2009 e InterTIC 2009
Del 22 al 24 de juny de 2009. Sevilla
<http://www.iask-web.org/intertic09/intertic09.html>

14th IEEE Symposium on Computers and Communications
Del 5 al 8 de juliol de 2009. Sousse (Túnez)
<http://www.comsoc.org/iscc/2009/>

XV Jornadas de Enseñanza Universitaria de la Informática JENUI 2009
Del 8 al 10 de juliol de 2009. Barcelona
<http://jenui2009.fib.upc.edu/>



Metadades i dades personals

Hi ha propostes concretes de l'ús de metadades en relació a dades personals i a la privacitat. Pel que fa a dades personals, tenim el FOAF (Friend-of-a-Friend / Amic d'un amic), que està orientat a descriure persones mitjançant les seves dades personals (nom, adreça, correu electrònic, professió, interessos, plans de futur, imatges, publicacions, etc.).

«Hi ha propostes concretes de l'ús de metadades en relació a dades personals i a la privacitat.»

El arxius FOAF segueixen l'estructura RDF (Resource Description Framework7) i s'escriuen en XML (Extensible Markup Language8). RDF proporciona un marc per a la descripció de recursos digitals: és una especificació del W3C per definir, mitjançant metadades, els recursos que es poden trobar a Internet.

S'utilitza fonamentalment en l'entorn de blocs i xarxes socials (comunitats virtuals), com a mecanisme senzill i ràpid per compartir informació de caràcter personal i posar en contacte persones amb interessos comuns.

Les dades que es poden intercanviar o compartir amb els fitxers FOAF s'agrupen segons el FOAF Vocabulary Specification 0.9 Namespace, de 24 de maig de 2007 (<http://www.foaf-project.org/>).

I quant a privacitat, cal fer referència a EPAL (Enterprise Privacy Authorization Language) i a XACML (control d'accés basat en XML). Aquest últim és un estàndard per a l'intercanvi de dades codificades que, d'una manera senzilla i flexible, permet expressar i fer complir polítiques de control d'accés a dades personals en plataformes tècniques heterogènies, utilitzant un únic llenguatge.

EPAL és un llenguatge d'interoperabilitat orientat a l'intercanvi de polítiques de privacitat de forma estructurada, tant entre aplicacions com entre organitzacions. És capaç de comparar de forma automàtica polítiques de privacitat per verificar-ne coincidències o discrepàncies i, per tant, autoritzar o denegar l'accés o l'intercanvi de dades.

«Interoperabilitat: capacitat dels sistemes d'informació, i per tant dels procediments als quals aquests donen suport, de compartir dades i possibilitar l'intercanvi d'informació i coneixement entre ells.»

Metadades i protecció de dades personals

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, incorpora una definició d'interoperabilitat que inclou no només la transmissió de dades, sinó també de coneixement, que podria ser tramès i gestionat mitjançant l'ús de metadades:

«Interoperabilitat: capacitat dels sistemes d'informació, i per tant dels procediments als quals aquests donen suport, de compartir dades i possibilitar l'intercanvi d'informació i coneixement entre ells.»

La Llei 11/2007 preveu, a la lletra a) de l'art. 4 (principis generals), que l'ús de les tecnologies de la informació s'ha d'ajustar al que preveu la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. La mateixa Llei regula, a l'art. 9, la transmissió de dades entre administracions públiques i, a l'art. 20, preveu que dins de les condicions i garanties per compartir informació s'hi ha d'incloure la naturalesa de les dades a intercanviar. Vist això, es pot plantejar la conveniència de preveure que els nostres esquemes d'interoperabilitat d'administració electrònica incloguin, juntament amb les especificacions de les dades a intercanviar o compartir, informacions en forma de metadades, relacionades



amb el requeriments o circumstàncies previstes a la legislació en matèria de protecció de dades personals.

«Proposem d'abordar el disseny d'un model de metadades per a l'intercanvi d'informació de caràcter personal (MDP), que faciliti el compliment de la normativa de protecció de dades.»

Aquest model de metadades sobre protecció de dades (que té alguns punts en comú amb el concepte de *privacy metadata*), podria proporcionar informació addicional sobre les dades intercanviades o compartides, per donar resposta a aspectes absolutament pragmàtics de la gestió de la informació de caràcter personal, inclosa la perspectiva del compliment normatiu, com:

- La gestió del consentiment.
- La data d'actualització de les dades.
- Les finalitats o ús autoritzats arran de l'intercanvi.
- La circumstància que es tracti d'intercanvis que tinguin el seu origen en l'exercici de drets: accés, rectificació, cancel·lació i oposició.
- Possibles terminis de cancel·lació de les dades, quan són coneguts o determinables.
- Tipus de dades intercanviades: especialment les de caràcter més sensible.
- Nivell de seguretat en origen, o que s'aplicarà en destí.
- Gestió de les comunicacions efectuades (en relació a l'exercici de possibles drets d'accés).
- La indicació que s'intercanvien dades de menors.
- Etc.

Per tant, proposem d'abordar el disseny d'un model de metadades per a l'intercanvi d'informació de caràcter personal (MDP), que faciliti el compliment de la normativa de protecció de dades, especialment en relació al ús o tractament de la informació intercanviada o compartida, i faci més eficient la gestió d'aquesta informació compartida o intercanviada. Aquesta actuació estaria alineada amb la perspectiva que aporta el concepte de *privacitat dissenyada*, que estem treballant des de l'Agència Catalana de Protecció de Dades.

«Privacy by design és una proposta que aglutina diferents iniciatives, que tenen com a objectiu comú prevenir i tractar les qüestions derivades de la privacitat i la protecció de dades personals.»

El model de privacitat dissenyada o *privacy by design* és una proposta que aglutina diferents iniciatives, que tenen com a objectiu comú prevenir i tractar les qüestions derivades de la privacitat i la protecció de dades personals, incorporant elements de seguretat i privacitat en el disseny de les solucions de gestió de la informació personal (protecció de dades). Aquest model de privacitat dissenyada es contraposa a models de privacitat incorporada o accessòria, on la seguretat i la protecció de les dades personals s'incorporen una vegada les solucions de gestió de la informació ja s'han dissenyat i construït.

Si desitgeu aprofundir en aquesta qüestió, podeu consultar els enllaços següents:

http://es.wikipedia.org/wiki/Resource_Description_Framework
<http://es.wikipedia.org/wiki/XML>
http://es.wikipedia.org/wiki/World_Wide_Web_Consortium
<http://www.foaf-project.org>
<http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html>
<http://sunxacml.sourceforge.net/>
<http://www.w3.org/P3P/>
<http://dublincore.org/>
<http://www.govtalk.gov.uk/schemasstandards/metadata.asp>
<http://www.iptc.org/>
<http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1013>
<http://www.niem.gov/>