



Destaquem... 2n Pla d'auditoria

El 15 de juny passat, l'APDCAT va presentar el seu segon Pla d'auditoria, que s'ha posat en marxa aquest mes d'octubre i que té per objecte verificar algunes mesures de seguretat de caràcter organitzatiu, recollides al reglament de desplegament de la LOPD.

El desenvolupament del primer Pla d'auditoria, l'any 2008, adreçat a verificar el compliment del dret d'informació en la recollida de dades i que ara és en la fase final d'informes d'auditoria, ha permès a l'Agència fer una primera aproximació a la situació real dels tractaments de dades de caràcter personal en les entitats que estan sota el seu control. Alhora, però, també ens ha permès apropar-nos a les diferents realitats de les administracions públiques catalanes i ens ha dut a la convicció que els plans d'auditoria són una eina útil, no únicament per a l'Agència, sinó també per a les entitats auditades.

Les mesures de seguretat objecte de verificació són que hi hagi el responsable de seguretat i que es porti el registre d'incidències i processos relacionats; a diferència del primer Pla d'auditoria, en aquest segon està previst que els treballs d'auditoria es desenvolupin de forma presencial.

En total, les entitats incloses en aquest segon Pla són 144: tots els departaments de la Generalitat de Catalunya i un organisme que depengui de cadascun d'ells; totes les universitats que integren el sistema universitari català; les diputacions; els consells comarcals que no es van auditar al primer Pla d'auditoria; i tots els municipis de Catalunya amb una població superior a 20.000 habitants. Tal i com està previst en la metodologia que utilitza l'APDCAT per als plans d'auditoria, durant el mes d'octubre s'enviaran cartes a les entitats seleccionades, comunicant l'inici del Pla d'auditoria i demanant la designació d'un interlocutor per als treballs que es derivin del procés de verificació.



Parlem... del sistema de gestió de la protecció de dades personals (SGPDP)

Des de l'Agència Catalana de Protecció de Dades, hem anat insistint en la idea que el compliment de les obligacions dels responsables de tractaments de dades de caràcter personal és un assumpte que no s'ha d'abordar exclusivament des d'una perspectiva de compliment normatiu, és a dir, per evitar els expedients sancionadors: s'ha de tractar sobretot com una qüestió derivada de les necessitats d'una gestió responsable de la informació, amb una vinculació molt estreta amb l'eficàcia i eficiència dels processos de negoci en què es puguin veure involucrades dades de caràcter personal.

Un altre dels missatges llançats amb reiteració des de l'APDCAT és la importància de tot allò que pugui prevenir incidents amb les dades personals. En un número anterior del +KDades ja vam parlar de la nostra visió del concepte de *privacy by design*. Doncs bé, emmarcat en el que podem considerar el paraigües de la privacitat en el disseny, volem tractar ara una qüestió que ens sembla rellevant i que pot marcar l'evolució futura dels mecanismes de compliment de la normativa de protecció de dades de caràcter personal.

Us volem parlar d'orientar el compliment normatiu cap a un procés sistemàtic, documentat i conegut per tota l'organització que, sota la denominació de sistema de gestió de la protecció de dades personals (SGPDP), doni resposta tant a les obligacions normatives com a les necessitats dels processos de negoci.

Continguts

Destaquem...	1
Parlem de...	1
Tecnologia i protecció de dades	2
On anar...	2
Incidents de seguretat relacionats amb la protecció de dades	3
Butlletí revisió vulnerabilitats	3
Responsables de Seguretat	4
Enllacem amb...	4
El sistema de gestió de la protecció de dades personals (SGPDP)	5

+info

Tecnologia i protecció de dades

Security Essentials Microsoft llança un programari gratuït de seguretat

Microsoft Security Essentials constitueix el primer esforç de Microsoft per combinar una solució antivirus gratuïta en un paquet d'aproximadament 5 Mb, compatible amb Windows XP, Vista i 7 (32 i 64 bits). L'únic requisit per poder utilitzar Microsoft Security Essentials és tenir una còpia de Windows original.

Durant alguns mesos, Security Essentials ha estat disponible en versió beta per a una selecció d'usuaris, alguns dels quals opinen que sorprenen positivament la rapidesa, facilitat d'ús i eficàcia. Les definicions de programari maliciós (*malware*) s'actualitzen tres cops al dia.

Tot fa pensar que la combinació de Security Essentials amb un sistema operatiu actualitzat, el tallafocs de Windows i un navegador actualitzat constitueixen un esquema òptim per a la majoria dels usuaris d'Internet, tot i que les companyies que es dediquen a la seguretat afirmen que no es tracta d'un paquet complet de seguretat.

A l'hora d'instal·lar Microsoft Security Essential es recomana desinstal·lar els antivirus, ja que es podrien generar conflictes i provocar errors del sistema.

<http://www.diarioti.com/gate/n.php?id=24207>

<http://www.gigle.net/microsoft-security-essentials-listo-para-descarga/>

INTECO impulsa la certificació i implantació de sistemes de gestió de seguretat de la informació (SGSI) a les pimes espanyoles

144 pimes, 45 empreses d'implantació i 10 empreses certificadores han participat en una iniciativa que té com a finalitat augmentar la seguretat, la competitivitat i l'optimització de processos i recursos en sistemes d'informació, i reduir-ne els riscos.

L'Institut Nacional de Tecnologies de la Comunicació (INTECO) ha lliurat, a la seva seu de Lleó, els diplomes que acrediten la participació de les 144 pimes espanyoles en el programa de foment i impuls de la implantació i certificació de sistemes de gestió de seguretat de la informació (SGSI) a les seves empreses. Les pimes que hi han participat provenen de tot el territori nacional i procedeixen de diferents sectors, però sobretot del serveis empresarials i les comunicacions.

INTECO ha ajudat aquestes petites i mitjanes empreses a certificar-se d'acord amb la norma internacional de referència en seguretat, UNE-ISO/IEC 27001, posant a la seva disposició un catàleg de 45 empreses implantadores i un altre de 10 certificadores. Les empreses participants van seleccionar una empresa implantadora, que

els va ajudar a complir amb els requisits de la norma, i una de certificadora, que va comprovar que realment la pime complia aquells requisits.

INTECO, dins del marc del Pla Avança, té com a objectiu potenciar la incorporació de la seguretat a les pimes. D'altra banda, INTECO donarà continuïtat al programa a través de l'elaboració de material formatiu derivat de l'experiència obtinguda en aquest projecte. Tot això donarà lloc a una web temàtica (<https://sgsi.inteco.es>), un vídeo tutorial i un curs de formació en línia.

http://www.inteco.es/Prensa/Actualidad_INTECO_diplomas_SGSI_pymes

L'Associació d'Internautes posa a disposició de la comunitat el programa d'avís "Alerta-Bulos"

Alerta-Bulos és una aplicació per a llocs web, que conté informació fiable d'alerta sobre les informacions enganyoses existents a la xarxa. L'aplicació enllaça amb la Comissió encarregada del seguiment d'aquestes informacions de l'associació d'internautes, on informaran en línia dels últims avisos sobre informacions enganyoses a Internet. Cada avís disposarà d'un enllaç per poder aprofundir més en l'alerta.

Aquest sistema està preparat per exportar-lo a qualsevol web que desitgi tenir aquest servei.

Què pretén "Alerta-Bulos"?

- Trobar solucions per combatre i pal·liar els efectes negatius que les informacions enganyoses a Internet ocasionen a les persones, institucions i empreses.
- Crear solucions de referència perquè internautes, entitats públiques i privades i mitjans de comunicació hi puguin acudir, per obtenir informació completa, fiable i actualitzada sobre la situació de les informacions enganyoses a Internet.
- Aconseguir que els internautes informin en línia sobre les informacions enganyoses que reben.
- Que hi hagi una informació fiable i en línia sobre les informacions enganyoses que circulen per Internet.

Els internautes podran informar sobre les informacions enganyoses que rebin per al seu compte de correu a alertabus@internautas.org.

<http://www.internautas.org/html/5710.html>

On anar...

Congressos i esdeveniments

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.svsu.edu.cn/ProvSec2009/>

16th ACM Conference on Computer and Communications Security (ACM CCS 2009)

Del 9 al 13 de novembre de 2009. Chicago (EUA)
<http://www.sigsec.org/ccs/CCS2009/index.shtml>

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/>

IADIS International Conference WWW Internet 2009

Del 19 al 22 de novembre de 2009. Roma (Itàlia)
<http://www.internet-conf.org/>

IEEE Globecom 2009

Del 30 de novembre al 4 de desembre de 2009. Honolulu, Hawaii (EUA)
<http://www.ieee-globecom.org/2009/>

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

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

8th International Information and Telecommunication Technologies Symposium I2TS 2009

Del 9 al 11 de desembre de 2009. Florianópolis, Santa Catarina State (Brasil)
<http://www.i2ts.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/>

The Second International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems (MPIS-2009)

Del 10 al 12 de desembre de 2009. Jeju Island (Corea)
<http://www.ftrg.org/MPIS2009/>

The 2009 International Conference on Information and Communications Security

Del 14 al 17 de desembre de 2009. Beijing (Xina)
<http://www.icics2009.org/>

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?opfi=on=com_content&view=article&id=2140&Itemid=188&lang=es

Incidents de seguretat relacionats amb la protecció de dades

Segons un estudi, el 98% de les empreses d'Amèrica Llatina exposen les seves dades confidencials (octubre 2009)

Segons un estudi realitzat per Mattica, laboratori d'anàlisi forense, el 98% de les empreses d'Amèrica Llatina consideren que, en formatar un equip informàtic, els arxius no es poden recuperar de cap manera. Això vol dir que no saben que l'única forma d'esborrar totalment les dades del disc dur és sobreescriure els arxius o destruir físicament el disc dur.

Segons el director d'investigacions digitals de Mattica, "és molt comú que, fins i tot en l'àmbit personal, formatem un equip i el venguem o regalem. Aquesta situació permet que algú amb coneixements de sistemes pugui recuperar la informació continguda en el disc, des de contrasenyes i dades personals fins a fotografies. Ara imaginem el que succeeix en una organització: bases de dades de clients, plans de vendes, etc".

Finalment, l'especialista va afirmar que "en la mesura que els alts comandaments de les organitzacions comptin amb un pla de destrucció controlada de mitjans, i siguin conscients que les dades rellevants no s'eliminen dels equips pel simple fet d'haver estat formatats i, per tant, poden caure en mans de criminals o tercers amb males intencions i, en definitiva, perjudicar l'organització, podem estar més a prop de protegir la privacitat".

Font: Mattica

Es publiquen contrasenyes de milers d'usuaris de Hotmail (octubre 2009)

Uns delinqüents van publicar en el lloc web pastebin.com les dades d'accés de més de 10.000 comptes de Windows Live. Encara que la llista va ser eliminada d'aquest lloc, la BBC afirma que encara n'hi ha còpies a Internet.

La llista està conformada solament per comptes de Hotmail, MSN i Live que comencen per les lletres A i B i, per tant, pot ser només una petita mostra de la base de dades creada pels delinqüents.

Encara no se sap amb seguretat com els delinqüents van poder recollir les dades, però és molt possible que hagi estat mitjançant atacs de pesca (*phishing*). Microsoft ha remarcat que aquest problema no és resultat de cap atac als seus sistemes i bases de dades.

Microsoft recomana als usuaris de Windows Live que canviïn les contrasenyes dels seus correus electrònics el més aviat possible i que canviïn les contrasenyes dels seus comptes cada dos mesos.

També és important que els internautes evitin utilitzar la mateixa contrasenya en diferents serveis. Si ho han fet així, haurien de canviar-les perquè els delinqüents podrien utilitzar-la per entrar en els comptes d'altres serveis, com per exemple Facebook.

Font: www.viruslist.com

T-Mobile i Microsoft admeten la pèrdua quasi segura de les dades personals dels usuaris de telèfons Sidekick (octubre 2009)

T-Mobile i Microsoft han confirmat que, després d'una sèrie de problemes d'accés al servei d'usuaris de dispositius Sidekick, uns telèfons mòbils bastant populars als Estats Units, és molt probable que aquests usuaris hagin perdut les seves dades personals, com contactes, notes, calendaris, fotografies, etc.

I és que, per increïble que pugui semblar, no hi havia una còpia de seguretat d'aquesta informació i, per tant, tots els usuaris que no tinguessin una còpia local dels seus Sidekicks no hi tenen res a fer.

Tot i que no s'ha confirmat, la hipòtesi és que tot va ser degut a una actualització dels sistemes d'emmagatzematge dels centres de procés de dades en què residia la informació de tots els usuaris del servei.

Font: www.lainformacion.com

Bulletí revisió vulnerabilitats

Servidor intermediari (*proxy*) anònims (navegació anònima?):

Els servidors intermediaris (*proxy*) s'utilitzen per gestionar l'accés a Internet en les empreses. És una eina de verificació i control, important per fer complir les polítiques, i se sol desplegar en la xarxa interna, en la zona de distensió o en ambdues zones. Els ports utilitzats normalment són 3128, 8080 i 80, però es pot utilitzar qualsevol port TCP. Dels productes que hi ha al mercat, els més coneguts són Squid i ISA, de Microsoft.

En molts països, l'ús d'un *proxy* obert pot ser considerat il·legal, de manera semblant a estar utilitzant l'ordinador d'una persona sense el seu coneixement. L'empresa / ordinador actua com a servidor intermediari obert pot incomplir algunes lleis, especialment si s'està utilitzant per propagar la pornografia infantil o en altres activitats criminals.

Nou tipus d'atac: *spear phishing*

És un tipus d'estafa que consisteix a enviar un correu electrònic al personal d'un àmbit corporatiu, on l'estafador suplanta la identitat d'algun dels membres de l'empresa per cometre el delictes. En el correu, es demanen noms d'usuaris, contrasenyes o qualsevol informació de caràcter confidencial, amb l'objectiu principal d'obtenir accés al sistema informàtic de l'empresa.

Top vulnerabilitats

Vulnerabilitats més consultades a la pàgina web d'INTECO.

[servei Server a Microsoft Windows \(CVE-2008-4250\)](#)

Gravetat: alta

Data de publicació: 23/10/2008

[mshtml.dll a Microsoft Internet Explorer \(CVE-2008-4844\)](#)

Gravetat: alta

Data de publicació: 11/12/2008

[fitxer blosxom.cgi a Blosxom \(CVE-2008-2236\)](#)

Gravetat: mitjana

Data de publicació: 03/10/2008

[gdiplus.dll a GDI+ \(CVE-2008-3015\)](#)

Gravetat: alta

Data de publicació: 10/09/2008

[Acces InstallShield Update Agent \(CVE-2008-1093\)](#)

Gravetat: alta

Data de publicació: 18/09/2008

[pkcs15-tool a OpenSC \(CVE-2008-3972\)](#)

Gravetat: mitjana

Data de publicació: 10/09/2008

[Defecte de configuració a Red Hat Enterprise IPA versió 1.0.0 i FreeIPA versions anteriors a 1.1.1 \(CVE-2008-3274\)](#)

Gravetat: alta

Data de publicació: 12/09/2008

[Desbordament de búfer basat en pila en Fedora Directory Server de Red Hat \(CVE-2008-2932\)](#)

Gravetat: alta

Data de publicació: 12/09/2008

Secció responsables de seguretat

Nom i cognoms
Ferran Martínez Ferrer

Lloc que ocupa
Director Àrea TIC

Des de quan
Gener de 2009

Entitat
Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI)

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

El Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI) és l'ens públic responsable de la direcció, planificació, gestió i control dels serveis d'informàtica i de les telecomunicacions de la Generalitat de Catalunya. El CTTI està adscrit al Departament de Governació i Administracions Públiques, a través de la Secretaria de Telecomunicacions i Societat de la Informació.

El meu àmbit d'actuació són els fitxers automatitzats dels quals el CTTI n'és responsable. Queden fora de la meua responsabilitat, per tant, tots aquells fitxers gestionats pel CTTI des de l'àmbit dels serveis centrals TIC i dels quals en són responsables els departaments i altres organismes de la Generalitat. En aquest sentit doncs, el meu àmbit de responsabilitat és el de qualsevol responsable d'una empresa o organisme, amb treballadors, proveïdors, clients, etc.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

No, com a director de l'Àrea TIC del CTTI, la de responsable de seguretat TIC LOPD només és

una més de les funcions que he de desenvolupar.

Cal dir, també, que no estic sol per desenvolupar la funció de responsable de seguretat LOPD. Per una banda, compto amb un equip que m'ajuda a fer la gestió TIC del CTTI i tot el que això comporta respecte de la LOPD, i, per l'altra, dins de l'organització LOPD del CTTI comptem amb un Grup de Treball LOPD, amb representació de totes les àrees. Aquest grup es reuneix periòdicament per fer el seguiment de tots els temes LOPD, on es distribueixen tasques i es consensuen i coordinen totes les actuacions.

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

Només fa uns mesos que he assumit el càrrec de director de l'Àrea TIC al CTTI i, per tant, també sóc relativament novell com a responsable de seguretat LOPD. La principal dificultat ha estat entendre exactament quin és l'abast de la llei i el reglament, i quines implicacions té la seva implantació en el dia a dia de la gestió TIC d'una organització. Realment són moltes i diverses, i sovint hi ha qüestions que cavalquen entre l'àmbit tècnic, l'organitzatiu i el jurídic i cal anar trobant solucions i compromisos contínuament.

En segon lloc, la sensibilització del personal. El CTTI, per la seva activitat, no és una organització que tracti dades especialment sensibles i, fora de les àrees de Recursos Humans, on la sensibilitat és elevada de forma generalitzada, en la resta d'àmbits costa explicar el per què de determinades mesures i controls, i és difícil mantenir el nivell d'atenció necessari.

Finalment, i suposo que és un aspecte comú per a tots aquells que no es dediquin en exclusiva al "càrrec", el dia a dia rabiós i els canvis continus fan que sigui difícil mantenir una planificació i mantenir permanentment actualitzada tota la documentació de processos i procediments de seguretat, que és molt àmplia. En aquest sentit, però, darrerament el CTTI ha signat un acord

marc de subministrament de llicències d'una eina per a la gestió de la LOPD (acord obert a tots els departaments i organismes de la Generalitat que hi estiguin interessats). Aquesta eina, actualment en fase d'implantació, ens suposarà una gran ajuda en la gestió del dia a dia de la LOPD, el seguiment de les accions a portar a terme, la inscripció / supressió i modificació de fitxers, el manteniment de tota la documentació i registres que la normativa requereix i el manteniment d'un quadre de comandament LOPD.

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

Des de la meua incorporació al càrrec, en el Grup de Treball LOPD s'ha fet una revisió de tots els procediments i documentació en general que requereix la normativa. Per tant, fins a aquest moment, aquesta ha estat la meua dedicació principal i encara ho serà durant un temps.

Un cop tancada aquesta fase de revisió, entenc que la meua principal dedicació consistirà a donar el suport necessari a qui ho requereixi dins la casa, per tal d'aplicar correctament les mesures de seguretat, donar suport a la formació i conscienciació en la matèria i mantenir permanentment actualitzats uns indicadors sobre el grau de compliment de la LOPD dels diferents fitxers automatitzats, a través del quadre de comandament LOPD.

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

A dia d'avui encara no ho he fet personalment, tot i que sí que hi ha contacte habitual entre el CTTI i l'APDCAT a través d'alguns dels membres del grup de treball del CTTI.

Enllacem amb...

<http://www.oecd.org/sti/securitevieprivee>

L'enllaç que hem triat aquest mes difereix una mica del que és habitual en aquesta secció. Si normalment dediquem unes línies a comentar un lloc web que té com a principal objectiu la seguretat de la informació, la privacitat o la protecció de dades, en aquesta ocasió us proposem la pàgina d'una organització que té una missió més general, però que també és molt sensible a les qüestions derivades de la privacitat i la protecció de dades de caràcter personal.

Es tracta de l'Organització per a la Cooperació i el Desenvolupament Econòmic, amb seu a París i coneguda per les seves sigles OCDE. Es va crear mitjançant una convenció internacional, l'any 1960, i actualment en formen part 30 països, entre els quals l'Estat espanyol. Tal i com la mateixa organització descriu, la seva missió és donar suport al creixement sostenible, impulsar l'ocupació, augmentar el nivell de vida, procurar l'estabilitat financera,

ajudar al desenvolupament econòmic dels països i contribuir al creixement del comerç mundial.

Les seves principals activitats són fer d'observatori i elaborar informes de situació o recomanacions, per a la qual cosa s'estructura en diferents àmbits de treball. Una d'aquestes àrees, la Direcció de Ciència, Tecnologia i Indústria, té una secció dedicada a "la seguretat de la informació i la protecció de la vida privada". És en aquesta part de la pàgina on trobarem informació d'interès en relació a la protecció de dades de caràcter personal, especialment en forma de publicacions i documents: directrius, bones pràctiques, anuals, recomanacions, informes, etc. Tots ells aborden en profunditat qüestions derivades de l'economia i el tractament de dades de caràcter personal.

La seva pàgina principal és <http://www.oecd.org>.

Sistema de gestió de la protecció de dades personal (SGPDP)

Ramon Miralles. Coordinador d'Auditoria i Seguretat de la Informació
Agència Catalana de Protecció de Dades

En el context de la seguretat de la informació, les propostes orientades a establir sistemes de gestió de la seguretat de la informació (SGSI) s'han materialitzat en normes estàndard de la indústria, de caràcter internacional, principalment les elaborades per l'Organització Internacional per a l'Estandardització, més coneguda per les seves sigles ISO. Amb la família de normes ISO/IEC 27000, algunes ja desenvolupades i altres en procés de desenvolupament, proporcionen un marc de gestió de la seguretat de la informació que té com a element clau el fet que la seva implantació passa per la definició d'un cicle PDCA (planificar, implantar, revisar i millorar), amb la mateixa orientació que els sistemes de gestió de la qualitat.

El grau de maduresa en la definició de com ha de ser un sistema de gestió de la seguretat de la informació ha permès que la implantació d'aquests sistemes de gestió es pugui certificar externament, segons la norma ISO 27001. Aquesta certificació pot ser un indicador clau que la manera en què es gestiona la seguretat de la informació en una organització ofereix uns alts graus de fiabilitat.

La ISO/IEC 27001, que té el seu origen en la BS 7799:2 (British Standard), incorpora a l'annex A de la norma, de forma resumida, els controls previstos a la ISO 27002; en total, són 39 objectius de control i 133 controls, agrupats en 11 dominis. Un d'aquests dominis és el de Compliment, que de forma genèrica obliga que el sistema de gestió de la seguretat de la informació prevegi tot el que calgui per complir els requisits legals que siguin d'aplicació al tractament de la informació, amb una referència específica a la protecció de dades i la privacitat de la informació personal (control 15.1.4).

Ara bé, certament el control previst en aquest estàndard ISO no diu gran cosa, més enllà de recordar l'obligació de complir amb la normativa legal vigent en matèria de protecció de dades o privacitat; concretament, a l'annex de la norma UNE-ISO/IEC 27001 (la ISO/IEC 27001 ha estat adoptada per AENOR com a norma espanyola) aquest control diu el següent:

“Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes”.

Altres organitzacions de caràcter internacional també dediquen esforços a crear marcs de treball o bé a establir directrius per a la gestió de sistemes d'informació –i, en general, de processos de negoci– que, a l'hora de tractar dades de caràcter personal, necessitin tenir en compte i complir requisits legals pel fet d'utilitzar informació de caràcter personal.

Tenim, per exemple, que tant l'Organització per a la Cooperació i el Desenvolupament Econòmic (OCDE), i en especial els treballs que realitza en el marc del Working Party on Information Security and Privacy (WPISP), com l'Asia-Pacific Economic Cooperation (APEC) dediquen recursos a estudiar i desenvolupar directrius i bones pràctiques, en el context dels mercats i les economies, en relació al tractament de les dades de caràcter personal i el respecte a la privacitat.

Quant a treballs específics que recullin propostes destinades a crear marcs de gestió de la privacitat o de la protec-

ció de dades, tenim d'una banda la ISO 29100. Aquesta norma encara és en procés de redacció, però en un dels seus capítols preveu la fase d'implantació de controls de privacitat en el sistema d'informació i tracta, especialment, sobre l'establiment d'un *privacy management system*.

En la redacció de juny de 2009 del document de treball de la futura ISO 29100.2, s'identifiquen una sèrie de consideracions clau a l'hora d'implantar un sistema de gestió de la privacitat (en la text de la ISO es fa referència a la PII *personally identifiable information*, que aquí hem traduït com a “informació de caràcter personal”):

Hi ha d'haver una política clara pel que fa a la recollida, ús, cessió, emmagatzemament, arxiu i disponibilitat de la informació de caràcter personal.

- La informació de caràcter personal tractada s'ha d'inventariar i classificar.
- Els procediments i controls relacionats amb el tractament de la informació de caràcter personal han d'estar d'acord amb els principis de privacitat.
- Hi ha d'haver un responsable de protecció de dades o una autoritat interna de control, amb funcions de “govern” de la privacitat a cada organització.
- S'han de preveure processos que permetin avaluar quin impacte poden tenir sobre la privacitat els tractaments de dades personals.
- S'han de preveure mecanismes que permetin tenir documentada l'activitat desenvolupada sobre la informació; en definitiva, la traçabilitat dels tractaments.
- I s'ha de preveure la formació necessària per a totes les persones que tenen accés a les dades personals, especialment en els aspectes relacionats amb les responsabilitats que assumeixen en relació al tractament de la informació de caràcter personal.

Actualment, el Comitè Europeu de Normalització (que elabora i publica les normes CEN) també està redactant documents que, sense tenir inicialment el rang de normes estàndard, sí que poden arribar a tenir un impacte important en relació a la gestió de la protecció de dades i la privacitat. Un exemple és la iniciativa Data Protection & Privacy Good Practices que, tot i estar també en fase document de treball (setembre de 2009), recull la conveniència d'implantar un *data protection management system* i fins i tot apunta que aquest sistema de gestió de la privacitat es pot arribar a utilitzar com una eina de màrqueting, en clau d'avantatge competitiu en els negocis.

Per últim, farem referència a un document que ens sembla d'especial interès de cara a la futura consolidació del sistema de gestió de la protecció de dades personals. Es tracta del British Standard publicat al maig de 2009, sota la denominació BS10012:2009 “Data protection – Specification for a personal information management system”. Tenint en compte que en matèria de tecnologies de la informació i la comunicació, i específicament en el sector de la seguretat de la informació, el British Standard sovint s'ha convertit en norma estàndard de caràcter internacional (habitualment sota el paraigües de la ISO), convé començar a tenir present la BS 10012.

El BS 10012 considera que un PIMS (*personal information management system*) és una part més de l'arquitectura de

govern de les organitzacions i, per tant, no es tracta d'una iniciativa aliena a les necessitats globals del negoci. L'estàndard proveeix d'un marc de treball orientat a mantenir i millorar tant el compliment de la legislació de protecció de dades com l'adopció d'unes bones pràctiques, en la gestió de la informació de caràcter personal.

En el cas britànic, el compliment normatiu es refereix a la seva legislació de protecció de dades, concretament "The Data Protection Act" de 1998 i els seus principis, tot i que el mateix text de l'estàndard recorda que és una transposició de la Directiva Europea 95/46/CE, com ho és també la nostra LOPD de l'any 1999.

L'estàndard aplica el cicle PDCA (*Plan-Do-Check-Act*), al qual ja ens hem referit en parlar dels SGSI, per determinar les especificacions que cal seguir en cada fase del cicle fins a considerar que es disposa d'un sistema de gestió de la protecció de dades personals conforme al BS 10012.

La secció 3 de l'estàndard identifica les especificacions de la fase de planejament del sistema de gestió de la protecció de dades personals (SGPDP). Per descomptat, l'element clau és que es tracta d'un pla documentat i que ha d'abordar qüestions tals com:

L'àmbit d'aplicació i objectius del SGPDP.

La política de gestió de les dades personals, que pot ser d'aplicació a tota o a una part de l'organització, i per descomptat ha de ser coneguda per tota l'organització.

Hi ha un detall de quines han de ser les qüestions mínimes que ha d'abordar aquesta política.

També s'han de determinar les responsabilitats i la implicació de la direcció en relació al SGPDP, així com la rendició de comptes.

La provisió de recursos per a la definició, implementació, operació i manteniment del SGPDP.

I les accions necessàries perquè el SGPDP formi part de la cultura de l'organització.

La secció 4 aborda la qüestió de la implantació i operació del SGPDP. Per raons òbvies, és la secció amb un major contingut. No és aquest el lloc per detallar totes les especificacions que conté, però en podem destacar la primera, que em sembla clau: el responsable de la gestió de la protecció de dades personals a l'organització ha de ser un membre de l'equip de direcció (*senior management team*), perfectament identificat.

La secció 5 es dedica a la monitorització i revisió del funcionament del SGPDP i, per tant, aborda principalment aspectes relacionats amb l'auditoria.

I per últim, la secció 6 aborda la fase de millora del cicle PDCA, on cal identificar les accions preventives i correctives, així com la manera en què es planteja la millora contínua del sistema de gestió, d'acord amb els resultats de la revisió del sistema realitzada a la fase anterior del cicle (*check*).

Finalment, com a exemple d'adopció d'aquests sistemes de gestió de la protecció de dades personals, voldria destacar el cas suís. La llei de protecció de dades suïssa preveu que es puguin establir certificacions relacionades amb el tractament de dades de caràcter personal i, com a compliment del que preveu la legislació suïssa, al gener de 2008 va entrar en vigor un decret federal sobre certificacions en matèria de protecció de dades.

L'article 4 del decret federal esmentat identifica com a possible objecte de certificació el que anomenen *systeme de gestion de la protection des données*. Com a conseqüència d'aquest decret, al juliol de 2008 l'autoritat federal de protecció de dades suïssa va publicar unes "Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir".

El cert és que les exigències es centren fonamentalment en aspectes de seguretat, tot i que no exclusivament, de manera que al text hi ha una forta remissió a la ISO 27001 i es detalla com es pot sincronitzar aquesta ISO amb les obligacions de la llei de protecció de dades suïssa, quan es vol certificar el SGPDP d'una organització.

Sembla, doncs, que un dels camins a mitjà termini serà alinear el compliment normatiu en matèria de protecció de dades amb les necessitats de l'activitat de les entitats públiques i privades, una alineació basada en models de millora contínua acceptats a nivell internacional. En tot cas, cal desterrar la idea que la protecció de dades suposa un fre o una barrera al normal desenvolupament dels negocis o del serveis públics, ja que, ben al contrari, s'ha de considerar un element clau, integrat en la cultura de les organitzacions i que aporta eficàcia i eficiència.

Ramon Miralles

Creació del Data Privacy Institute (DPI)

Recentment s'ha creat el Data Privacy Institute (DPI), un organisme que neix amb l'objectiu de convertir-se en fundació i que es centrarà a tractar temes vinculats amb la privacitat i la protecció de dades. Aquesta entitat ha sorgit a instància de qui avui n'és el director, Antoni Bosch, un professional històricament molt vinculat a aquest segment de la protecció.

Entre les activitats a organitzar, Bosch, professor de la Universitat Autònoma de Barcelona, ha explicat que aviat es presentaran iniciatives molt concretes per oferir una formació d'alt nivell dirigida als futurs *Data Privacy Officers*, una figura professional que creixerà a Espanya per la necessitat creixent de les empreses. Aquestes iniciatives consistiran en formació de postgrau, seminaris i jornades sobre privacitat, així com una futura certificació, actualment inexistent al nostre país, específica per al personal dedicat a la privacitat.

En l'acte de presentació oficial hi va intervenir el director de l'Agència Espanyola de Protecció de Dades (AEPD), Artemi Rallo, qui va donar suport a aquesta iniciativa i va impartir una conferència inaugural titulada "Hacia un estándar de privacidad".