

Destaquem... el sistema de videovigilància



Durant els mesos de març i abril, l'Agència ha organitzat a Barcelona, Girona, Tarragona i Lleida jornades de presentació de la seva [Instrucció 1/2009 sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància](#), publicada al febrer de 2009.

La convergència de diferents tecnologies a l'entorn de la funcionalitat de control i vigilància, com ara les telecomunicacions, les xarxes IP, les bases de dades, la biometria o les tecnologies de geoposicionament, totes elles amb possibilitats d'integració en els sistemes de videovigilància, amplien considerablement la capacitat de control.

Aquesta major complexitat tecnològica comporta un augment dels riscos i, per tant, cal que les mesures de seguretat també siguin presents en el disseny del sistema de videovigilància. La Instrucció 1/2009, en incloure l'obligació d'elaborar una memòria del sistema de videovigilància, en la qual tenen rellevància especial les característiques tècniques del sistema i les mesures de seguretat aplicades, planteja un instrument preventiu que ha de facilitar la tasca dels tècnics a l'hora de protegir convenientment els sistemes.

El cicle de gestió de la informació audiovisual dels sistemes de videocontrol es divideix en 4 fases: fase de captació, de transport, d'emmagatzemament i d'anàlisi. En cadascuna d'elles, caldrà avaluar i definir els millors mecanismes de protecció de la informació.

Continguts

Destaquem...	1
Parlem de...	1
Vulnerabilitats de seguretat	2
Tecnologia i protecció de dades	2
Incidents de seguretat	3
Responsables de seguretat	4
Enllacem amb...	5
On anar...	6
La privacitat dissenyada, com a instrument preventiu en la gestió de la informació de caràcter personal	7

Parlem de... la privacitat dissenyada, com a instrument preventiu en la gestió de la informació de caràcter personal

L'Agència Catalana de Protecció de Dades té com a línia estratègica d'actuació el suport a totes aquelles iniciatives i solucions que, a l'entorn de la gestió d'informació de caràcter personal, aportin elements preventius. Això, en contraposició als plantejaments on les qüestions de privacitat i seguretat de la informació s'incorporen de forma accessòria, és a dir una vegada les solucions de gestió de la informació ja han estat dissenyades, o fins i tot construïdes.

La prevenció en matèria de protecció de dades de caràcter personal resulta especialment rellevant i útil quan les dades objecte de tractament són sensibles, o bé les necessitats d'exploració de la informació impliquen compartir i intercanviar informació amb d'altres sistemes d'informació.

+info



Revisió de vulnerabilitats de seguretat

Conficker

Segons les dades recollides per Kaspersky Security Network (KSN), el virus informàtic Conficker es va mantenir durant el mes de març en la primera posició del rànquing de deteccions de virus, i ja és el programa maliciós més important des de principis de 2009.

El cuc Conficker va començar a propagar-se al novembre de 2008, aprofitant una vulnerabilitat crítica de Microsoft, ja corregida, i ràpidament ha assolit alts nivells de detecció a causa de la manca d'actualització del sistema operatiu dels usuaris. Després, es van anar propagant noves variants amb mètodes d'infecció diferents, com l'ús de recursos compartits i de fitxers *autorun* per a dispositius d'emmagatzematge extraïbles, entre d'altres.

Waledac

Durant el mes de març, també van aparèixer noves variants del troià Waledac. Aquest *malware* es difon a

través de correus electrònics considerats correu brossa, que simulen ser notícies enviades per la prestigiosa agència de notícies Reuters sobre una explosió en diferents ciutats del món.

Aquest troià havia aparegut durant el mes de febrer passat, en forma de postals falses amb motiu del dia dels enamorats, i ara està utilitzant aquest nou missatge d'enginyeria social per fer que els usuaris vegin un suposat vídeo de l'explosió. En realitat, però, acaben descarregant el programari maliciós.

Els creadors de *malware* han 'redescobert' la propagació del programari maliciós per mitjans extraïbles, com les memòries USB. A més, a finals de març va aparèixer una nova tècnica d'atac que, per primera vegada, va infectar encaminadors (*routers*) i mòdems amb plataformes Linux. Es demostra, així, que avui dia l'espectre de plataformes i dispositius que poden ser infectats es continua ampliant, gràcies a la professionalització dels creadors de programari maliciós.

Clickjacking: una amenaça creixent a Internet

A les amenaces ja conegudes pels internautes, com el correu brossa, la pesca informàtica (*phishing*), els troians, etc., se n'hi suma una de nova que comença a tenir una gran incidència: el *clickjacking*. Aquesta pràctica consisteix a enganyar l'internauta perquè premi un determinat botó o l'enllaç d'una pàgina d'aparença legal; d'aquesta manera, aprofitant una vulnerabilitat del navegador que utilitza javascript, plugins o ActiveX, el que realment es fa és donar via lliure perquè tercers controlin i infectin l'ordinador.

Com a mesures de protecció, hem de tenir actualitzat el nostre sistema operatiu i, sobretot, el navegador que utilitzem. El més aconsellable és utilitzar un navegador que no executi aplicacions javascript, encara que enfront d'aquesta opció hi ha navegadors, com Firefox, que disposen d'opcions extra per evitar l'engany del *clickjacking*.

Tecnologia i protecció de dades

MILLORA LA PRIVACITAT A FACEBOOK

IBM ha llançat al mercat una aplicació que ajuda els usuaris de Facebook a configurar polítiques de seguretat més fortes, amb la finalitat de garantir la seva intimitat. Es tracta de la primera aplicació per a Facebook Marketplace (on els usuaris compren i venen) i s'utilitzarà per recopilar dades sobre les preferències d'intimitat dels usuaris.

L'eina s'anomena Privacy-aware Marketplace i permet als usuaris de Facebook comparar les seves preferències d'intimitat amb el nivell recomanat. A més, suggereix canvis a l'usuari.

L'aplicació podria permetre als usuaris, en un futur i de manera eventual, vincular les seves preferències de privacitat a totes les pàgines web on es comparteixi informació. Així mateix, les empreses podrien utilitzar aquesta informació per controlar la informació que comparteixen amb els clients.

Més informació <http://www.idg.es/pcworld/Mejora-la-privacidad-en-Facebook/doc78068-seguridad.htm>.



Incidents de seguretat relacionats amb dades personals

Una fallada de seguretat a Google Docs permet accedir als documents de manera no autoritzada (març 2009)

Google va confirmar la fallada de seguretat descoberta per una empresa holandesa en el servei de Google Docs. El problema es produïa quan un usuari seleccionava diversos documents alhora, per modificar-ne els permisos d'accés, i a partir d'aquell moment el servei compartia tots els documents que només tenien accés de lectura.

A banda de corregir aquesta fallada de seguretat, Google va enviar un missatge d'avís a tots els usuaris afectats.

Detingut un pirata informàtic que va accedir als ordinadors de més de 1.000 persones (març 2009)

Les Forces i Cossos de Seguretat van detenir un *cracker* que havia vulnerat la seguretat electrònica de més de 1.000 persones, entre les quals hi ha polítics, periodistes, escriptors, grups de professionals de la comunicació, metges i bufets d'advocats.

El detingut va ser capaç de vulnerar la seguretat d'ordinadors connectats a Internet, d'on va extreure claus d'accés a comptes de correu electrònic, als quals va accedir després per buscar informació sensible de les víctimes. El pirata, a més, tenia quaderns amb dades sobre les víctimes, relatives a comptes de correu electrònic, contrasenyes, números de compte bancari, números de targetes amb el PIN, etc.

Un troià s'oculta darrere d'un vídeo per robar claus bancàries (març 2009)

PandaLabs, el laboratori de detecció i anàlisi de programari maliciós (*malware*) de Panda Security, ha avisat sobre l'aparició d'un troià anomenat Nabload.DLU. Aquest troià es fa passar per un vídeo divertit, que enganya l'usuari mentre un codi maliciós, encarregat de robar contrasenyes de banca en línia, es descarrega a l'equip.

Els troians són el principal mètode usat pels ciberdelinqüents per obtenir dades privades dels usuaris. Segons un estudi de PandaLabs, durant el 2008 més d'11 milions de persones a tot el món van ser víctimes d'un robatori d'identitat.



Secció responsables de seguretat

Nom i cognoms
Fernando Marín Gurrea

Lloc que ocupa
Cap de l'Àrea de Seguretat i Anàlisi de la Informació

Entitat
Departament d'Interior, Relacions Institucionals i Participació

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

El Departament d'Interior, Relacions Institucionals i Participació ha impulsat un Programa d'Anàlisi i Seguretat de la Informació (PASI), per donar resposta, de manera transversal i per a totes les unitats que componen el Departament, a les peticions que tinguin i calguin per a la seguretat i l'explotació de la seva informació. Ha de permetre identificar i donar suport a la posada en marxa de totes aquelles iniciatives necessàries per al procés de transformació que comporta l'avenç cap a un nou model.

Dins del Departament som una àrea responsable de la gestió de les dades, molt lligada a un àmbit de negoci i diferenciats de l'Àrea TIC, i treballem alineats i en consonància tant amb el CATCert i el CTTI com amb l'APDCAT.

En definitiva, el que pretenem és exercir el rol de responsable de seguretat en els projectes que afectin els sistemes d'informació, aprovar plans de contingència i continuïtat de negoci dels sistemes d'informació del Departament, definir polítiques de seguretat per a la recollida, accés i comunicació de la informació i garantir en tot moment el marc legal vigent. L'òrgan del Programa d'Anàlisi i Seguretat de la Informació ofereix, transversalment a totes les unitats del Departament, models i eines per donar resposta a les peticions que les unitats esmentades facin quant a la seguretat i l'explotació de la informació.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

No. El Programa d'Anàlisi i Seguretat de la Informació que dirigeixo es focalitza en dos grans àmbits d'actuació, que determinen dues subestructures relacionades:

Per una banda, hi ha l'Oficina de Seguretat de la Informació, que està enfocada a la coordinació i participació en tots aquells projectes del Departament en els quals el tractament de la informació faci necessari establir procediments de control, tant per garantir els principis de confidencialitat i disponibilitat de les dades com per a l'acompliment de la LOPD. En aquest moment, hem endegat un Pla Director de Seguretat que segur que ens donarà molta feina, però que ha de ser el full de ruta de les principals actuacions en l'àmbit de la seguretat en el Departament.

Per altra banda, però, el Programa està format per l'Àrea d'explotació de dades, que pretén la integració de diferents sistemes d'informació perquè l'explotació es faci amb totes les garanties legals necessàries.

A fi de garantir l'alineament entre les actuacions de les dues unitats, fixar un model de gestió únic i compartit i establir la relació amb la resta d'unitats del Departament, el PASI disposa també de la Unitat de Suport a la Intel·ligència de Negoci, que creiem que té un valor diferencial en el Programa. En aquest sentit, aquesta unitat farà actuacions en matèria de vigilància competitiva i actuarà com a observatori, dins l'àmbit del PASI, en matèria de seguretat i explotació de la informació.

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

Per la sensibilitat de les dades que tracta el Departament, ja siguin les relatives a les emergències, les policials o de seguretat, o bé aquelles referents a protecció civil, ens trobem davant de problemes diferents en cada moment.

Cada unitat del Departament està dotada de formes de treball molt consolidades, que fa que en un primer moment es mostrin poc receptives a l'hora d'incorporar canvis, fins i tot si els suposen avantatges en el tractament de les dades. No obstant això, una vegada han pogut veure els beneficis que el nou model de gestió que volem posar en marxa els



pot proporcionar, no trobem impediments per definir els processos de seguretat de la informació i els controls que sigui necessari establir.

En aquesta línia, dins del Programa hem definit el Comitè de Seguretat i Anàlisi de la Informació, com un òrgan de representació de totes les direccions generals i els organismes del Departament, així com de les unitats transversals. El Comitè tindrà la responsabilitat d'aprovar, impulsar i comunicar a l'organització les polítiques i projectes relacionats amb la seguretat i la explotació de les dades dels sistemes d'informació del Departament.

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

Actualment, i sens dubte, el desplegament del PASI. El Programa es centra, bàsicament, en quatre punts: la posada en marxa de la cartera de serveis; la realització d'auditories, controls de seguretat i compliment legal; la implantació d'una eina per integrar diferents bases de dades, agilitant el tractament de grans volums d'informació, i la creació d'un dipòsit corporatiu. Això, a banda d'una de les grans tasques en aquest àmbit dins de qualsevol organització, que és la gestió del canvi i la implantació d'una cultura de seguretat.

El desplegament d'aquest programa, molt intens quant al tractament de dades, inclou molt sovint dades de caràcter personal. Per això, cal una actitud proactiva de vigilància, a fi d'assolir els objectius estratègics i complir, alhora, amb els preceptes relatius a la protecció de dades que, en definitiva, són drets fonamentals dels ciutadans.

Amb això, aconseguim dirigir i englobar sota el mateix paraigües iniciatives que condueixen a la millora de la gestió en els diferents àmbits del Departament, en el manteniment de les dades i la seva explotació. D'aquesta manera, volem aconseguir posar a disposició de les estructures directives i operatives del Departament la major i millor quantitat d'informació estructurada, així com les polítiques de seguretat més adients per a la recollida, accés i comunicació de la informació, alineades amb el que estableix la LOPD.

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

Estem en contacte permanent amb l'APDCAT, ja que la naturalesa de les dades del Departament fa que ens calguin totes les propostes i aportacions que l'APDCAT pugui aportar.

Val a dir que l'Agència sempre ha mostrat una actitud de total col·laboració amb nosaltres, que ens ha estat molt útil a l'hora de posar en marxa i dur a terme els nostres projectes. Actualment, pretenem establir-hi una col·laboració més estreta, per poder definir un model de treball conjunt que es centri, bàsicament, en la prevenció i en l'auditoria prèvia.

Des d'aquí, aprofito per felicitar l'APDCAT per aquesta iniciativa de comunicació entre responsables de seguretat de l'Administració. Crec que és necessari un fòrum d'aquest tipus per posar en comú experiències i projectes, aprofitant bones pràctiques i compartint aspectes de millora apresos.

Enllacem amb... <http://www.inteco.es>

L'Institut Nacional de Tecnologies de la Comunicació (INTECO) és una iniciativa del Ministeri d'Indústria, Turisme i Comerç que, segons la seva pròpia definició, constitueix una plataforma per al desenvolupament de la societat del coneixement. Amb aquesta finalitat, defineix i desenvolupa iniciatives de seguretat tecnològica, accessibilitat i inclusió en la societat digital, així com solucions de comunicació per a particulars i empreses.

En l'àmbit de la seguretat de la informació, actualment desenvolupa 3 programes: el del Centre de Resposta a Incidentes en Tecnologies de la Informació per a Pimes i Ciutadans; l'Observatori de la Seguretat de la Informació; i el Centre Demostrador de Seguretat per a la PIME.

De la seva pàgina a Internet, té una rellevància especial la publicació dels informes, estudis i guies de l'Observatori de la Seguretat de la Informació, que tracten tot tipus de qüestions: l'ús de les tecnologies per part dels menors; guies per protegir les xarxes sense fils domèstiques; estudis sobre la situació de la seguretat en diferents sectors; guies d'adequació de la LOPD; guies per utilitzar de forma segura els telèfons mòbils, etc.



On anar...

Congressos i esdeveniments

International Workshop on Coding and Cryptography

Del 10 al 15 de maig de 2009. Ullensvang (Noruega)
<http://wcc2009.org/>

IEEE Symposium on Security & Privacy

Del 17 al 20 de maig de 2009. Oakland, California (EUA)
<http://oakland09.cs.virginia.edu/>

24th IFIP International Information Security Conference (SEC 2009)

Del 18 al 20 de maig de 2009. Pafos (Xipre)
<http://www.sec2009.org/>

International Workshop on Coding and Cryptology (IWCC2009)

De l'1 al 5 de juny de 2009. Zhangjiajie (Xina)
<http://www.iwcc2009.com/>

7th International Conference on Applied Cryptography and Network Security (ACNS'09)

Del 2 al 5 de juny de 2009. París (França)
<http://acns09.di.ens.fr/>

11th Information Hiding (IH'09)

Del 7 al 10 de juny de 2009. Darmstadt (Alemanya)
<http://www.ih09.tu-darmstadt.de/>

SegurYnfo 2009

18 i 19 de juny de 2009. La Paz (Bolívia)
<http://www.segurinfo.com.bo/>

3rd International Conference on Information Security and Assurance (ISA-09)

Del 25 al 27 de juny de 2009. Seül (República de Corea)
<http://www.sersc.org/ISA2009/index.php>

21st Annual FIRST Conference, AFTERMATH: Crafts and Lessons of Incident Recovery

Del 28 de juny al 3 de juliol. Kyoto (Japó)
<http://conference.first.org/>

Workshop on RFID Security 2009 (RFIDsec09)

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

14th Australasian Conference on Information Security and Privacy (ACISP 2009)

De l'1 al 3 de juliol de 2009. Brisbane (Austràlia)
<http://conf.isi.qut.edu.au/acisp2009/>

Western European Workshop on Research in Cryptology 2009 (WEWoRC 2009)

Del 7 al 9 de juliol de 2009. Graz (Àustria)
<http://events.iaik.tugraz.at/weworc09/>

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

Del 13 al 16 de juliol de 2009. Orlando, Florida (EUA)
<http://www.promoteresearch.org/2009/isp/index.html>

Second International Conference on the Applications of Digital Information and Web Technologies

Del 4 al 6 d'agost de 2009. Londres (Gran Bretanya)
<http://www.dirf.org/diwt2009/>

Fourth Joint Workshop on Information Security (JWIS 2009)

6 i 7 d'agost de 2009. Kaohsiung (Taiwan)
<http://jwis2009.nsysu.edu.tw/index.php/jwis/jwis2009>

18th USENIX Security Symposium (Security '09)

Del 10 al 14 d'agost de 2009. Montreal (Canadà)
<http://www.usenix.org/events/sec09/index.html>

The 10th International Workshop on Information Security Applications (WISA 2009)

Del 25 al 27 d'agost. Busan (República de Corea)
<http://www.wisa.or.kr/>

IEEE International Conference on Privacy, Security, Risk, and Trust 2009 (PASSAT-09)

Del 29 al 31 d'agost de 2009. Vancouver (Canadà)
<http://cse.sfx.ca/~passat09/>

Cursos de postgrau i especialitat en seguretat de la informació

Activitats criptogràfiques 2009. Programa de postgrau

Universitat Autònoma de Madrid (UAM)
http://www.uam.es/personal_pdi/ciencias/engonz/docencia/0809/cripto/minicursos09.html

Seminari "Seguridad en redes sociales: ¿están nuestros datos protegidos?"

Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información
Universitat Politècnica de Madrid
<http://www.euit.upm.es/uploaded/eventos/eventos/TripticoSeminarioRedesSociales2009.pdf>



La privacitat dissenyada com a instrument preventiu en la gestió de la informació de caràcter personal

« ...
incorporant
elements de
seguretat i
privacitat al
disseny de
les solucions
de gestió de
la informació
personal. »

L'Agència treballa en la identificació i l'anàlisi de propostes innovadores que afavoreixin la prevenció. Com a primer resultat dels treballs realitzats, hem fet una aproximació a un primer model teòric que va més enllà del compliment del marc normatiu, que aglutina propostes i solucions aportades pel mercat i pels investigadors en l'àmbit internacional.

El model de privacitat dissenyada que proposa l'Agència es basa en el concepte de «*privacy by design*». Es tracta d'una proposta aglutinadora, que pot ser clau per prevenir i tractar les qüestions derivades de la privacitat i la protecció de dades personals, incorporant elements de seguretat i privacitat al disseny de les solucions de gestió de la informació personal.

Una de les tasques de l'Agència ha estat donar estructura a aquest model, amb una visió absolutament pragmàtica, de manera que les organitzacions que tracten informació de caràcter personal, tant del sector públic com del privat, el puguin aplicar amb facilitat.

« ... totes
tres
qüestions
(processos,
organització
i tecnologia)
tenen una
incidència
directa en la
gestió de la
informació de
caràcter
personal. »

En síntesi, la proposta de l'Agència planteja explotar el concepte de «*privacy by design*», que implica incloure solucions de seguretat i privacitat en el moment de dissenyar els projectes. Això significa afegir nous processos comuns a tota l'organització, definir estructures organitzatives que dissenyin, implantin i controlin l'aplicació dels criteris de privacitat i/o seguretat, i tenir-ho també en compte al seleccionar la tecnologia utilitzada per tractar la informació; totes tres qüestions (processos, organització i tecnologia) tenen una incidència directa en la gestió de la informació de caràcter personal.

Pel que fa als procediments, algunes de les solucions que permeten incorporar una privacitat dissenyada són:

- **Avaluació de l'impacte sobre la privacitat (*Privacy Impact Assessment – PIA*):** és un procés per determinar els efectes dels programes d'actuació i de la prestació de serveis públics sobre la privacitat de les persones. El PIA és una metodologia útil per garantir, ja des de l'inici, que tot nou programa o servei es construirà respectant els principis de privacitat i, alhora, garantir a l'opinió pública que la seva privacitat està salvaguardada.
- **Mecanismes de millora de la informació que es proporciona a les persones afectades sobre els tractaments (*Fair Processing Notifications – FPN* i *Multilayered Privacy Notice*):** Això és, dissenyar polítiques informatives comprensibles i coherents sobre els tractaments de dades personals; en definitiva, simplicitat i transparència.
- **Gestió de les opcions i preferències de privacitat dels usuaris (*Customer Preference and Choice – CPC*):** és a dir disposar de mecanismes per conèixer i gestionar les diferents opcions relacionades amb el tractament de les dades personals que tria cada persona.
- **La seguretat dissenyada entorn a les dades i els usuaris que les tracten (*Information-Centric Security*):** No és altra cosa que una orientació tècnica de com dissenyar l'arquitectura de seguretat dels sistemes, que es pot plantejar de fora cap endins, o bé de dins cap enfora. En aquest cas, es planteja que el més important es protegir la informació.



Quant a solucions relacionades amb el disseny de l'organització, tenim figures organitzatives com:

- El responsable de protecció de dades o *data protection officer* – DPO, segons la nomenclatura anglosaxona, que seria una adaptació de la figura de l'SPOC (*single point of contact*) d'ITIL. Amb el DPO, totes les qüestions relacionades amb els tractaments de dades de caràcter personal passen per una persona especialitzada en la matèria, que aglutina coneixements i característiques de perfils jurídics, tecnològics i d'organització.
- El responsable de seguretat: encarregat de coordinar la implantació de les mesures de seguretat i de controlar-ne l'eficàcia.
- L'existència de departaments d'auditoria facilita una revisió continuada que els processos es realitzen segons el previst i que, per tant, donen els resultats esperats. L'activitat d'auditoria permet detectar deficiències en els sistemes i proveir-los dels mecanismes correctius.
- El comitès de seguretat permeten prendre decisions relacionades amb la seguretat amb la participació de les àrees clau de les organitzacions, de manera que les decisions no solament estiguin suficientment consensuades, sinó que tota l'organització s'involucri en les decisions preses i les faci seves. Els comitès requereixen la participació i el suport dels nivells directius de les entitats, a fi de donar la major força possible a les seves decisions.

I, per últim, la implantació de les solucions tecnològiques, en triar aquelles que aportin valor afegit per tractar la informació tenint en compte els requeriments derivats de l'ús d'informació de caràcter personal. Així tenim, per exemple:

- Les tecnologies orientades a reforçar la privacitat (*Privacy Enhancement Technologies* - PET), un concepte que aglutina aquelles solucions de mercat que inclouen entre les seves prestacions elements especialment sensibles amb la privacitat (anonimat, dissociació d'informació, auditoria, xifrat, metadades, etc).
- Les tecnologies i solucions que porten activades les opcions de privacitat per defecte (*privacy by default*), enfront d'aquelles solucions que parteixen de l'accés a tota la informació i en les quals cal anar limitant els nivells de difusió de la informació de caràcter personal.
- Tecnologies per detectar i prevenir transmissions no autoritzades d'informació, fora de les organitzacions (*Data Loss Prevention* - DLP), que permeten controlar els fluxos d'informació i els mecanismes de transport i emmagatzemament de la informació, fins i tot a nivell físic. D'aquesta manera, es minimitza el risc de pèrdua o fuga d'informació.

«... "privacy by design, és una de les apostes clau de l'APDCAT per abordar d'una manera eficient i eficaç la prevenció en matèria de protecció de dades de caràcter personal.»

Ramon Miralles.
Coordinador
d'auditoria i
seguretat de la
informació.
APDCAT.

Tot aquest conjunt de solucions o propostes, englobades sota el concepte de "privacy by design, és una de les apostes clau de l'APDCAT per abordar d'una manera eficient i eficaç la prevenció en matèria de protecció de dades de caràcter personal. Òbviament, no totes les propostes són adients per a totes les organitzacions: cal adoptar aquelles que resulten útils i proporcionades, d'acord amb les necessitats i particularitats de cada organització i dels tractaments que tenen sota la seva responsabilitat.