

Destaquem... 5 números del +Kdades



El +Kdades marxarà de vacances a l'agost i, per tant, el proper número us arribarà a finals de setembre. Ens ha semblat que aquest interval era un bon moment per valorar què hem fet en aquests primers 5 mesos de vida del nostre butlletí.

En edicions anteriors, hem procurat parlar de temes que poguessin ser del vostre interès i que, a la vegada, aportessin algun valor afegit a la informació que podeu trobar en altres fonts, en relació als aspectes tècnics de la protecció de dades de caràcter personal.

Hem tractat l'ús de metadades en l'intercanvi d'informació de caràcter personal; també vam abordar la interpretació que fa l'Agència de la privacitat dissenyada, una qüestió de la qual sens dubte sentirem a parlar en l'àmbit internacional en els propers mesos; hem parlat de l'anàlisi de riscos, que va ser el tema central de debat de les jornades de dades i tecnologia (DAT2009) organitzades per l'Agència, i també vam dedicar un espai a la destrucció del paper. En aquest número, parlem dels responsables de protecció de dades a les organitzacions, una figura que ens sembla clau per a una gestió eficaç dels assumptes relacionats amb la protecció de dades de caràcter personal.

Hem intentat triar temes diversos que, juntament amb la resta de continguts del butlletí, pretenen mantenir l'interès dels nostres lectors. I sembla que ho hem aconseguit, ja que en aquests moments el butlletí té més de 900 usuaris fidels, que mensualment el descarreguen del portal de l'Agència. Sens dubte això ens anima a seguir amb la tasca de difondre continguts tecnològics relacionats amb la protecció de dades de caràcter personal.

Fins al setembre i bones vacances.

Parlem... del responsable de protecció de dades (DPO)

La Llei orgànica de protecció de dades estableix un conjunt de principis i garanties per tal de protegir el dret a la protecció de dades personals.

Aquests principis i garanties requereixen que els responsables de fitxer i, si és el cas, els encarregats del tractament, realitzin una sèrie d'accions a fi de tractar correctament les dades personals que necessiten per desenvolupar les seves funcions, competències o per assolir el seu objecte social. Així, per exemple, cal que compleixin amb el principi de qualitat de les dades, amb el de finalitat, que facilitin el dret d'informació en el moment de la recollida de les dades i, si cal, n'obtinguin el consentiment, legitimin les cessions de dades, creïn i inscrivin els fitxers i, en tot cas, implantin les mesures de seguretat tècniques i organitzatives necessàries segons el tipus de dades personals tractades.

+info

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
El responsable de protecció de dades (Data Protection Officer)	8

1



Revisió de vulnerabilitats de seguretat

Un altre "0 day" a Microsoft... a través de Microsoft Office Web Component

Per sorpresa, Microsoft ha publicat que s'estan detectant atacs contra Microsoft Office Web Components a través d'Internet Explorer, que permeten l'execució de codi. Aquest és el tercer "0 day" de Microsoft (tots amb ActiveX) en un mes i mig.

Microsoft Office Web Components és una col·lecció de controls COMSA (Component Object Model) que s'utilitza per publicar contingut d'Office a la web, a través d'Internet Explorer. En poques paraules, un ActiveX.

En aquest control hi ha un error que permet a un atacant executar codi arbitrari, si la víctima visita una web especialment manipulada. El programari afectat és el següent:

- * Microsoft Office XP Service Pack 3
- * Microsoft Office 2003 Service Pack 3

Amb això, Microsoft acumula tres "0 day" sense solució. No es recordava una activitat semblant des de l'estiu de 2006. Llavors, els atacants es van capficar amb l'Office. En aquell moment es van popularitzar les amenaces directes i personalitzades contra companyies que rebien aquest intent d'infecció. Es tractava d'atacs perpetrats especialment contra ells. Es van descobrir una mitjana de dues vulnerabilitats per mes, durant

juliol i agost, a Word, Excel o PowerPoint. A més, es van detectar sempre els atacs molt poc temps després del segon dimarts de cada mes, per la qual cosa normalment va caldre esperar quasi tot un mes perquè Microsoft complís el seu següent cicle d'actualitzacions i poder estar protegit. Es va observar llavors un canvi clar de tendència en la forma en què van aparèixer aquests problemes, unida a una obsessiva i oportunista fixació contra aquest programari de Microsoft.

El SANS Internet Institute va pujar l'índex de gravetat mundial al Centre d'Infocon a groc, durant 24 hores, per augmentar la consciència de l'explotació activa d'aquesta vulnerabilitat. La intenció de la Infocon és reflectir els canvis en el trànsit maliciós i la possibilitat de connexió interrompuda.

Tots els hosts connectats a Internet estan exposats a certa quantitat de trànsit causats pels cucs i virus. Tanmateix, una vegada un cuc ha estat identificat i el nombre de màquines infectades ja no està en augment, aquest trànsit no és susceptible de provocar cap trastorn.

<http://isc.sans.org/diary.html?storyid=6778>

Onada d'atacs a Corea del Sud

Tal com era d'esperar, Corea del Sud va patir una tercera onada d'atacs fa unes setmanes, quan en els ordinadors infectats pel programari maliciós es va

reactivar en un enorme *botnet*, que va llançar atacs contra el govern, la banca i els llocs dels mitjans de comunicació, segons nous informes.

Segons el *Washington Post*, els atacs de la denegació de servei distribuït (DDoS) estaven molt més estesos que a la primera onada prevista. A causa dels atacs, al voltant de mitja dotzena de llocs del govern, inclosos els parlamentaris, el Ministeri de Defensa i el Ministeri de Relacions Exteriors, van veure alentida o temporalment aturada la feina.

La causa dels atemptats ha estat una vegada més *MyDoom*, que converteix els PC en ordinadors zombi capaços de llançar un atac coordinat de DDoS en qualssevol llocs seleccionats pels pirates informàtics.

La Comissió de Comunicacions de Corea (KCC) creu que, tot i que la ubicació dels pirates és desconeguda, els responsables de l'onada poden ser nord-coreans i els atacs poden tenir l'origen a Alemanya, Àustria, Geòrgia, els EUA i Corea del Sud.



Tecnologia i protecció de dades

Toshiba llança el primer disc dur portàtil amb xifrat de dades

Toshiba posa al mercat els primers discs durs externs portàtils amb sistema d'accés basat en tecnologia de xifrat. Aquests dispositius componen la gama Stor.e Art, que es caracteritza per combinar un disseny atractiu amb els últims avenços tecnològics de seguretat i protecció de dades davant de robatoris, accessos no autoritzats i fallades informàtiques.

Stor.e Art també inclou un nou sistema per simplificar les còpies de seguretat, gràcies a l'aplicació NTI BackupNow, EZ. Aquest programa permet fer una còpia de seguretat de tot el sistema amb un sol clic, i fins i tot restaurar-lo si Windows no pogués iniciar-se. Una altra funcionalitat és oferir recomanacions personalitzades a cada usuari, per tal de millorar la cobertura per a totes les seves dades, arxius o carpetes.

Aquests nous discs s'han desenvolupat per al seu ús diari en moviment. Per això, per evitar danys en el disc davant moviments bruscs se'ls ha dotat amb un sensor antixoc, tecnologia RAMP-LOADING i una carcassa antilliscant que ajuda a fixar el disc en qualsevol superfície. Un altre sistema d'anàlisi i alertes, el Drive Space Alert, monitoritza els sistemes de còpies de seguretat i la capacitat del disc, i avisa quan la capacitat restant és escassa.

<http://www.diarioti.com/gate/n.php?id=23124>

Com lliurar-se de la publicitat no desitjada

L'Agència Espanyola de Protecció de Dades ha presentat un servei de 'llista Robinson' per Internet, que permet inscriure's per no tornar a rebre comunicacions comercials no desitjades.

Desenvolupada per la Federació de Comerç Electrònic i Màrqueting Directe (FECMD), la 'llista Robinson' aspira a ser el fitxer de referència per als usuaris farts de rebre

publicitat no sol·licitada, així com per a les empreses que han de complir amb la Llei de protecció de dades.

El reglament de la llei, aprovat al desembre de 2007, obliga les empreses, institucions i organitzacions a consultar aquest tipus de fitxers d'exclusió, abans de llançar una campanya publicitària que utilitzi dades personals que figurin a fonts públiques, o bé fitxers dels quals no siguin responsables.

Voluntari i gratuït

A través del servei d'aquesta llista, també serà possible informar una empresa que ja no es desitja rebre'n publicitat telefònica. Aquest servei és de caràcter voluntari i gratuït per als particulars, tot i que comporta una despesa entre 150 i 550 euros per a les empreses que desitgin consultar el fitxer. Fins ara, les llistes comuns d'exclusió, o 'llistes Robinson', només permetien restringir la publicitat no desitjada que rebien els ciutadans a través de correu postal. Ara, amb aquest nou servei, tampoc no rebran trucades, sms ni correus electrònics d'empreses amb les quals no mantinguin, o hagin mantingut, algun tipus de relació.

Els interessats que s'inscriguin a la [web](#) podran seleccionar per si mateixos el mitjà o mitjans a través dels quals no vulguin rebre publicitat. de les entitats que per al desenvolupament de les campanyes publicitàries utilitzen dades personals que obtingudes de fonts públiques (com guies telefòniques) o bases de dades de les quals no siguin responsables.

<http://www.listarobinson.es>

Sophos presenta IT Vigilante

Dins la seva estratègia, Sophos presenta *IT Vigilante*, un microlloc web que allotja un personatge fictici creat amb la finalitat de guiar clients i socis pel món de la protecció de dades.

Aquest personatge descriu, des de la seva pròpia experiència, la importància de la seguretat de les dades i del desenvolupament d'una política de protecció de dades.

<http://www.diarioti.com/gate/n.php?id=23119>



Incidents de seguretat relacionats amb dades personals

Un ciberdelinqüent es declara culpable de haver robat i venut dades bancàries (juliol 2009)

Un ciberdelinqüent, conegut amb el pseudònim Iceman, s'ha declarat culpable de dos càrrecs de frau de telecomunicacions davant d'una cort de Pennsilvània, i ha admès haver robat 1,8 milions de dades financeres d'usuaris d'Internet i haver-los venut en un mercat negre virtual, anomenat Cardersmarket.

Per obtenir les dades, utilitzava les xarxes sense fils (Wi-Fi) de llocs públics i, després, accedia a les bases de dades d'institucions financeres i d'empreses que processen targetes de crèdit.

El jutge el podria arribar a condemnar a 60 anys de presó.

El fiscal de Nova York demandarà una xarxa social per robar identitats (juliol 2009)

Segons informa la versió en línia del diari *El País* (EIPais.com), la xarxa social Tagged.com serà acusada de robar identitats, realitzar pràctiques enganyoses de màrqueting per correu electrònic i envair la privacitat.

El fiscal general de Nova York, Andrew Cuomo, ha explicat que "la companyia va robar agendes de correu electrònic i identitats de milions de persones" i que "els consumidors que van visitar el lloc web van ser enganyats, per proporcionar a l'empresa accés als seus contactes de correu electrònic. L'empresa utilitzava aquestes dades per enviar milions de missatges de correu electrònic promocionals".

Als aeroports dels EUA es perden 10.000 portàtils per setmana (juliol 2009)

Segons informa el diari *Clarín* (Argentina), en els 36 aeroports més grans dels Estats Units es perden uns 1.700 ordinadors portàtils cada dia, i uns 2.000 en els aeroports d'envergadura mitjana.

Aquest estudi, que té per objectiu determinar la freqüència amb què es perden els equips, es va fer en 106 aeroports dels Estats Units i van enquestar més de 800 passatgers de la classe *business*.

L'estudi assenyala que el 53% dels passatgers que van perdre l'ordinador portàtil va declarar que contenia informació confidencial de la seva empresa, mentre que el 65% va mostrar certa despreocupació i va manifestar que no havia adoptat cap mesura per protegir l'ordinador fins al moment de l'incident.

El 42% dels enquestats va reconèixer que no fa una còpia de seguretat de les seves dades.



Secció responsables de seguretat

Parlem dels responsables de seguretat

En aquesta edició del +Kdades, ens ha semblat oportú substituir l'habitual entrevista amb un responsable de seguretat per una breu descripció de quines són les funcions i responsabilitats que la normativa vigent atribueix a la figura del responsable, en relació a la protecció de dades de caràcter personal.

El 15 de juny passat, l'Agència va presentar el seu segon pla d'auditoria, que té per objectiu verificar dues mesures de seguretat, fonamentalment de caràcter organitzatiu: la designació del responsable de seguretat i l'existència del registre d'incidències. Tal i com es va anunciar, aquest segon pla s'iniciarà al setembre i, per tant, no està de més recordar ara quines són les funcions mínimes del responsable de seguretat, i algunes de les seves característiques.

En aplicació del Reial decret 1720/2007, de 21 de desembre, que aprova el Reglament de desplegament de la Llei orgànica 15/1999 (art. 88.4.a), el responsable de seguretat ha d'estar identificat en el document de seguretat de tots els fitxers o tractaments, que inclou tant els automatitzats i com els no automatitzats, que requereixin del nivell mitjà de mesures de seguretat.

Segons la definició que en fa el reglament a l'article 5.2.1, el responsable de seguretat és la persona o persones a les quals el responsable del fitxer o tractament assigna, formalment, la funció de coordinar i controlar les mesures de seguretat aplicables al fitxer o tractament.

Per tant, ja tenim una primera qüestió a tenir en compte: hi ha d'haver una designació formal, feta pel responsable del fitxer o tractament. La formalitat més bàsica seria disposar d'una justificació documental, que reculli el moment en què el responsable del fitxer o tractament fa la designació del responsable o responsables de seguretat.

5

Amb caràcter general, s'atribueix al responsable de seguretat la coordinació i el control de les mesures de seguretat

aplicables als fitxers o tractaments per als quals ha estat designat pel responsable del fitxer o tractament, però el reglament identifica també unes funcions o responsabilitats concretes. Aquestes funcions específiques tenen a veure amb el seu paper en relació a dues mesures de seguretat: l'auditoria i el registre d'accessos.

- El responsable de seguretat ha d'analitzar els informes de les auditories que els fitxers i tractaments han de passar com a màxim cada dos anys. N'ha d'extreure unes conclusions, que ha de posar en coneixement del responsable del fitxer o tractament a fi de que adopti, si escau, les mesures correctores adients.

Tot i que el reglament no ho especifica (art. 96), òbviament la millor opció és documentar les conclusions i el procediment de comunicació al responsable del fitxer o tractament.

- El mecanisme relacionat amb el registre d'accessos previst a l'art. 103 (rastre de l'activitat que desenvolupen els usuaris en accedir a les dades de nivell alt) ha d'estar sota el control del responsable de seguretat. Per tant, ha de garantir que es registra la informació que preveu el reglament, així com vetllar perquè aquest registre no es manipuli ni es desactivi. En definitiva, que les eines o sistemes utilitzats per registrar l'activitat del usuari que accedeixen a les dades personals funcionin correctament i continguin una informació ajustada a la realitat.

El control que ha d'exercir el responsable de seguretat sobre el registre d'accessos es materialitza en la revisió mensual de la informació enregistrada i en un informe on quedin reflectides, si escau, les incidències detectades.

Per últim, recordar algunes qüestions:

- El responsable del fitxer o tractament pot designar més d'un responsable de seguretat. En tot cas, en el document de seguretat cal no només identificar aquests diferents responsables de seguretat, sinó també explicitar com tenen atribuïdes les diferents funcions de coordinació i control de les mesures de seguretat, i sobre quins fitxers o tractaments les desenvolupen.



- En cap cas la designació del responsable de seguretat exonera el responsable del fitxer o tractament, o l'encarregat del tractament si és el cas, de les seves responsabilitats.
- El responsable de seguretat pot delegar totalment o parcialment algunes de les seves funcions de control i coordinació. Les delegacions han de quedar recollides en el document de seguretat, en especial quan l'autorització d'accés als diferents recursos dels sistemes sigui per delegació de funcions del responsable de seguretat (art. 5.2.a).

Enllacem amb...

<http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=es>

Aquest mes, hem triat la pàgina del Supervisor Europeu de Protecció de Dades. Tal com s'hi descriu, l'EDPS (European Data Protection Supervisor) és una autoritat de control independent, dedicada a la protecció de les dades personals i la intimitat, així com a la promoció de bones pràctiques entre les institucions i òrgans comunitaris.

Desenvolupa funcions de supervisió dels tractaments de dades de caràcter personal que fan les institucions europees i assessora, també, en relació a la legislació i les polítiques comunitàries que afectin la intimitat de les persones. Així mateix, coopera amb altres autoritats equivalents per garantir la protecció de dades de caràcter personal.

A banda de totes les qüestions relacionades amb les funcions que desenvolupa, a la pàgina hi ha novetats i informació sobre jornades i actes relacionats amb la protecció de dades. Hi trobem, també, altres iniciatives vinculades a la protecció de dades de caràcter personal, com les conferències internacionals o el treball del grup de l'article 29. A la pàgina ens podem subscriure a una llista de distribució, que ens permetrà estar informats de tota l'activitat que desenvolupa o en què intervé el Supervisor Europeu.



On anar...

Congressos i esdeveniments

18th USENIX Security Symposium (Security '09)

Del 12 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 de 2009. Busan (República de Corea)
<http://www.wisa.or.kr/>

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

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

Workshop in Information Security Theory and Practices WISTP'2009

Del 1 al 4 de setembre de 2009. Brussel·les (Bèlgica)
<http://www.wistp.org/index.php>

International Symposium: Recent Developments in Cryptography and Information Sec (CryptoBG*2009)

Del 3 al 5 de setembre de 2009. Oriahovitz (Bulgària)
<http://www.cryptobg.org/>

Information Security Conference (ISC 2009)

Del 7 al 9 de setembre de 2009. Pisa (Itàlia)
<http://isc09.dti.unimi.it/>

Summer School On Provable Security

Del 7 a l'11 de setembre de 2009. Facultat de Matemàtiques i Estadística. UPC. Barcelona
https://www.fme.upc.edu/recercaiempreses/oficina-de-suport-a-la-recerca-matematica/properes-activitats?portal_status_message=Changes%20saved

The First ICST International Workshop on Security in Emerging Wireless Communica (SEWCN09)

14 de setembre de 2009. Atenes (Grècia)
<http://sewcn.org/>

Curs de Protecció de Dades a les Administracions Públiques

Del 14 al 16 de setembre de 2009. Universitat Internacional Menéndez Pelayo (UIMP). València
http://www.uimp.es/uimp/home/homeUIMPdina.php?jci=AC_ADEMICAS_FICHA&iuj=2003&ipi=IdActividad=7970306&pg=1&orden=6

VI Conference on Broadband Communications, Networks and Systems

Del 14 al 17 de setembre de 2009. Madrid
<http://www.broadnets.org/>

14th European Symposium on Research in Computer Security (ESORICS 2009)

Del 21 al 25 de setembre de 2009. Saint Malo (França)
<http://conferences.telecom-bretagne.eu/esorics2009/EN/home.php>

Workshop on Computational Intelligence for Security in Information Systems CISIS 09

Del 23 al 26 de setembre de 2009. Burgos
<http://gicap.ubu.es/cisis2009/>

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/>

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/>

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>

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/>

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/>

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/>

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



El responsable de protecció de dades (*Data Protection Officer*)

«...model català de protecció de dades, basat en l'establiment de mesures preventives que tendeixen a evitar la vulneració del dret...»

Tot i això, un eficaç i eficient compliment de la normativa de protecció de dades exigeix l'establiment de mesures, podríem dir-ne organitzatives, que en alguns casos van més enllà del compliment de la legislació vigent i que impacten en la manera de treballar de l'organització.

L'Agència Catalana de Protecció de Dades treballa en el que anomena model català de protecció de dades, basat en l'establiment de mesures preventives que tendeixen a evitar la vulneració del dret. Tot dret, però particularment el dret a la protecció de dades, és difícil de restaurar, per no dir impossible, un cop ha estat vulnerat; per tant, no hi ha millor garantia que establir mesures que n'evitin la vulneració.

Aquest model es concreta en el que, utilitzant el terme anglosaxó, s'anomena *privacy by design*. És a dir, la privacitat dissenyada o privacitat en el disseny, que promou l'establiment d'elements preventius en la fase de disseny dels projectes, polítiques públiques, serveis, etc. i incorpora elements de seguretat i privacitat al disseny de les solucions de gestió de la informació personal. Aquest model incorpora solucions en tres àmbits: processos, organitzatiu i tecnològic.

És en l'àmbit organitzatiu on trobem el responsable de protecció de dades (*Data Protection Officer-DPO*). Aquesta figura s'encarrega, dins de l'organització, de gestionar totes les qüestions relacionades amb la normativa de protecció de dades.

La legislació espanyola no ha regulat aquesta figura, malgrat que sí que apareix en la Directiva 95/46/CE. Amb tot, la Directiva la regula de manera limitada, en relació a la possibilitat d'establir excepcions a l'obligació de notificar els fitxers i tractaments als registres de Protecció de Dades i com a mesura de garantia, en el cas de tractaments que comporten un risc especial.

«...la privacitat dissenyada promou l'establiment d'elements preventius en la fase de disseny dels projectes, polítiques públiques, serveis, etc.»

El DPO, com a element preventiu, permet aportar una visió de conjunt de la protecció de dades personals i millorar la gestió integral de la seguretat de la informació. És una mesura que ajuda en l'autogestió o l'autocontrol en la gestió de la informació. Però, com en qualsevol altre cas, el fet de crear internament aquesta figura i nomenar algú com a DPO no en garanteix per sí mateix l'eficàcia, sinó que cal que reuneixi una sèrie de característiques.

Per delimitar aquestes característiques, podem mirar com s'ha regulat en altres països de la Unió Europea que sí que l'han incorporat a la seva legislació, per exemple Alemanya, i, com serà el cas, analitzar com s'ha regulat en el si de les institucions de la Unió Europea. En aquest sentit, és d'especial interès el *Document de referència relatiu al paper de l'encarregat de protecció de dades per garantir el respecte efectiu del Reglament (CE) número 45/2001*, elaborat pel Supervisor Europeu de Protecció de Dades, on es donen els elements clau per garantir l'efectivitat del DPO.

En primer lloc, cal identificar les funcions mínimes que ha de desenvolupar un DPO:



*«...el DPO permet
aportar una visió
de conjunt de la
protecció de
dades personals i
millorar la
gestió integral
de la seguretat
de la
informació...»*

- Informar i sensibilitzar el conjunt de l'organització.
- Assessorar el responsable del fitxer o tractament.
- S'ha d'establir l'obligació que se li notifiquin tots els fitxers i tractaments de l'organització, perquè pugui garantir el correcte compliment de la normativa de protecció de dades.
- Cooperar amb l'autoritat de protecció de dades (interlocutor).
- Controlar el respecte a la normativa de protecció de dades.
- Gestionar les queixes i reclamacions en matèria de protecció de dades.

A fi que aquestes funcions es puguin desenvolupar correctament, la figura del DPO ha de reunir unes característiques o complir uns requisits:

1. Independència, en l'aplicació de la normativa de protecció de dades. Vindrà determinada per diferents factors, per exemple: el grau de dedicació que se li atribueixi, la posició jeràrquica que tingui (dependència directa del responsable del fitxer), l'assignació de recursos humans i materials per desenvolupar la seva tasca, que eviti l'existència de conflictes d'interès, que no estigui subjecte a instruccions de tercers i l'accés al conjunt de la informació, els locals i les instal·lacions on es tracta la informació.
2. Garantir que la persona triada reuneix les qualitats professionals i personals necessàries. És important que conegui l'organització i la seva estructura, que tingui coneixements en matèria de tecnologies de la informació, seguretat i qualitats en matèria d'organització i comunicació.

*«...el DPO ha de
reunir unes
característiques:
independència i
les qualitats
professionals i
personals
necessàries...»*

A partir d'aquest breu resum, podríem concloure que, tot i que aquesta figura no està regulada en la nostra legislació, no hi ha res que impedeixi que es designi un responsable o encarregat de protecció de dades dins d'una organització. No serviria per eliminar l'obligació de notificar els fitxers, però sí que aportaria, des de la perspectiva de l'organització i la gestió de les dades personals, importants beneficis; i no únicament des del punt de vista del dret a la protecció de dades, sinó també com a element de control sobre el conjunt de tractaments que es porten a terme dins d'una institució (evitar duplicitats, evitar pèrdues de dades derivades d'actes de bona fe...). En tot cas, no podem oblidar que la construcció o definició dels elements configuradors d'aquesta figura no és una tasca acabada. Cal actualitzar-la i ampliar-la, d'acord amb l'evolució del dret a la protecció de dades.

Joana Marí.
Responsable de
Consultoria del
Registre de
Protecció de
Dades de
Catalunya