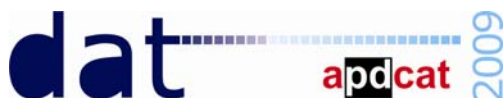


Destaquem... DAT2009 Jornades Tecnològiques per a la Protecció de Dades



Jornades Tecnològiques per a la Protecció de Dades

Patrocinadors:



Col·laboradors:



El proper 9/6/2009, l'Agència Catalana de Protecció de Dades organitza, amb el suport d'empreses del sector de la seguretat de la informació, les primeres Jornades de Tecnologia i Protecció de Dades DAT2009 (dades i tecnologia). Seguint la línia d'actuacions iniciades per l'APDCAT amb l'objectiu de dotar d'eines els perfils professionals de caràcter tècnic involucrats en la protecció de dades personals, en aquesta jornada de matí i tarda s'abordanen qüestions relacionades amb la presa de decisions en matèria de seguretat de la informació.

Les Jornades DAT de l'APDCAT tenen la vocació de convertir-se en un esdeveniment anual i de caràcter monogràfic. És a dir que en cada convocatòria es tractarà, des de la perspectiva tecnològica, una qüestió concreta relacionada amb la gestió de la informació de caràcter personal: les bases de dades, el control d'accés, la disponibilitat de la informació, la prevenció en la fuga d'informació, etc. El lema de DAT2009 és "Analitzant els riscos i planificant la seguretat".

Els responsables de tractaments i fitxers de dades de caràcter personal tenen el deure de protegir la informació que gestionen i, per tant, han de prendre decisions en matèria de seguretat de la informació. Aquestes decisions no es poden prendre sense saber què s'ha de protegir, qui es el propietari d'allò que es vol protegir o quines poden ser les conseqüències dels incidents que afectin les dades. Per això, en aquesta jornada es proposarà una reflexió àmplia sobre la importància de disposar d'informació que permeti prendre decisions tècniques i organitzatives, proporcionades i conformes amb les exigències de la normativa.

Per a més informació i inscripcions adreceu-vos a: dat.apdcat@gencat.cat

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
Anàlisi i gestió de riscos: eines clau per a la seguretat de la informació	8

Parlem de... l'anàlisi de riscos

L'anàlisi i la gestió dels riscos es configuren com a processos fonamentals en una organització i en l'assegurament dels seus actius més crítics, entre els quals la informació. Però no únicament perquè identifiquen els perills que amenacen la integritat d'aquesta informació, sinó també perquè proporcionen una visió global del seu estat i això en facilita el tractament.

No s'ha d'oblidar, a més, que l'anàlisi i la gestió dels riscos garanteixen una participació total de l'organització, més enllà dels departaments que, erròniament, es consideren més relacionats amb la seguretat de la informació (les àrees més tècniques). Arran de l'execució d'aquests processos, tots els treballadors es trobaran més implicats amb la seguretat.

+info



Revisió de vulnerabilitats de seguretat

Pesca (*phishing*) a Facebook

Facebook declara que ha posat fre a l'onada de pesca informàtica que intentava enganyar els usuaris d'aquesta eina social, amb l'objectiu de divulgar les seves credencials d'accés. A principis d'aquest mes de maig, s'havien enviat missatges de *phishing* als membres de Facebook, aparentment provinents dels seus amics. La realitat, però, és que els estafadors poden haver estat piratejant aquests comptes d'usuari, cosa que els hauria donat la possibilitat d'enviar missatges i suplantar la identitat de la víctima.

Al contingut dels missatges de correu electrònic enviats hi havia enllaços a 2 llocs web: *fbstarter* [es] i *fbaction* [net], que van ser dissenyats per imitar la pantalla d'inici de sessió de Facebook. Els pirates intentaven que els destinataris renunciessin al seu nom d'usuari i la seva contrasenya per accedir a Facebook, després de diversos intents fallits d'autenticar-se.

Un cop es va assabentar de l'atac, Facebook va bloquejar els comptes que utilitzaven els estafadors i va impedir que el contingut fos compartit a la web. Seguidament, l'empresa va canviar les contrasenyes dels perfils que havien estat víctimes de l'enviament de falsos missatges.

Copyright Suècia

Tele2, una altra de les companyies que posen els drets dels seus clients per sobre de les pressions de les

organitzacions de drets d'autor, ha comunicat la seva intenció d'eliminar, al cap de dos dies, el registre de les adreces IP dels seus clients. És la segona operadora sueca, després Bahnhof, que aquest mes anuncia la mateixa mesura, malgrat la directiva europea que permet als diferents països exigir als proveïdors la identificació de clients.

Aquestes companyies s'han negat a tancar el servei al lloc web The Pirate Bay, ja que, segons diuen, no estan disposades a convertir-se en la policia de la xarxa. En opinió de Tele2, es tracta d'un dret democràtic i l'objectiu de la seva decisió és respectar la integritat dels seus clients. Les operadores desafien així la més que probable norma sueca que obligarà a identificar els usuaris que, suposadament, descarreguin material protegit per drets d'autor.

No obstant això, la informació personal dels seus usuaris i la IP corresponent es lliurarà a les autoritats judicials quan es sol·licitin, sempre i quan encara estiguin disponibles.

Hackers estafadors

La setmana passada, els pirates informàtics van prendre el control del Programa de Monitorització de Prescripció Virginia (PMP), que conté informació mèdica i de les receptes de medicaments dels pacients i que està destinat a impedir que s'abusi de l'accés als medicaments. Els *hackers* exigien uns 10 milions de dòlars de rescat pel retorn dels 8.257.378 registres de pacients i els 35.548.087 de receptes que tenien al seu

poder, ja que en cas contrari la informació bàsica d'identitat s'oferiria al millor postor. Van afegir, a més, que havien fet una còpia de seguretat i l'havien xifrat, i posteriorment havien eliminat l'original. L'FBI ha optat per no pagar rescat per la informació i ho està investigant, juntament amb la policia estatal.

Segons Bojan Zdrnja, del SANS Internet Security Center, si això es confirma indica que la protecció de diverses capes al PMP no funciona. Va afegir que, sense saber-ne més detalls, no es pot valorar si l'aplicació web és bona o no (el pirata hi pot tenir accés a través d'una vulnerabilitat), però que mai un *hacker* hauria de tenir la capacitat d'eliminar les còpies de seguretat. I, de fet, qualsevol bon sistema de còpia de seguretat només li permetrà copiar o llegir, ja que únicament l'administrador de còpies de seguretat pot esborrar-les.

El cas planteja qüestions a llarg termini per a les empreses que tenen grans quantitats de dades sobre clients, sobretot en relació a la seva responsabilitat en el cas que es donés un atac.

Aquesta no és la primera vegada que s'ataquen bases de dades mèdiques per demanar rescat. A l'octubre de 2008, l'Express Scripts va ser víctima del robatori de la base de dades dels EUA i el pirata demanava 1 milió de dòlars per al seu retorn segur.



Tecnologia i protecció de dades

Microsoft, l'AEPD i Red.es presenten un llibre sobre la protecció de dades personals

Microsoft Ibèrica, amb el suport de l'Agència Espanyola de Protecció de Dades (AEPD) i Red.es, ha anunciat la seva segona iniciativa adreçada a facilitar a les empreses espanyoles el compliment del reglament vigent sobre protecció de dades personals: la publicació del llibre *La protección de datos personales: soluciones en entornos Microsoft, versión 2.0*, que es pot descarregar en línia, gratuïtament, a l'enllaç següent:

http://download.microsoft.com/download/C/2/6/C2689C05-2B67-4D11-BD2A-43CF9DBCE59E/Libro_LOPD_V2_Alta.pdf

Es tracta d'un manual gratuït de caire divulgatiu, que té com a fil conductor els articles amb major repercussió tecnològica del reglament de la Llei orgànica de protecció de dades (RLOPD). A més de comentar aquests articles de forma senzilla i entenedora, l'exemplar fa la recomanació tècnica més adequada per al seu compliment, utilitzant la tecnologia Microsoft. D'aquesta manera ajuda les organitzacions a aplicar amb garanties les mesures tecnològiques dictades per la llei.

Més informació

<http://www.hoytecnologia.com/noticias/Microsoft-AEPD-Redes-presentan/108234>

Protecció de Dades investigarà les principals operadores de telecomunicacions i proveïdors d'Internet

L'Agència Espanyola de Protecció de Dades (AEPD) ha començat una sèrie d'inspeccions d'ofici a les principals operadores de telecomunicacions i proveïdors d'Internet. L'objectiu de l'actuació és analitzar el compliment de les garanties de protecció de dades respecte de les obligacions establertes per la legislació nacional, en relació a la conservació de dades de trànsit de les comunicacions electròniques.

Aquesta normativa, aprovada l'octubre de 2007, obliga totes les operadores a conservar durant un any les dades de trànsit i de localització de les comunicacions. Estableix, a més, el deure de cessió de les dades a les persones autoritzades, sempre que es requereixi a través d'autorització judicial amb la finalitat de detectar, investigar i enjudiciar delictes greus.

Aquesta investigació la desenvoluparan, de forma sincronitzada, les autoritats en matèria de protecció de dades de tots els països de la Unió Europea (UE) i les seves conclusions, que s'avaluaran tant individualment com per al conjunt de la UE, podrien decidir noves accions i orientacions pràctiques per al sector.

Més informació

https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/abril/220409_conservacion_datos_operadoras.pdf

Aquest dispositiu iniciarà la seva autodestrucció en cinc segons

Fujitsu Labs ha presentat un dispositiu d'emmagatzemament USB en el qual la informació s'esborra automàticament, després d'un període de temps establert o bé si es connecta a un ordinador no autoritzat. La unitat té a l'interior una bateria i un processador que, a més de ser capaç d'autodestruir la informació i inutilitzar el dispositiu, pot prevenir que els arxius es puguin posar en una xarxa d'intercanvi d'arxius, s'enviïn com a adjunts de correu electrònic o fins i tot s'imprimeixin.

Les seves aplicacions pràctiques seran prevenir l'espionatge industrial, evitar el robatori de dades sensibles o ajudar les empreses a complir les polítiques respecte a dades. El prototip encara és en fase de proves internes, però l'empresa pretén comercialitzar-lo.

Més informació

<http://www.fujitsu.com/global/news/pr/archives/month/2009/20090417-02.html>



Incidents de seguretat relacionats amb dades personals

Verizon Business presenta un informe sobre els incidents relacionats amb fugues d'informació al 2008 (abril 2009)

En el seu informe "2009 Data Breach Investigation Report", l'empresa Verizon Business ha subratllat que al 2008 s'han produït alguns dels incidents de seguretat més grans, relacionats amb les fugues o exposicions d'informació.

Algunes de les dades més rellevants de l'informe són:

- Qui va produir l'incident:
 - o El 74%, agents externs a l'organització
 - o El 20%, personal intern
 - o El 32%, socis empresarials
- Com es va produir l'incident:
 - o El 67% per errors de l'organització
 - o El 64% per atacs de pirateria (*hacking*)
 - o El 38% utilitzant codi maliciós (*malware*)
- Què tenen en comú:
 - o El 69% dels incidents els van descobrir terceres parts
 - o El 17% dels atacs eren d'un nivell de dificultat alt
 - o El 87% del incidents es podrien haver evitat, amb la implementació de controls de seguretat senzills

Trobats a les escombraries documents confidencials de Vitalicio Seguros (abril 2009)

Segons informa l'edició sevillana del diari *20 minutos*, un empleat d'una sucursal de la companyia Vitalicio Seguros va llençar a un contenidor de paper per reciclar milers de documents amb informació dels seus clients.

El diari esmentat, que es va desplaçar fins al contenidor després que un lector els truqués per denunciar-ho, va poder comprovar directament aquest fet.

Reforcen la seguretat després que es perdi un llapis de memòria amb dades mèdiques de 741 pacients (abril 2009)

Segons va informar la BBC, a finals de l'any passat l'hospital Addenbrooke, que depèn de la Fundació Cambridge University Hospital NHS Foundation Trust, va patir un incident de seguretat relacionat amb la protecció de dades.

Un informe de l'Oficina del Comissionat d'Informació (ICO) afirma que la Fundació va informar de la pèrdua d'un llapis de memòria sense xifrar, que contenia dades mèdiques de pacients, després que un membre del personal se'l deixés en un vehicle particular. Un empleat d'una companyia de rentat de cotxes va trobar el dispositiu USB, va accedir-hi per esbrinar qui n'era el propietari i posteriorment el va retornar a la Fundació.

Aquesta fundació mèdica, juntament amb tres més que han tingut incidents de seguretat relacionats amb la protecció de dades, aplicarà mesures per protegir les dades personals de forma més efectiva. Una de les primeres serà el xifrat de tots suports i dispositius mòbils que s'utilitzin per emmagatzemar dades personals.

Es perd un disc dur amb un 1TB d'informació del govern de l'expressident Clinton (maig 2009)

L'Agència d'Administració de Registres i Arxius Nacionals dels Estats Units (NARA) ha informat que, entre octubre de 2008 i març de 2009, es va perdre un disc dur amb informació confidencial del govern de l'expressident Bill Clinton.

Sembla que la NARA va treure el disc d'un magatzem de seguretat, on era per digitalitzar-ne part del contingut, i el va deixar en una àrea de treball a la qual tenien accés més d'un centenar de persones. Es desconeix si el disc ha estat sostret o bé s'ha extraviat.



Secció responsables de seguretat

Nom i cognoms

Neus Bellavista Arimany

Lloc que ocupa

Responsable de l'Oficina de Seguretat TIC de l'IMI

Des de quan

5 anys

Entitat

Institut Municipal d'Informàtica de l'Ajuntament de Barcelona

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

L'Institut Municipal d'Informàtica (d'ara endavant, IMI), és un organisme autònom de l'Ajuntament de Barcelona constituït el 1990, com a continuació dels antics Centre Ordinador Municipal (COM) i Centre de Cartografia Automàtica (CCA). Estatutàriament, l'IMI té assignada, entre d'altres, la funció d'establir estàndards, normatives i mesures en matèria de seguretat TIC per al gruix de l'organització municipal.

Fa dos anys, l'IMI va adoptar com a marc de referència en matèria de seguretat de la informació l'estàndard internacional ISO/IEC 27002, que gaudeix d'un important reconeixement dins del sector TIC, i l'està implantant de manera progressiva. Mitjançant el domini de Compliment, l'estàndard dona cabuda a les obligacions reguladores nacionals. Aquest domini ens permet complementar els controls (mesures de seguretat) de la norma ISO amb els que la LOPD imposa a través del seu Reglament de desenvolupament, a banda d'altres mesures derivades de la creixent pressió reguladora (Llei de signatura electrònica, LISI, LSCP, etc.).

I és dins de l'àmbit d'actuació de l'IMI i sobre la base de l'estàndard de seguretat de la ISO/IEC 27002 on desenvolupo la meva activitat, amb el rol de responsable de l'Oficina de Seguretat. Pel que fa a la LOPD, s'exclou de les competències de l'Oficina tot allò relatiu al registre dels fitxers de DCP, a l'exercici dels drets ARCO i a les auditories bianuals.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

Sí, amb l'ajuda d'un equip de professionals que componen l'Oficina de Seguretat (entre els quals, 3 CISA), en col·laboració amb responsables d'altres departaments de l'IMI i amb serveis contractats a una empresa externa.

L'objectiu principal és anar configurant processos de seguretat i construir un sistema de gestió de seguretat dels sistemes d'informació en diferents camps, com el cos normatiu, la configuració de processos de seguretat, l'arquitectura de seguretat, la protecció d'intrusions i l'anàlisi forense, la gestió d'identitats, la criptografia i processos d'identitat i signatura digital, plans de contingència i gestió d'incidències i peticions de seguretat. Tot això, sobre la base de la ISO/IEC-27001, amb l'objectiu d'arribar a la posició de certificable.

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

Prefereixo parlar de reptes i no tant de dificultats. Bàsicament, són tres:

D'una banda, la conscienciació en matèria de seguretat, tant interna com externa: la seguretat com a valor afegit per generar confiança. Aquest repte és típic d'un sector, el de seguretat, que s'està construint i que en els últims deu anys ha evolucionat progressivament i ha adquirit importància en les organitzacions.

D'una altra banda, els reptes tecnològics de l'e-administració i dels nous marc reguladors.

I, finalment, la coordinació entre diferents àrees per establir controls de seguretat i implantar-los en les metodologies de treball.

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

Quant al compliment de la Llei de protecció de dades, la responsabilitat del fitxer recau, sobre la base dels diferents serveis municipals, en els gerents dels organismes i les empreses municipals.



A través de la Comissió de Protecció de Dades, es vetlla pel compliment de la LOPD i s'estableixen les directrius generals en matèria de protecció de dades personals, per al conjunt de l'organització municipal. També es fixen els criteris d'aplicació de la normativa, la publicació i difusió dels procediments per a la declaració de fitxers subjectes a la LOPD, l'estandardització del document de seguretat, les bones practiques i els plans de formació per al compliment de la normativa de protecció de dades.

La meua responsabilitat en relació a la protecció de dades es centra en el compliment de les mesures de seguretat de fitxers automatitzats, a mantenir una coordinació i a fer el seguiment de les actuacions de la comissió de protecció de dades. També em responsabilitzo de donar suport als responsables dels fitxers, en aspectes relacionats amb les mesures tècniques de seguretat de la informació automatitzada que exigeix el Reglament.

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

Si, però sempre amb relació a aspectes de Reglament, no de la Llei. Sovint, els projectes presenten requeriments o solucions que plantegen dubtes pel que fa a la implantació de mesures de seguretat.

Enllacem amb...

<http://www.privacyinternational.org/>

Privacy International és un grup de protecció dels drets humans creat el 1990 i que es defineix com a *watchdog* (gos guardià) de la privacitat de les persones. Té la seu central a Londres i una oficina a Washington DC.

Tal i com expliquen a la seva pàgina web, la seva activitat principal és fer campanyes a tot el món per protegir les persones contra la intrusió dels governs i les empreses, que intenten soscar aquest dret tan fràgil que consideren essencial per al lliure exercici de les llibertats individuals.

A la seva pàgina, resulten d'interès tant les activitats que organitzen com les notícies que recullen al voltant de la seva activitat de vigilància. Tenen una rellevància especial els informes que recopilen i elaboren en relació a àrees específiques, com ara: la llibertat d'accés a la informació, els documents nacionals d'identitat, la lluita contra el terrorisme, la vigilància de viatgers i fronteres, la protecció de dades, el control de les telecomunicacions o dels serveis financers, la privacitat de l'ADN i les dades genètiques etc.

The screenshot shows the Privacy International website. The main content area features a list of news articles with titles and dates. The sidebar on the right contains a navigation menu with categories like 'ABOUT', 'NEWS', 'REPORTS', and 'CONTACT'. The top of the page has the Privacy International logo and name.



On anar...

Congressos i esdeveniments

The First International ICST Conference on Security and Privacy in Mobile Information and Communication Systems – MobiSec 2009

Del 3 al 5 de juny de 2009. Torí (Itàlia)
<http://mobisec.org/index.shtml>

Key Management Workshop

8 i 9 de juny de 2009. Gaithersburg, Maryland (EUA)
http://csrc.nist.gov/groups/ST/key_mgmt

DAT2009 Jornades Tecnològiques per a la Protecció de Dades

9 de juny de 2009. Barcelona
<http://www.apd.cat/>

The Third International Conference on Emerging Security Information, Systems and Technologies – SECURWARE 2009

Del 18 al 23 de juny de 2009. Atenes (Grècia)
<http://www.iaia.org/conferences2009/SECURWARE09.html>

Workshop on Security and High Performance Computing Systems

Del 21 al 24 de juny de 2009. Leipzig (Alemanya)
<http://leibniz.diiga.univpm.it/~spalazzi/leipzig>

Lone Star Information Security Forum

24 de juny de 2009. Dallas, Texas (EUA)
http://www.ianetsec.com/forums/splash.html?forum_id=45

The Eighth Workshop on the Economics of Information Security (WEIS 2009)

24 i 25 de juny de 2009. Londres (Regne Unit)
<http://weis09.infoecon.net>

European Workshop on Challenges in Modern Massive Data Sets (EMMDS 2009)

De l'1 al 4 de juliol de 2009. Lyngby (Dinamarca)
<http://mmds.imm.dtu.dk/>

Redes sociales. Autocontrol o descontrol de la privacidad en Internet?

Del 6 al 10 de juliol de 2009. *Els juliols linguae*. Universitat de Barcelona (UB)
<http://www.ub.edu/juliols/linguae>

20th IEEE International Conference on Application-specific Systems, Architectures and Processors

Del 7 al 9 de juliol de 2009. Boston, Massachusetts (USA)
<http://asap-conference.org/>

22nd IEEE Computer Security Foundations Symposium

Del 8 al 10 de juliol de 2009. Port Jefferson, Nova York (EUA)
<http://www.cs.sunysb.edu/csf09/>

The fifth Symposium on Usable Privacy and Security (SOUPS)

Del 15 al 17 de juliol de 2009. Mountain View, Califòrnia (EUA)
<http://cups.cs.cmu.edu/soups/2009/>

5th Int'l Workshop on Automated Specification and Verification of Web Systems (WWW '09)

17 de juliol de 2009. Castell de Hagenberg (Àustria)
<http://www.risc.uni-linz.ac.at/about/conferences/www09>

2nd IEEE International Workshop on Hardware-Oriented Security and Trust

27 de juliol de 2009. San Francisco, Califòrnia (EUA)
<http://www.engr.uconn.edu/HOST>

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/>

SIGCOMM 2009

Del 17 al 21 d'agost de 2009. Barcelona
<http://conferences.sigcomm.org/sigcomm/2009/>

Seventh Annual International Conference on Privacy, Security and Trust

Del 25 al 27 d'agost de 2009. Saint John, New Brunswick (Canadà)
<http://www.unb.ca/pstnet/pst2009/>

Workshop on Information Security and Privacy in a De-Perimeterised World (DISP09)

29 d'agost de 2009. Vancouver (Canadà)
<http://www.disp09.info/>

6th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS '09)

Del 31 d'agost al 4 de setembre. Linz (Àustria)
<http://www.icsd.aegean.gr/trustbus2009/index.html>

Cursos seguretat TIC 2009-05-06

Centre Criptològic Nacional (CCN-Cert)
https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2140&Itemid=188&lang=es

Anàlisi i gestió de riscos: eines clau per a la seguretat de la informació

«Les anàlisis de riscos són útils per aconseguir la implicació de tota l'organització en matèria de seguretat de la informació, i no només de les àrees tècniques.»

La seguretat dins de les organitzacions s'ha plantejat, al llarg del temps, des de diferents perspectives: si bé en un primer moment es desconeixien els riscos als quals estaven exposades –cosa que n'incrementava la vulnerabilitat-, més tard, amb la proliferació d'equips informàtics, es va estendre la percepció errònia que la seguretat era una competència total i exclusiva del personal informàtic (àrees TIC, personal tècnic, etc.).

Actualment, una concepció més integral de la seguretat es preocupa d'atendre no solament els aspectes tècnics (equips informàtics) d'una organització, sinó totes aquelles qüestions que d'alguna manera participen en l'execució de les tasques de negoci. Així, es tindrien en compte, per esmentar alguns exemples, els recursos humans, les instal·lacions o els canals de comunicació. Una de les peces clau en aquest conjunt d'elements és la informació, un actiu fonamental per al desenvolupament d'un negoci, sense la qual no seria possible executar els processos. És per aquest motiu que pren més rellevància la *seguretat de la informació*, per sobre de la *seguretat informàtica*.

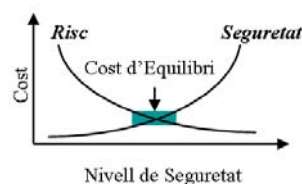
Cal tenir present que el recursos de les organitzacions són limitats, i més en aquests temps de crisi, amb la qual cosa resulta essencial que les inversions en seguretat de la informació redueixin els riscos més importants que poden afectar-ne el funcionament. Els processos per determinar aquests riscos i les millors accions de seguretat a implantar són *l'anàlisi i la gestió de riscos*.

«Permeten tenir una visió total dels elements que s'han de protegir en una organització, sobretot d'aquells més crítics, com ara la informació.»

L'objectiu de **l'anàlisi de riscos** és detectar quines són les situacions potencials que poden arribar a afectar una organització i els seus processos de negoci, és a dir, tot el que pot provocar una execució deficient del seu funcionament. Amb aquests processos, s'aconsegueix donar resposta a les tres preguntes fonamentals de la seguretat de la informació: *Què hem de protegir? De què ens hem de protegir? Per què ens hem de protegir?*

Un cop contestades aquestes preguntes, s'hauran identificat els actius, les amenaces i les vulnerabilitats de l'organització. Després, es farà una anàlisi de les probabilitats de ser perjudicats per una amenaça que aprofiti la vulnerabilitat d'un actiu, així com de l'impacte que podria arribar a causar aquesta situació, si s'arribés a donar.

Un cop recollida aquesta informació, es determina la totalitat de riscos existents, que s'hauran de reduir per tal d'aconseguir un nivell de risc "adient".





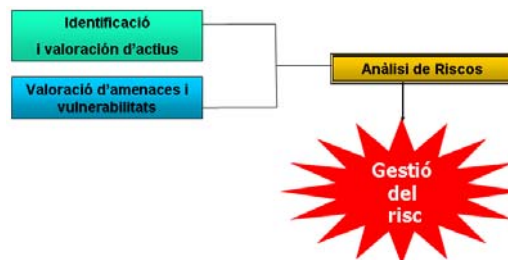
Cal esmentar que el procés d'anàlisi de riscos permet tenir una visió total dels elements que s'han de protegir en una organització, i concretament d'aquells més crítics, com ara la informació. A partir de la identificació de la informació més sensible, es pot exercir un control més acurat sobre el tipus de dades de caràcter personal que posseeix l'organització i ajudar, de forma directa, a un major i millor compliment de la legislació de protecció de dades de caràcter personal.

Gestió de riscos: la solució més apropiada

De forma complementària a l'anàlisi de riscos actua la gestió de riscos, que estableix les possibles solucions de seguretat per reduir els riscos identificats: la solució més adequada per a cada organització, d'acord amb les seves probabilitats i impactes. En general, un procés de gestió de riscos és útil per donar resposta a la pregunta *Com ens hem de protegir?*

Tot procés de gestió de riscos requereix analitzar les diferents opcions de seguretat i seleccionar aquella que comporti un menor cost per a l'organització, sempre tenint present que en cap cas la despesa en protecció pot ser superior al cost d'exposició del risc; és a dir, no s'ha d'invertir més en protecció del que suposarien les pèrdues que podria provocar una determinada situació de risc, si arribés a materialitzar-se.

«Els resultats de la inversió en seguretat queden garantits, ja que s'haurà portat a terme després d'una anàlisi exhaustiva.»



Anticipació i eficiència

Els processos d'anàlisi i gestió de riscos no s'han de veure com una despesa en seguretat, sinó com una inversió de cara a millorar l'efectivitat i eficiència dels processos de negoci d'una organització, ja que permet reduir el nombre d'incidents de seguretat en anticipar-se a la seva aparició.

Aquest tipus de projecte d'anàlisi i gestió de riscos és la millor inversió en seguretat que poden fer les organitzacions, ja que l'exhaustiva anàlisi feta permetrà assegurar que la despesa en seguretat de la informació serà la més adequada.

*Daniel Cruz,
consultor sènior
de seguretat de
la informació,
CISA, CISM.*

D'altra banda, aquests tipus de projecte són útils per aconseguir la implicació de tota l'organització –i no únicament de les àrees tècniques– en aspectes de seguretat de la informació, perquè l'anàlisi es fa des del punt de vista de procés de negoci i no només des de la visió estrictament informàtica. Aquest canvi de visió de la seguretat es reflectirà en un menor nombre d'incidents, ja que s'aconseguirà una major participació de tots els departaments.