Legislació de seguretat i protecció de dades

Miquel Colobran Huguet
Josep Ma. Arqués Soldevila

Seguretat informàtica

Índex

Introducció

L'ús creixent de les tecnologies a les organitzacions, la qual cosa les converteix en imprescindibles per a la gestió de qualsevol activitat, comporta un augment del volum d'informació emmagatzemat dins dels sistemes informàtics. Algunes d'aquestes dades, molt probablement, contindran informació relacionada amb l'esfera personal o íntima de treballadors o persones. Una gestió incorrecta d'aquesta informació pot ocasionar sancions (multes) o un comportament que contravingui la llei (accions il·legals).

Al llarg d'aquest crèdit heu treballat diversos conceptes tècnics relacionats amb la seguretat informàtica. En aquesta unitat, però, veureu que amb els aspectes tècnics no n'hi ha prou per garantir o satisfer tots els requisits de seguretat d'un sistema informàtic. La legislació, el marc jurídic, és absolutament vital en aquest sentit. No és que la legislació s'adapti a la tecnologia, sinó més aviat al contrari: els usos i la implantació dels sistemes informàtics són condicionats per la normativa vigent (que, a més, sol tenir les seves peculiaritats a cada país). En aquesta unitat aprendreu que no tot allò que us permet fer la tecnologia és legal i que les conseqüències de no adequar els sistemes informàtics a la legislació poden ser molt greus.

En l'apartat "Marc jurídic penal", s'estudien els elements més estretament relacionats amb la informàtica i amb l'àmbit jurídic que poden ser causa de conductes il·legals. El fet de conèixer-los us permetrà prevenir-los, detectar-los i evitar-los. Malgrat no ser l'objectiu d'aquesta unitat formativa, podeu trobar una definició més acurada dels termes jurídics en el "Glossari" del web.

En l'apartat "Marc jurídic extrapenal", s'estudien aspectes relatius a la protecció de dades i se'n justifica la importància. Es desenvolupa la normativa existent i s'analitza com afecta l'operativa diària, tant des del punt de vista informàtic com des del punt de vista de l'organització. Tot seguit veureu algunes regles que us ajudaran a detectar situacions en què no s'aplica correctament i com es poden millorar aquests escenaris.

Al llarg de tota la unitat us adonareu que les dades que facin referència a aspectes d'una persona (econòmics, salut, domicili, sociològics...) s'han de gestionar amb una cura especial. També se'ns farà clar que la legislació ha estat conscient d'aquest problema i que, per aquest motiu, hi ha moltes normes –com, per exemple, la Llei orgànica de protecció de dades personals (LOPDP)– que regulen aquests aspectes.

Per tot el que acabem d'esmentar, creiem que aquesta unitat reflecteix aspectes essencials dins de l'àmbit de la seguretat informàtica, ja que és

la base per conèixer com s'interrelaciona la informàtica amb el seu entorn, i també les obligacions que persones i organitzacions han de seguir per adequar-se a les normes establertes. És una unitat tant teòrica com pràctica.

Per treballar els continguts d'aquesta unitat és convenient fer les activitats i els exercicis d'autoavaluació, i també llegir els annexos.

Resultats d'aprenentatge

En acabar la unitat heu de ser capaços del següent:

1. Distingir les principals accions i conductes que poden ser constitutives de delictes.

2. Conèixer els mecanismes de control d'accés a la informació personal emmagatzemada en un sistema informàtic.

3. Identificar les dades de caràcter personal.

4. Delimitar la informació sensible en un sistema informàtic.

5. Saber aplicar la normativa bàsica sobre protecció de dades.

6. Classificar les dades i els fitxers en els nivells de seguretat determinats a la LOPDP.

7. Conèixer les principals etapes en la protecció de dades d'una organització.

8. Saber aplicar la normativa bàsica sobre els serveis de la societat de la informació, comerç i correu electrònic.

9. Configurar programes clients de correu electrònic per al compliment de normes sobre gestió de seguretat de la informació.

10. Dur a terme les actualitzacions de seguretat d'un sistema informàtic.

11. Conèixer la legislació sobre llicències d'ús de programari i adequar-la a un sistema informàtic determinat.

12. Conèixer i implantar, bàsicament, els plans de manteniment d'un sistema informàtic.

13. Interpretar les situacions anòmales i transgressores de la llei.

14. Comprendre com la legislació afecta la seguretat d'un sistema informàtic.

15. Entendre com es vincula la seguretat informàtica amb la legislació.

1. Legislació i normes sobre seguretat i protecció de dades

D'una manera intuïtiva, tots coneixem l'existència d'un conjunt de normes jurídiques que regulen les conductes constitutives de delicte, i també les sancions previstes en aquestes situacions (algunes poden ser fins i tot privatives de llibertat). El recull legislatiu aplicable en aquest tipus de matèria s'anomena **Codi penal**. Cada país disposa de les seves pròpies normes i, per tant, és possible que variïn d'un país a un altre.

El *delicte*...

... es defineix com una conducta típica (tipificada per la llei), antijurídica (contrària a dret), culpable i punible. Implica una conducta infraccional del dret penal, és a dir, una acció o una omissió tipificades i penades per la llei.

És molt important conèixer l'essència de la normativa que afecta l'ús de les tecnologies, ja que, amb independència de la nostra voluntat, condiciona l'ús de les tecnologies, tant des del punt de vista del treballador tècnic, com del de l'usuari d'un ordinador d'una llar qualsevol.

Límits tècnics i legals

El límit de velocitat d'un cotxe no és imposat per límits tècnics, sinó per normes legals. De fet, hi ha limitadors per evitar que la tecnologia pugui ultrapassar el límit fixat per la legislació.

1.1. El delicte informàtic

El **delicte informàtic** no apareix explícitament definit en l'actual Codi penal (1995), ni en les reformes posteriors (Llei 15/2003) que se n'han fet i, per tant, no es podrà parlar de *delicte informàtic* pròpiament dit, sinó de delictes fets amb l'ajut de les noves tecnologies, en els quals l'ordinador s'usa com a **mitjà d'execució** del delicte (per exemple, l'enviament d'un correu electrònic amb amenaces), o bé com a **objectiu** d'aquesta activitat (per exemple, una intrusió en un sistema informàtic).

La legislació del nostre país encara presenta buits pel que fa als mal anomenats *delictes informàtics*, de manera que tan sols oferirem un seguit de directrius bàsiques, més aviat relacionades amb el sentit comú, que no pas amb la normativa complexa que es va generant entorn de l'aplicació de les noves tecnologies.

Una intrusió consisteix en un accés no autoritzat a un sistema informàtic.

El Codi penal de 1995...

... es divideix, a grans trets, en un títol preliminar i tres llibres. Conté 639 articles, els quals recullen totes les conductes susceptibles de ser sancionades pel Codi penal.

El vessant tecnològic o científic dels estudis d'informàtica sovint deixa de banda el vessant social de l'aplicació dels avenços que es van produint en aquestes disciplines. Consegüentment, els usuaris i tècnics d'un sistema informàtic poden ser molt competents en el seu treball, però és més que probable que tinguin molts dubtes a l'hora d'abordar problemes com els següents:

- Si el meu cap em demana que li mostri el contingut de la bústia de correu personal d'un treballador, tinc l'obligació de fer-ho?
- Puc entrar a la bústia de correu electrònic d'un amic?
- Uns intrusos han modificat la pàgina web de l'empresa en què treballo. Aquest fet és denunciable? A qui ho he de denunciar?

- El sistema informàtic de la feina emmagatzema dades de caràcter personal (com, per exemple, el nom, els cognoms, l'adreça i el DNI dels treballadors). Cal protegir aquestes dades amb alguna mesura de seguretat determinada?
- Puc penjar a Internet una pàgina web amb les fotografies i logotips del meu grup de música preferit?
- Puc descarregar lliurement qualsevol arxiu de música de la Xarxa?

Segurament, cap dels exemples descrits no us representa cap mena de dificultat tècnica. No obstant això, cal que tingueu molt present que, si bé no totes les accions vistes són constitutives de delicte, totes elles poden tenir conseqüències importants. Així, doncs, haureu de ser molt conscients que no hi ha una línia d'actuació única i que cal ser molt prudent a l'hora d'enfrontar-nos amb aquest tipus de problemes, ja que **no tot allò que és tècnicament possible és legal**, i, sobretot, cal que tingueu en compte que el desconeixement de les normes no exonera de responsabilitat (penal o no) el treballador informàtic.

1.2. El Codi penal i les conductes il·lícites vinculades a la informàtica

El nostre Codi penal és especialment sever amb la protecció dels drets fonamentals i les llibertats públiques, recollits en el títol I de la Constitució. Aquests drets i llibertats són inherents a la condició de persona i, per aquest motiu, gaudeixen d'una protecció tan especial.

La Constitució (1978) és la norma fonamental de l'Estat, superior a la resta de lleis i a qualsevol tipus de norma.

Un dels articles de la Constitució més directament relacionat amb la pràctica informàtica (tant des del punt de vista tècnic, com del simple usuari), és l'article 18, el qual reconeix el **dret a la intimitat**. Han de ser objecte de protecció no sols l'àmbit íntim de l'individu, sinó també l'esfera familiar i domiciliària.

!!

Podeu trobar una descripció de l'estructura (i la seva divisió en articles) de la Constitució en el "Glossari" del web.

Article 18 CE

1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.

2. El domicili és inviolable. No s'hi pot entrar ni fer-hi cap escorcoll sense el consentiment del titular o sense resolució judicial, llevat del cas de delicte flagrant.

3. Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial.

4. La llei limita l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

!!

Per tal de consultar la Constitució en català podeu consultar la secció "Adreces d'interès" del web.

1.2.1. Delictes contra la intimitat

Una part molt important dels delictes produïts entorn de la informàtica s'ubica dins de la tipificació dels **delictes contra la intimitat**. Sovint, els au-

tors d'aquestes conductes no són conscients de la importància dels béns protegits per la llei i no s'adonen de les conseqüències de les seves accions fins que ja és massa tard.

Els delictes contra la intimitat són recollits en l'article 197.1 de l'actual Codi penal (d'ara endavant, CP). Com a conseqüència de l'assimilació de la **intercepció del correu electrònic** amb la **violació de la correspondència**, aquest article disposa que les conductes següents són constitutives de delicte:

- L'apoderament de papers, cartes, **missatges de correu electrònic** o qualsevol altre document o efectes personals.
- La **intercepció de les telecomunicacions**.
- La utilització d'artificis tècnics d'escolta, transmissió, gravació o reproducció de so, o de qualsevol altre senyal de comunicació.

Per ser constitutives de delicte, aquestes activitats s'han de produir **sense el consentiment de la persona afectada** (ni autorització judicial motivada o justificada), i amb la intenció de descobrir-ne els secrets o vulnerar-ne la intimitat.

Per tant, obrir la bústia d'un correu electrònic que no sigui el nostre propi i llegir els missatges que s'hi emmagatzemen podria esdevenir una conducta constitutiva de delicte. Cal anar amb molt de compte amb aquest tipus d'accions (tècnicament solen ser molt senzilles d'efectuar, però no per això són conductes legals) i, com a norma general, mai no s'ha de llegir cap correu electrònic que no vagi adreçat a nosaltres mateixos (ni tan sols si el nostre cap, dins de l'àmbit laboral, ens ho demana).

En el cas de la intercepció del correu electrònic dins de l'àmbit empresarial, se sol argumentar que els treballadors no poden fer ús dels mitjans de l'empresa per a qüestions personals. Moltes sentències s'han pronunciat a favor de l'empresa perquè s'entén que, efectivament, els mitjans pertanyen a l'empresa i que, per tant, no és un lloc adient per enviar i rebre missatges de caràcter privat. No obstant això, davant del dubte, cal que sempre tingueu present que els correus electrònics dels treballadors de l'empresa gaudeixen de la mateixa protecció legal, pel que fa a la intimitat, que els correus electrònics personals.

Activitats personals

Aquestes activitats personals abracen també, per exemple, l'ús dels jocs inclosos per defecte en els sistemes operatius.

Una manera útil per fer saber als usuaris d'una organització quins són els usos correctes dels mitjans de l'empresa, i les seves limitacions, consisteix en l'ús de contractes en els qual s'especifica, per exemple, quines obligacions i responsabilitats té un usuari d'un compte de correu electrònic. Si com a tècnics se'ns requereix que demostrem l'ús indegut d'algun mitjà electrònic de l'organització, sempre serà preferible usar controls tan poc lesius com sigui possible, com ara el monitoratge o el seguiment del nom-

bre de bytes transmesos (o rebuts) per un usuari concret (per exemple, si un usuari descarrega arxius de vídeo o cançons, el nombre de bytes rebuts serà, probablement, molt més gran que el que seria si fes un ús adequat del correu).

Usurpació i cessió de dades reservades de caràcter personal

Els articles 197, 198, 199 i 200 del CP tipifiquen com a conductes delictives l'accés, la utilització, la modificació, la revelació, la difusió o la cessió de dades reservades de caràcter personal que es trobin emmagatzemades en fitxers, suports informàtics, electrònics o telemàtics, sempre que aquestes conductes les facin persones no autoritzades (conductes anomenades, genèricament, **abusos informàtics sobre dades personals**). A més de la responsabilitat penal en què poden derivar aquests tipus d'accions, també cal considerar que les dades personals s'han d'emmagatzemar i declarar segons una normativa especificada en la **Llei orgànica de protecció de dades personals** (LOPDP).

Vegeu la LOPDP, i també una definició més acurada de *dada personal*, en l'apartat "Marc juridic extrapenal" d'aquesta unitat.

Pel que fa al Codi penal, explícitament es fa esment de l'agreujant d'aquestes conductes quan les dades de l'objecte del delicte són de caràcter personal que revelin ideologia, religió, creences, salut, origen racial o vida sexual. Altres agreujants que cal tenir en compte es produeixen quan la víctima és un menor d'edat o incapacitat, o bé la persona que comet el delicte és el responsable dels fitxers que hi estan involucrats. Mereix una consideració especial l'article 199.2, en el qual es castiga la conducta del professional que, incomplint l'obligació de reserva, **divulga els secrets** d'una altra persona.

Article 25 CP

A l'efecte d'aquest Codi es considera incapaç tota persona, se n'hagi declarat o no la incapacitació, que pateixi una malaltia de caràcter persistent que li impedeixi governar la seva persona o béns per ella mateixa.

Podeu trobar el Codi penal traduït al català en la secció "Adreces d'interès" del web.

La revelació del secret professional és una conducta que apareix tipificada en l'article 199 del Codi penal.

En definitiva, el sentit comú ja ens avisa que aquestes accions poden tenir algun tipus de repercussió. El que probablement desconeixem és que se'n puguin derivar responsabilitats penals. Així, com a tècnics i usuaris de sistemes informàtics, és molt probable que tinguem accés a dades personals, sobre les quals tenim l'obligació de mantenir el secret i no cedir-les a ningú.

1.2.2. Delicte de frau informàtic

En l'article 248.2 CP es castiga la conducta de qui, emprant qualsevol manipulació informàtica, aconsegueixi la transferència no consentida de qualsevol bé, amb ànim de lucre i perjudici sobre tercer. També apareixen en el Codi penal les **conductes preparatòries** per a la comissió de delictes de frau informàtic, les quals poden consistir, a tall d'exemple, en la fabri-

cació, la facilitació o simplement la mera possessió de programari específic destinat a la comissió del delicte de frau informàtic.

Per exemple, l'anomenat *descaminament* (*pharming*) és una de les tècniques que es podrien englobar dins d'aquesta tipificació. Aquesta tècnica permet que un atacant pugui redirigir un nom de domini a una màquina diferent. Així, doncs, un usuari pot creure que accedeix al seu compte bancari via Internet, quan en realitat el que fa és proporcionar les seves claus d'accés a l'atacant. El desencaminament està molt relacionat amb un altre terme anomenat *pesca* (*phishing*). En aquest darrer cas, però, no estarem parlant d'una tècnica informàtica, sinó d'una estratègia d'**enginyeria social**, en la qual s'usa la suplantació de correus electrònics o pàgines web per intentar obtenir la informació confidencial de l'usuari. És a dir, a diferència del desencaminament, molt més tècnic, en la pesca l'usuari creu que introdueix les dades en el portal d'una entitat bancària, però en realitat és un portal diferent, amb una adreça diferent de la real. En el cas del desencaminament, l'usuari introdueix l'adreça real del portal d'Internet, però es produeix una redirecció a una màquina diferent.

L'enginyeria social...

... és la pràctica d'obtenir informació confidencial mitjançant la manipulació i l'engany dels usuaris legítims (per exemple, amb una trucada telefònica en la qual algú es fa passar per un administrador del sistema, se'ns demana la nostra contrasenya d'accés).

Tot i que la duplicació o clonació de les bandes magnètiques d'una targeta de crèdit podria semblar una operació similar a les anteriors, en realitat pot comportar conseqüències encara més greus, ja que, segons l'article 387 CP, aquesta acció es pot assimilar a un delicte de **falsificació de moneda**.

1.2.3. Delicte d'ús abusiu d'equipaments

L'article 256 CP castiga l'ús de qualsevol equipament terminal de telecomunicacions sense el consentiment del titular, sempre que li ocasioni un perjudici superior a 400 euros. Aquesta quantitat va ser establerta per la Llei 15/2003.

Wi-Fi

Fixeu-vos que l'aprofitament no consentit d'una connexió Wi-Fi es podria incloure dins de l'article 256 CP. Caldria, no obstant això, acreditar el perjudici econòmic que s'ha pogut produir.

1.2.4. Delicte de danys

Els delictes de danys, juntament amb els delictes contra la intimitat i contra la propietat intel·lectual, són, amb diferència, els que succeeixen amb més freqüència. De manera similar a com passa amb els que s'efectuen contra la intimitat de les persones, sovint els autors d'aquestes accions no són conscients de les conseqüències que poden comportar els delictes que cometen.

Segons l'**article 264 CP** el **delicte de danys** consisteix en la destrucció, l'alteració, la inutilització o qualsevol altra modalitat que impliqui el dany de dades, programari o documents electrònics emmagatzemats en xarxes, suports o sistemes informàtics.

Tal com ens podem imaginar, aquest delicte pot tenir repercussions econòmiques molt importants en les organitzacions afectades i, en conseqüència, les sancions d'aquestes accions poden comportar grans sumes de diners per a les persones implicades.

Els danys produïts en un sistema informàtic s'han de poder valorar i és essencial adjuntar-ne una valoració en el moment d'efectuar la denúncia davant d'un cos policial. La valoració dels danys és un procés complex de dur a terme i pot abraçar diferents aspectes: cost de restauració d'una pàgina web, pèrdues en conceptes de publicitat no emesa (**lucre cessant**), o per serveis que no s'han pogut prestar, etc. A tall d'exemple, l'alteració d'una pàgina web per una persona no autoritzada és un cas de delicte de danys. Tot i que en alguns casos pugui semblar una acció innocent (i fins i tot engrescadora, dins de l'entorn dels pirates), pot comportar pèrdues de milers d'euros.

Un pirata (*cracker*) és una persona que fa atacs a sistemes informàtics amb finalitats destructives.

Cal dir que si bé la **intrusió** en un sistema informàtic de moment no és en si mateixa constitutiva de delicte (tot i que en breu tindrà aquesta consideració), aquests tipus d'accions se solen trobar vinculades a altres conductes que sí que ho són, com, per exemple, els delictes contra la intimitat, els danys en un sistema informàtic o els mitjans que s'hagin utilitzat per dur a terme l'accés no autoritzat (com, per exemple, la detecció o *sniffing* de contrasenyes).

Exemple de danys

L'enviament d'un virus (amb la voluntat clara de causar danys), entre altres de similars, també podria tenir la consideració de delicte de danys. Tingueu present, però, que la quantitat de 400 euros marca el llindar entre la falta i el delicte.

1.2.5. Delictes contra la propietat intel·lectual

El delicte contra la propietat intel·lectual és una de les qüestions que més interès suscita entre la comunitat informàtica, ja que està vinculat amb una de les activitats més polèmiques entorn d'Internet: la descàrrega de fitxers protegits per les lleis de la propietat intel·lectual i l'ús de programaris d'intercanvis de fitxers en xarxes d'igual a igual (anomenades també *peer-to-peer* o *P2P*).

Xarxes d'igual a igual (*peer-to-peer*)

En les xarxes d'igual a igual, cada node pot efectuar alhora tasques de **servidor** i de **client**. A causa de la seva natura intrínseca, les xarxes P2P són molt adequades per compartir fitxers entre tots els usuaris que la formen, els continguts dels quals poden ser (o no) protegits per les lleis de propietat intel·lectual. Sens dubte, el programari P2P més conegut per tothom (i objecte de molta controvèrsia) és l'**eMule**, basat en la xarxa **eDonkey** (2002).

Segons l'**article 270 CP**, les conductes relatives als delictes contra la propietat intel·lectual són aquelles en què es reprodueix, plagia, distribueix o comunica públicament, tant d'una manera total com parcial, una obra literària, artística o científica sense l'autorització dels titulars dels drets de propietat intel·lectual de l'obra.

Llei de propietat intel·lectual

Dins del marc jurídic no penal, la Llei de propietat intel·lectual regula la protecció de les obres literàries, artístiques i científiques.

Aquestes condicions s'apliquen independentment del suport en què s'hagi enregistrat l'obra –textos, programaris, vídeos, sons, gràfics o qualsevol altre fitxer relacionat. És a dir, els delictes relatius a la venda, la distribució o la fabricació de còpies no autoritzades de programari són delictes contra la propietat intel·lectual. No obstant això, segons la interpretació literal del Codi penal, cal que aquestes accions s'hagin efectuat amb **ànim de lucre** i en perjudici de tercers. Així, doncs, per poder aplicar aquest article resulta essencial que es pugui demostrar l'existència d'aquest lucre. Malgrat que això no pugui ser fàcilment demostrable, recordem que, de qualsevol manera, tota obra (literària, científica o artística) és protegida per uns drets de propietat intel·lectual que cal respectar, independentment de les consideracions personals que cadascú pugui tenir amb relació a aquest tema.

Permís dels titulars

No podem fer un ús lliure de la informació que es pugui trobar a Internet, com, per exemple, gràfics, animacions, logotips, fotografies, etc., sense el permís dels titulars dels drets de propietat intel·lectual.

Exemples de delictes contra la propietat intel·lectual

Vegem alguns exemples de delictes contra la propietat intel·lectual:

- Reproducció íntegra de programari i venda al marge dels drets de llicència.
- Instal·lació de còpies no autoritzades de programari en un ordinador en el moment de la compra.
- Publicació del codi font de programari (o el programari en si mateix), o altres fitxers (MP3, llibres, etc.) a Internet, al marge dels drets de llicència d'aquestes obres.
- Utilització d'una llicència de programari per només un sol ordinador per donar servei a tota la xarxa.
- Trencament dels mecanismes de protecció que permeten el funcionament correcte del programari (motxilles o *dongles*, contrasenyes i altres elements de seguretat). Aquestes tècniques reben el nom genèric de *cracking*. Així, doncs, el terme *cracker* es referirà tant a la persona que s'introdueix en un sistema amb finalitats destructives, com a la que fa *cracks* amb la intenció de trencar els mecanismes de protecció dels programaris.

El mateix article 270 CP preveu penes per a qui faci circular o disposi de qualsevol mitjà específicament dissenyat per anul·lar qualsevol dispositiu tècnic de protecció del programari (per exemple, els programaris que permeten "saltar" les proteccions anticòpia de CD o DVD).

Una llicència de programari...

... és un contracte entre l'autor/titular dels drets d'explotació/distribuïdor i l'usuari, per utilitzar el programari segons les seves condicions d'ús.

Tot i els esforços d'alguns països de la Comunitat Europea per evitar la descàrrega i la compartició (mitjançant programaris d'igual a igual) de continguts protegits, encara no s'ha arribat a una solució de consens. No obstant això, cal aclarir que l'ús i la instal·lació de programaris d'igual a igual en els nostres ordinadors no es considera (des del punt de vista jurídic) cap pràctica il·legal. De la mateixa manera que no es prohibeix que tinguem ganivets a la cuina únicament pel fet que el seu mal ús pot ser delictiu, tampoc no se sanciona el fet d'instal·lar i usar programaris d'intercanvi de fitxers (ja que poden tenir un ús perfectament lícit). Recordem, però, que la simple tinença de qualsevol mitjà (per exemple, un programari) dissenyat per anul·lar la protecció dels programaris sí que és susceptible de ser sancionada.

Pel que fa a la **creació de programari**, també hi ha algunes consideracions que cal tenir en compte. Segons el tipus de contracte al qual es trobi subjecte el treballador, el programari que desenvolupi per a una organització determina-

da pertany a l'empresa i, en conseqüència, si el treballador abandona l'organització, no es pot emportar el programari que ha creat en el seu antic lloc de treball. Com en el cas de la utilització del correu electrònic, seria recomanable que el contracte de treball especifiqués aquesta qüestió.

Dret de còpia privada

Al nostre país està permesa la realització de còpies d'obres literàries, artístiques o científiques sense prèvia autorització dels titulars de l'obra (sempre que s'hi hagi accedit legalment) i la còpia no s'empri amb finalitats col·lectives, ni lucratives, ni amb ànim de perjudicar a tercers. No obstant això, cal tenir present que el dret de còpia privada no és aplicable a programaris (i, per tant, a videojocs tampoc). El dret a còpia privada es limita a una sola còpia.

El cànon compensatori...

... és una taxa aplicada (no sense una certa polèmica) a diversos mitjans de gravació (per exemple, els CD), la qual és percebuda pels autors, editors, productors i artistes, associats a alguna entitat privada de gestió dels drets d'autor, en compensació per les còpies que es puguin fer de les seves obres dins dels àmbits privats.

Tipus de llicències

L'ús d'una llicència no adequada (per exemple, una llicència personal en lloc d'una llicència de xarxa) pot comportar problemes diversos i no es pot argumentar el desconeixement com a eximent d'aquesta conducta. Així, doncs, caldrà estudiar quins tipus de llicències de programari diferents hi ha amb la finalitat d'adquirir-les i emprar-les adequadament segons les nostres necessitats i del pressupost de què es disposi. Vegeu-ne algunes:

Adquisició d'un programari

Quan adquirim un programari, no l'adquirim en si mateix, sinó únicament una llicència d'ús d'aquest programari, subjecte a les condicions que determina la llicència.

1) Llicències de programari no lliure.

- **OEM (*original equipment manufacturer*)**: tipus de llicència, normalment referida a sistemes operatius (encara que també es pot aplicar al maquinari), que supedita la venda del programari com a part integrant d'un equip informàtic nou (programaris preinstal·lats). Així, doncs, aquest programari no es pot vendre aïlladament, sinó juntament amb el maquinari que l'incorpora. Solen no disposar de l'embolcall de la versió normalitzada del producte. No es poden vendre ni cedir a tercers independentment del maquinari.

- ***Retail***: consisteix en les versions de venda normalitzades d'un programari, amb els embolcalls que se solen veure a les botigues d'informàtica. A diferència de les versions OEM, es poden vendre independentment del maquinari que les suporta i poden tenir algun extra que no apareix en les versions OEM.

- **Llicències per volum**: llicències destinades a empreses i institucions (com instituts i universitats). Són similars a les llicències OEM, però no estan vinculades a equips nous. Poden servir, per exemple, per instal·lar un programari d'ús comú en una xarxa d'ordinadors d'un institut.

2) Llicències de programari lliure. Segons la Free Software Foundation (Fundació pel Programari Lliure), el **programari lliure** ha de satisfer les quatre condicions següents:

- Llibertat perquè els usuaris emprin els programaris amb qualsevol propòsit.
- Llibertat per estudiar el funcionament del programari i adaptar-lo a les necessitats de cada usuari (aquesta condició requereix accedir al codi font del programari).
- Llibertat per redistribuir còpies del programari.
- Llibertat per efectuar millores dels programaris i fer-les públiques (redistribuir les còpies del programari modificat) en benefici de tota la comunitat (tal com passa amb la segona condició, aquesta també només pot ser possible si es té accés al codi font del programari).

La Free Software Foundation...

... és una organització creada l'any 1985 per Richard Stallman (entre altres defensors del programari lliure). Un dels seus principals objectius consisteix en la defensa del projecte GNU.

Així, doncs, el programari lliure es caracteritza perquè pot ser usat, estudiat i modificat sense restriccions de cap mena, es pot redistribuir en una versió modificada (o sense modificar) sense cap restricció, o amb aquelles mínimes que permetin garantir als futurs usuaris que podran gaudir de les mateixes llibertats a què hem fet referència.

El fet que un programari sigui lliure no vol pas dir que sigui **gratuït**. Per exemple, el programari gratuït pot patir certes restriccions que fa que no s'adapti a la definició de *programari lliure* abans enunciada (un programari pot ser gratuït, però podria no incloure el codi font, tal com obliguen les llibertats del programari lliure). D'altra banda, sovint trobem a la venda CD de **distribucions de Linux** (programari lliure). No obstant això, en aquest cas, el comprador podrà copiar el CD i distribuir-lo.

Programaris descatalogats (*abandonware*)

Els programaris descatalogats solen ser programaris antics, dels quals els creadors han alliberat els drets d'autor. Es poden trobar a la Xarxa, en webs dedicats i no tenen cap altra via de distribució.

Pel que fa al programari lliure, les llicències més habituals són les següents:

- **Llicències GPL (llicència pública general de GNU)**: en aquest tipus de llicències, el creador conserva els drets d'autor (*copyright*) i permet la redistribució i la modificació, però amb la condició que totes les versions modificades del programari es mantinguin sota els termes més restrictius de la llicència GNU GPL. Això implica que si un programari té parts sota llicència no GPL, el resultat final ha de ser forçosament programari sota llicència GPL.

Projecte GNU (*GNU is Not Unix*)

Iniciat per Richard Stallman, el seu objectiu va ser crear un sistema operatiu totalment lliure, anomenat **sistema GNU**. El projecte es va anunciar per primera vegada l'any 1983. Linus Torvalds, l'any 1991, va començar a escriure el nucli del sistema operatiu **Linux**, el qual va distribuir sota lli-

cència GPL. Gràcies a les aportacions de molts altres programadors, el nucli de Linux es va acabar combinant amb el sistema GNU, i va formar l'anomenat **GNU/Linux** o **distribució Linux**, paradigma dels sistemes operatius lliures.

- **Llicències BSD *(Berkeley software distribution)***: BSD identifica un sistema operatiu derivat de l'Unix, fet gràcies a les aportacions fetes per la Universitat de Califòrnia, Berkeley. Precisament, aquestes llicències s'anomenen *BSD* perquè s'utilitzen en molts programaris distribuïts amb el sistema operatiu BSD. Són llicències sense restriccions, compatibles amb les llicències GNU GPL, que proporcionen a l'usuari una llibertat il·limitada, fins i tot per redistribuir el programari com a no lliure. No obstant això, el creador manté els drets d'autor (*copyright)* pel reconeixement de l'autoria en treballs derivats.

- **Llicències MPL (*Mozilla public license*) i derivades**: aquest tipus de llicència rep el nom del projecte de programari lliure **Mozilla**, a bastament conegut per tota la comunitat d'internautes. En aquest cas, i a diferència de les llicències GPL, no cal que el producte final també sigui llicenciat en MPL. D'aquesta manera, es promou efectivament la col·laboració entre autors i la generació de programari lliure, ja que les llicències GPL presentaven el problema d'afavorir una certa expansió vírica i endogàmica a causa de l'obligació que el producte final fos també llicenciat en GPL. A més, són més restrictives que les BSD i eviten que l'usuari gaudeixi de les llibertats excessives que comporta aquesta llicència.

- **Llicències *copyleft***: en aquest cas, el propietari de la llicència gaudeix del dret de còpia, modificació i redistribució. A més, també pot desenvolupar una versió d'aquest programari (amb llicència subjecte a *copyright*) i vendre'l o cedir-lo sota qualsevol de les llicències estudiades, sense que això afecti les llicències *copyleft* ja atorgades. L'autor també pot retirar una llicència *copyleft*, encara que sense efectes retroactius, ja que l'autor no té dret a retirar el permís d'una llicència que encara es troba vigent.

1.2.6. Delicte de revelació de secrets d'empresa

Segons l'article 278.1 CP, fa **revelació de secrets d'empresa** qui, amb la finalitat de descobrir un secret d'empresa, intercepti qualsevol tipus de telecomunicació o utilitzi artificis tècnics d'escolta, transmissió, gravació o enregistrament del so, imatge o de qualsevol altre senyal de comunicació.

L'exemple més característic de la revelació de secrets d'empresa és l'espionatge industrial.

1.2.7. Delicte de defraudació dels interessos econòmics dels prestadors de serveis

La defraudació dels interessos econòmics dels prestadors de serveis és un nou delicte, introduït arran de la reforma 15/2003 del Codi penal, apareix

en l'article 286, i castiga qui faciliti a tercers l'accés a serveis interactius o audiovisuals (com, per exemple, les televisions de pagament), sense el permís dels prestadors d'aquests serveis. De fet, la simple explicació, per exemple en una pàgina web d'Internet, sobre com es poden evitar o "saltar" els mecanismes de protecció d'aquests sistemes, ja és considerada com una activitat delictiva.

1.2.8. Altres delictes i la investigació dels delictes informàtics

A més dels delictes que s'han descrit, és evident que molts altres, coneguts intuïtivament per tots nosaltres, es poden dur a terme amb el concurs de la tecnologia. En aquests casos, la tecnologia esdevé únicament el mitjà de comissió del delicte, el qual ja es troba perfectament tipificat dins dels delictes ocorreguts en el món "real":

- Amenaces i coaccions (per mitjà de xats o correus electrònics).
- Falsedat documental (alteracions i simulacions de documents públics o privats).
- Difusió de pornografia infantil a Internet (la tinença també és un delicte).

Els investigadors dels delictes informàtics (policials o d'empreses especialitzades) disposen, a grans trets, de dues fonts d'informació essencials:

- **Els fitxers o registres (*logs*) locals**: el sistemes operatius i els programaris que s'executen als ordinadors enregistren algunes de les activitats que fan en els anomenats *fitxers de registre*. Per exemple, la intrusió d'un pirata en un sistema informàtic deixaria, si l'atacant no és molt hàbil, empremtes en diversos fitxers del sistema. La informació que contenen aquests arxius (per a l'exemple l'adreça IP de l'atacant) és la primera baula que els investigadors analitzarien per tal d'arribar a establir l'origen de l'atac o el fet investigat.

- **Els registres (*logs*) dels proveïdors de servei d'Internet (PSI)**: la persona que ha comès el delicte (o qualsevol altre fet susceptible de ser investigat) haurà utilitzat la connexió oferta per un cert proveïdor de serveis d'Internet. Les dades associades a aquesta connexió són emmagatzemades pels PSI segons la **Llei de serveis de la societat de la informació i del comerç electrònic** (LSSICE), les quals només poden ser cedides als investigadors per un manament judicial. Així, doncs, una vegada els investigadors han establert la informació bàsica del succés (IP d'origen, franja horària i la data en què s'ha produït l'esdeveniment), caldrà que sol·licitin al jutge un manament judicial per tal que el proveïdor de serveis els lliuri la informació requerida (associada a la IP i a la resta de dades determinades en les etapes inicials de la inves-

Un proveïdor de serveis (PSI)...

... és una empresa dedicada a connectar els usuaris (clients) a Internet. També sol oferir, entre d'altres, serveis d'allotjament web i registre de dominis.

Vegeu l'LSSICE en l'apartat "Marc jurídic extrapenal" d'aquesta mateixa unitat.

tigació) per continuar el procés i identificar l'usuari que ha emprat la connexió sospitosa.

Si l'administrador d'un sistema informàtic és víctima de qualsevol d'aquests delictes, o bé, per exemple, descobreix que el sistema que administra és utilitzat com a plataforma de distribució de còpies de programari no autoritzades o de pornografia infantil, ho ha de denunciar immediatament a la comissaria de policia més pròxima, tenint en compte el protocol d'actuació següent:

1) Adjunció dels fitxers de registre (registres locals del sistema) relacionats amb el delicte comès. Aquests fitxers hauran de reflectir, en cas que hagin quedat registrats, la IP de l'atacant, les accions produïdes en el sistema investigat, etc.

2) En cas que s'hagi produït un delicte de danys, cal adjuntar una valoració dels danys ocasionats.

3) Actuar amb rapidesa (els proveïdors no emmagatzemen indefinidament els fitxers de registre dels seus servidors).

4) En cas que aquesta acció delictiva s'hagi produït per correu electrònic, cal adjuntar les capçaleres completes del correu rebut.

5) En cas que sigui necessari, cal considerar la possibilitat de duplicar (o clonar) el disc dur del servidor per preservar les proves del delicte i, a continuació, reinstal·lar el sistema per evitar que el delicte es continuï produint. No obstant això, cal anar amb compte amb aquesta consideració. Suposem, per exemple, que l'administrador d'un sistema descobreix que el servidor del qual és responsable allotja pornografia infantil. La duplicació del disc dur (a l'efecte de salvaguardar les proves) i la reinstal·lació posterior de tot el sistema permetrien evitar que el delicte (la difusió de pornografia infantil) es continués produint, però al mateix temps en podria dificultar la investigació.

Els usuaris domèstics també poden ser víctimes de delictes relacionats amb les noves tecnologies (contra la intimitat, amenaces, coaccions, suplantacions d'identitat, etc.). Moltes de les aplicacions per mitjà de les quals s'executen aquestes accions poden emmagatzemar els seus propis ***logs*** (per exemple, les converses de xat, capçaleres de correu electrònic), els quals caldria adjuntar en cas de denúncia.

2. Plans de manteniment i administració de la seguretat

La Constitució vol protegir d'una manera molt curosa una sèrie de drets inherents a tota persona (els anomenats **drets fonamentals**). Entre aquests destaca, entre d'altres, el **dret a la intimitat**. A més de les conseqüències penals que pot comportar la vulneració d'aquest dret, hi ha altres lleis, independentment del marc penal, que també protegeixen la privacitat de la persona en tots els seus aspectes, també pel que fa a les seves pròpies dades.

Marc extrapenal

En dret s'entén per *marc extrapenal* el sector o la branca de l'ordenament jurídic que no és penal, és a dir, que conté sancions menys greus que el dret penal (per exemple, dret administratiu, dret civil, dret laboral, etc.).

A causa d'aquest fet, la legislació és molt proteccionista amb les dades. Això afecta d'una manera negativa els sistemes informàtics, la manera com operen les organitzacions, i fins i tot el dia a dia de les persones. El conjunt de normes intenta trobar un equilibri entre aquests elements, aparentment oposats, per aconseguir un nivell de seguretat de les dades adequat, juntament amb una protecció suficient de la intimitat, i garantir a les empreses el poder operar amb la informació d'una manera eficient.

2.1. Legislació sobre protecció de dades

La protecció de les dades de caràcter personal ha pres darrerament una gran rellevància. Les persones es mostren cada dia més curoses amb les seves dades i, a la vegada, són més conscients dels drets de protecció de què ha de gaudir la seva informació personal.

Els factors que sembla que han dut a la situació actual han estat, d'una banda, la normativa en matèria de protecció de dades i, de l'altra, l'activitat creixent de l'**Agència Espanyola de Protecció de Dades**, organisme autònom encarregat d'assegurar el compliment de la legislació vigent (i fruit de la mateixa legislació).

Estem convençuts que per dur a terme una tasca professional de qualitat és molt important (i fins i tot ens atreviríem a dir que imprescindible) conèixer la normativa espanyola aplicable a la protecció de dades de caràcter personal.

Què és una dada de caràcter personal?

Segons la Llei orgànica de protecció de dades de caràcter personal (LOPDP), és qualsevol informació concernent a persones físiques identificades o identificables.

Una de les lleis més importants encaminada a protegir la intimitat de les persones és la **Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPDP)**. Aquesta norma té per objecte garantir i protegir, amb relació al tractament de dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i en especial el seu honor, intimitat i privacitat.

Aquesta llei apareix com a conseqüència de l'existència de l'article 18, apartat 4 de la Constitució, i de la Directiva europea 94/46 de 24 d'octubre del Parlament Europeu i del Consell, relativa a la protecció de les persones físiques i referida al tractament de dades personals i a la lliure circulació de les seves dades.

Aquesta directiva és una norma d'àmbit europeu per protegir les dades personals i per garantir el flux de dades entre els països de la Unió Europea. Per tant, els països necessiten **integrar** aquesta directiva a les seves legislacions. El resultat és la **Llei orgànica de protecció de dades** (15/1999) i l'aparegut recentment **Reglament d'aplicació de mesures de seguretat tècniques i organitzatives** (1720/2007). Aquest reglament desenvolupa aquesta llei orgànica i estableix l'obligació de les organitzacions d'engegar diverses mesures destinades a garantir la protecció d'aquestes dades, que afectin sistemes informàtics, arxius de suport d'emmagatzemament, personal i procediments operatius.

Directiva comunitària (o directiva de la Unió Europea)

És una decisió col·lectiva mútuament obligatòria aprovada pels estats membres de la Unió Europea. Obliga que tots els estats membres assoleixin, totalment o parcialment, els objectius de la directiva. No obstant això, cada estat pot triar la forma i els mitjans per arribar a assolir-los. Les directives, doncs, proporcionen un **marc normatiu** que cada país ha de desenvolupar, tenint en compte les seves característiques específiques, però, al mateix temps, respectant els límits de la directiva.

La LOPDP és aplicable a qualsevol informació sobre persones físiques identificades o identificables (nom, cognoms, edat, sexe, dades d'identificació fiscals, estat civil, professió, domicili...) que aparegui enregistrada en qualsevol suport físic (inclòs el paper), que en permeti el tractament (conjunt d'operacions que es poden dur a terme sobre les dades) manual o automatitzat i ús posterior pel sector públic o privat. Traspassat a l'àmbit de les empreses, s'ha d'interpretar que la LOPDP és aplicable a qualsevol organització que manipuli o arxivi fitxers, tant en paper com en suport magnètic, que continguin informació o dades de caràcter personal, tant dels seus empleats, clients o proveïdors (persones físiques), la qual cosa obliga les empreses, institucions, professionals i, en general, totes les persones jurídiques o físiques, que operin sobre fitxers de dades de caràcter personal, al compliment d'una sèrie d'obligacions legals.

Reviseu el subapartat "El Codi penal i les conductes il·lícites vinculades a la informàtica" d'aquesta mateixa unitat.

Què és un *fitxer automatitzat*?

Segons la Llei orgànica de protecció de dades de caràcter personal (LOPDP), un fitxer és qualsevol conjunt organitzat de dades de caràcter personal, amb independència de la forma o modalitat de la seva creació, emmagatzemament, organització i accés (article 5). Un fitxer pot ser un CD-ROM, un disquet o fins i tot un quadern.

Si el tractament és automatitzat, llavors serà un fitxer automatitzat per a l'usuari.

Les mesures de seguretat...

... que han de satisfer els fitxers que continguin dades de caràcter personal es refereixen d'una manera genèrica a tots els fitxers que continguin aquestes dades personals, no tan sols aquells als quals es pot accedir des d'Internet.

Tinc una agenda personal...

... amb gran quantitat de dades de persones físiques, ho he de notificar a l'Agència de Protecció de Dades?

La LOPDP recull una sèrie d'exclusions, entre d'altres hi ha els fitxers mantinguts per persones físiques en l'exercici d'activitats exclusivament personals o domèstiques.

2.1.1. Objectiu de la normativa

L'**objectiu de la LOPDP** és el de garantir i protegir la privadesa i la intimitat de les persones físiques.

L'**objectiu del reglament** (que desenvolupa la LOPDP) és el d'establir les mesures tècniques i organitzatives necessàries per garantir la seguretat

dels fitxers i dels sistemes que prenguin part en el tractament de dades de caràcter personal.

Per **tractament** s'entendrà el conjunt d'operacions i procediments tècnics de caràcter automatitzat o no que permetin la recollida, la gravació, la conservació, l'elaboració, la modificació, el bloqueig i la cancel·lació de dades.

Cancel·lació i bloqueig de dades

Procediment en virtut del qual el responsable cessa en l'ús de les dades. La cancel·lació implicarà el bloqueig de les dades, el qual consisteix a identificar-les i reservar-les amb la finalitat d'impedir-ne el tractament, excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a l'atenció de les possibles responsabilitats nascudes del tractament, i només durant el termini de prescripció de les responsabilitats esmentades. Transcorregut aquest termini, caldrà eliminar efectivament les dades.

La LOPDP distingeix entre el **responsable dels fitxers** i el **responsable de la seguretat dels fitxers**. A la vegada, el responsable dels fitxers es desdobla en dues figures que no cal que siguin coincidents: el **responsable del fitxer o tractament** (per exemple, l'empresa Editorial Nova) i **l'encarregat del tractament** (per exemple, una altra empresa, Gestions Informàtiques, contractada per l'empresa Editorial Nova amb la finalitat d'efectuar el tractament de les dades). Finalment, el responsable de seguretat dels fitxers és la persona o persones a les quals el responsable dels fitxers ha assignat la funció de coordinar i controlar les mesures de seguretat aplicables.

2.1.2. Principis bàsics de la LOPDP

El principis i directrius en què es fonamenta la LOPDP són els següents:

- **Principi de qualitat de les dades**: les dades de caràcter personal només es poden recollir per al seu tractament, i també sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives amb relació a l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'hagin obtingut.

- **Finalitat expressa**: les dades de caràcter personal objecte de tractament no poden ser usades per a finalitats que no siguin compatibles amb aquelles per a les quals les dades s'han recollit. Es consideren compatibles, tanmateix, el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques.

- **Actualitat de les dades**: les dades personals que s'incorporin en un fitxer han de respondre a una situació actual.

- **Principi d'exactitud**: les dades personals han de ser susceptibles de modificació i de rectificació des del moment en què es coneix la modificació.

- **Deure d'informació a la persona afectada**: les persones interessades a les quals se sol·licitin dades de caràcter personal hauran de ser advertides prèviament de manera expressa, precisa i inequívoca:

  – Que les seves dades seran incloses en un fitxer, de la finalitat de la recollida i dels destinataris de la informació.

– De l'obligatorietat o el caràcter voluntari de donar aquestes dades.
– De les conseqüències que porten aparellades l'obtenció de les dades o de la negativa a subministrar-les.
– De la possibilitat d'exercir els **drets d'accés, rectificació, cancel·lació i oposició** (drets ARCO).
– De la identificació, i també de l'adreça de la persona encarregada de dur a terme el tractament del fitxer o, si escau, del seu representant, perquè els afectats puguin exercir els seus drets.

Drets ARCO

Són el conjunt de drets (accés, rectificació, cancel·lació i oposició) a partir dels quals la LOPDP garanteix a les persones el control sobre les seves dades personals.

- **Necessitat de consentiment de la persona afectada**: el tractament de les dades requereix el consentiment de la persona afectada, llevat que la llei disposi una altra cosa. Igualment, és exigible que perquè les dades estiguin especialment protegides, sigui necessari donar el **consentiment exprés i per escrit**, donada la seva importància.

Excepcions del consentiment

- Prevenció/diagnòstic mèdic.
- Prestació d'assistència sanitària o tractaments mèdics.
- Gestió de serveis sanitaris.

En tots els casos, el professional està subjecte al deure de secret.

2.2. Mecanismes de control d'accés a informació personal emmagatzemada

La protecció de les dades personals passa per controlar-ne l'accés, el qual només hauria de poder ser fet pels usuaris autoritzats. La primera mesura que, intuïtivament, se'ns pot ocórrer per protegir-nos dels accessos no autoritzats consisteix en el control dels accessos físics als sistemes informàtics. De fet, a més de ser la mesura més intuïtiva, també és una de les més importants i la que amb més freqüència es descuida. Penseu que una organització pot invertir molts diners en programaris que evitin i detectin els accessos informàtics no autoritzats als seus equipaments, però tota aquesta despesa no servirà de res si els recursos físics del sistema es troben a l'abast de tothom.

El maquinari sol ser l'element més car d'un sistema informàtic i, per tant, cal tenir una cura especial amb les persones que hi tenen accés material. Una persona no autoritzada que accedís al sistema podria causar pèrdues enormes: robatori d'ordinadors, introducció de programari maliciós en el servidor (per exemple, un cavall de Troia o un *key logger*), destrucció de dades, etc.

Un *key logger* és un programari o maquinari que enregistra l'activitat d'un teclat d'una estació de treball.

Els cavalls de Troia

Els cavalls de Troia són parts de codi inserides en el programari que habitualment s'utilitza en el sistema. Aquest codi es manté ocult i duu a terme tasques sense que l'usuari o l'administrador se n'adonin. Camuflats sota l'aparença d'un programari útil o habitual, no solen ocasionar efectes destructius. Generalment, capturen contrasenyes i altres dades confidencials i les envien per correu electrònic a la persona que ha introduït el cavall de Troia dins del sistema atacat.

Per evitar aquest tipus de problema es poden adoptar diverses mesures, moltes d'elles de sentit comú, com, per exemple, les següents:

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.

- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic (útil en casos de robatori).
- Protegir i aïllar el cablatge de la xarxa (tant per protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància.
- Utilitzar contrasenyes en els estalvis de pantalla.
- Utilitzar contrasenyes de BIOS.
- Desactivar les opcions d'autocompletar i recordar contrasenyes dels navegadors d'Internet.
- Triar una topologia de xarxa adequada a les nostres necessitats de seguretat.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Mantenir el sistema informàtic actualitzat.
- Tenir mecanismes d'**autenticació** per als usuaris que volen accedir al sistema.

La BIOS (*basic input-output system*)...

... és un programa emmagatzemat en un xip ROM que s'encarrega, en el moment en què l'ordinador s'inicia, de carregar el sistema operatiu a la memòria de l'ordinador i comprovar els dispositius que té connectats.

Vegeu les pautes de manteniment d'un sistema informàtic en la secció "Annexos" del web.

S'anomena **autenticació** el procés de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic.

Situació d'un mecanisme d'autenticació

Hi ha diversos nivells en els quals es pot situar un mecanisme d'autenticació:

- Instal·lat a la BIOS.
- Instal·lat en el sector d'arrencada de l'equip.
- Sol·licitat pel sistema operatiu.
- Sol·licitat per un programari.

De mecanismes d'autenticació, n'hi ha de molts tipus diferents, des del més barats i senzills (com, per exemple, un nom d'usuari i una contrasenya) fins als més cars i complexos (com, per exemple, un analitzador de retina). Com sempre, segons els objectius i el pressupost de l'organització, cal triar el que més s'ajusti a les nostres necessitats. També cal tenir en compte que molts d'aquestes mecanismes són complementaris i es poden utilitzar alhora.

2.2.1. Mecanismes d'autenticació d'usuaris

Una xifra o criptosistema...

... és un mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un text xifrat o criptograma, il·legible si no es disposa de les claus de desxifratge.

Hi ha diversos mecanismes d'autenticació d'usuaris. Els podem classificar de la manera següent:

1) Sistemes basats en elements coneguts per l'usuari. El principal mecanisme dins d'aquest tipus d'autenticació són els sistemes basats en **con-**

trasenyes. És un dels mètodes que es fan servir més sovint per autenticar un usuari que vol accedir a un sistema. Òbviament, és el mètode més barat, però també és el més vulnerable, ja que encara que la paraula de pas o contrasenya hauria de ser personal i intransferible, sovint acaba en poder de persones no autoritzades. D'altra banda, encara que les contrasenyes s'emmagatzemin **xifrades** en un fitxer, és possible desxifrar-les amb múltiples tècniques.

Tot i que l'assignació de les contrasenyes als usuaris es basa en el sentit comú, no és sobrer tenir en compte les recomanacions següents:

Molts usuaris poc curosos anoten les contrasenyes en notes adhesives penjades al monitor de l'ordinador.

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No repetir la mateixa contrasenya en comptes diferents.
- No llençar documents amb contrasenyes a la paperera.
- Evitar utilitzar **paraules de diccionari** (hi ha tècniques de descobriment de contrasenyes basades en la comparació amb diccionaris sencers de paraules).
- Evitar utilitzar dades que puguin ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el *login*, DNI, número de mòbil, etc.).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament numèriques.
- Afavorir l'aparició de caràcters especials (¡, *, ?, etc.).
- No utilitzar seqüències de teclat del tipus "*qwerty*".
- Fer servir mnemotècnics per recordar les contrasenyes.

Molts sistemes informàtics forcen els usuaris a triar contrasenyes amb un cert nivell de robustesa: obliguen a canviar la contrasenya cada cert temps, que tingui un nombre mínim de caràcters, etc.

2) Sistemes basats en elements que té l'usuari. En aquest cas, l'autenticació no es farà d'acord amb el que recorda o coneix un usuari, sinó a partir d'un dispositiu que porta al damunt (el qual també pot requerir la introducció d'una contrasenya o d'un número PIN), o bé a partir de les pròpies característiques físiques de l'usuari (sistemes **biomètrics**).

El PIN (*personal identification number*)...

... és una contrasenya numèrica, sovint format per quatre xifres, com, per exemple, el codi numèric que ens cal introduir en un caixer automàtic.

a) Sistemes basats en targetes intel·ligents i testimonis (*tokens*) de seguretat. Una targeta intel·ligent (*smartcard*) és similar a una targeta de crèdit, però a diferència d'aquesta, les targetes intel·ligents allotgen un microprocessador (i memòria) que les dota de les característiques següents:

- Capacitat per fer càlculs criptogràfics sobre la informació que emmagatzemen.

La criptografia és la ciència i l'estudi de l'escriptura secreta.

- Emmagatzematge xifrat de la informació.
- Protecció física i lògica (mitjançant una clau d'accés) a la informació emmagatzemada.
- Capacitat per emmagatzemar claus de signatura digital i xifratge.

La signatura digital és un mecanisme de xifratge emprat per autenticar una informació digital.

És un mètode d'autenticació que cada vegada fan servir més les organitzacions, tot i el cost d'adaptació de la infraestructura als dispositius que permeten la lectura de les targetes. Un exemple de targeta intel·ligent és el DNI (document nacional d'identitat) electrònic espanyol (també anomenat *DNIe*).

Per comprendre millor els conceptes de *criptografia* i *signatura digital*, vegeu el subapartat "Protecció de dades" d'aquesta mateixa unitat.

A més, les targetes intel·ligents poden ser de **contacte** (és a dir, han de ser inserides en la ranura d'un lector perquè puguin ser llegides), o **sense contacte**. Aquest segon tipus de targetes s'ha començat a emprar amb èxit en diversos països com a sistema de pagament en el transport públic.

DNI electrònic expedit a Espanya, del qual s'han esborrat la fotografia i les dades identificatives del titular.

RFID

RFID (*radio frequency identification*, identificació per radiofreqüència) és un sistema d'emmagatzemament i de recuperació de dades remot que usen uns dispositius anomenats **etiquetes RFID**. Aquests dispositius es poden col·locar, per exemple, a la roba d'una persona (o qualsevol altre objecte) amb finalitats d'autenticació.

Una altra solució per resoldre el problema de l'autenticació, força popular en el sector empresarial, consisteix en l'anomenat *testimoni de seguretat* (*security token*). Solen ser dispositius físics de mida reduïda (alguns inclouen un teclat per introduir una clau numèrica o PIN), similars a un clauer, que calculen contrasenyes d'un únic ús (canvien a cada *login* o bé cada cert temps). També poden emmagatzemar **claus criptogràfiques**, com per exemple, la **signatura digital** o **mesures biomètriques**.

Dispositiu de lectura de targetes intel·ligents incorporat en un teclat d'ordinador.

b) Sistemes biomètrics. Els sistemes biomètrics es basen en les característiques físiques de l'usuari que s'ha d'autenticar (o en patrons característics que puguin ser reconeguts com, per exemple, la signatura). Com a principal avantatge, l'usuari no ha de recordar cap contrasenya, ni cal que porti cap testimoni o targeta al damunt. Solen ser més cars que els mètodes anteriors; per aquest motiu, encara no es fan servir gaire, tot i que alguns d'aquests mètodes ofereixen un alt nivell de seguretat a un preu econòmic molt raonable (per exemple, el **reconeixement dactilar**). Entre les diferents característiques que es poden utilitzar per reconèixer un usuari mitjançant mesures biomètriques destaquem les següents:

- Veu
- Olor corporal
- Escriptura
- Empremtes dactilars
- Patrons de la retina o de l'iris

Mesures biomètriques

Les mesures biomètriques són dades personals i caldrà que s'emmagatzemin segons es determina en la Llei orgànica de protecció de dades personals (LOPDP).

- Geometria de la mà
- Estructura facial
- Traçat de les venes

Lector d'empremtes dactilars incorporat en un ordinador portàtil.

2.2.2. Protecció de dades

Per aconseguir que la informació només sigui accessible als usuaris autoritzats i evitar que la informació en clar (és a dir, sense xifrar) que circula per una xarxa pugui ser interceptada per un espia, es poden usar diversos **mètodes criptogràfics**.

Una **xifra o criptosistema** és un mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un **text xifrat** o **criptograma.** El procés de transformar un text en clar en text xifrat s'anomena **xifratge**, i el procés invers, és a dir, la transformació del text xifrat en text en clar, s'anomena **desxifratge**. Tant el xifratge com el desxifratge són controlats per una o més **claus criptogràfiques**.

S'anomena **criptografia** la ciència i l'estudi de l'escriptura secreta. Juntament amb la **criptoanàlisi** (tècnica que té com a objectiu esbrinar la clau d'un criptograma a partir del text en clar i del text xifrat) formen el que es coneix amb el nom de **criptologia**.

Podeu trobar un exemple excel·lent i divertit de criptoanàlisi en el relat "L'escarabat d'or" d'Edgar Allan Poe.

Per protegir la confidencialitat de les dades (emmagatzemades o que circulen per la xarxa) es poden fer servir criptosistemes de **clau privada** (simètrics) o de **clau pública** (asimètrics).

1) Criptosistemes de clau privada o simètrics

Els **criptosistemes de clau privada o compartida** (o simètrics) són aquells en els quals emissor i receptor comparteixen una única clau. És a dir, el receptor podrà desxifrar el missatge rebut si i només si coneix la clau amb la qual l'emissor ha xifrat el missatge.

L'algorisme més representatiu dels criptosistemes de clau privada és el *data encryption standard* (DES), que data de l'any 1977. Actualment es troba en desús, ja que no és segur. En lloc del DES s'utilitza una variant anomenada *Triple DES*, o altres algorismes com, per exemple, IDEA, CAST, *Blowfish*, etc. No obstant això, l'estàndard actual (des de l'any 2002), adoptat com a tal pel Govern dels Estats Units, és l'anomenat *advanced encryption standard* (AES), representat per l'algorisme *Rijndael*.

2) Criptosistemes de clau pública. A diferència dels criptosistemes de clau privada, molt intuïtius i amb força desavantatges, els de clau pública són conceptualment molt enginyosos, elegants i aporten més funcionalitats que els asimètrics. No obstant això, són força lents, comparats amb els simètrics i moltes vegades no s'utilitzen per xifrar, sinó per intercanviar claus criptogràfiques en els protocols de comunicacions. La criptografia de clau pública va ser introduïda per Diffie i Hellman l'any 1976.

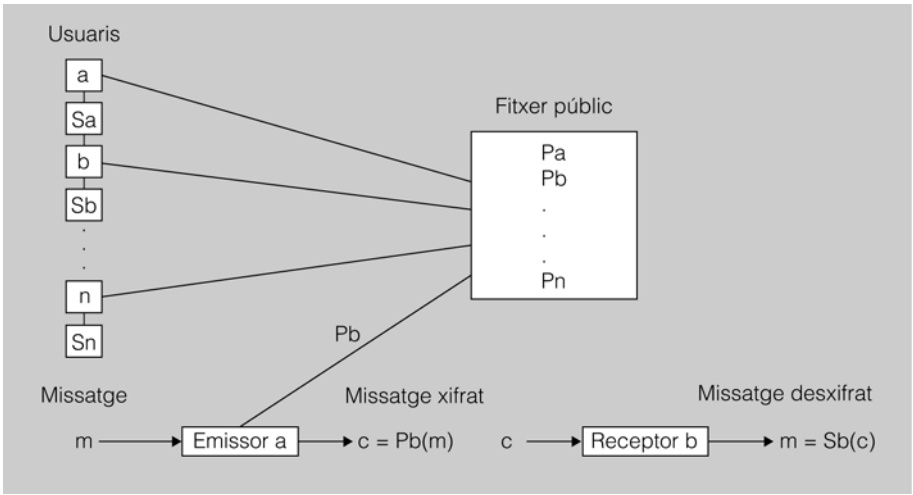
Criptosistemes de clau pública

Els **criptosistemes de clau pública** (o asimètrics) són un tipus de criptosistemes en què cada usuari u té associada una parella de claus $<P_u, S_u>$. La clau pública, P_u, és accessible per a tots els usuaris de la Xarxa i apareix en un directori públic, mentre que la clau privada, S_u, tan sols és coneguda per l'usuari u (és a dir, l'usuari propietari del parell de claus).

Donada qualsevol clau del parell $<P_u, S_u>$, no és possible esbrinar-ne una a partir de l'altra. És a dir, a partir del coneixement de la clau pública (visible per tothom), P_u,no és possible obtenir la clau privada o S_u.

Quan un usuari A vol enviar un missatge a un usuari B, xifra el missatge fent servir la clau pública de B (recordeu que aquesta clau és coneguda per tots els usuaris del criptosistema). Quan el receptor rebi el missatge, únicament el podrà desxifrar ell mateix, utilitzant la seva pròpia clau privada (la qual es troba exclusivament en el seu poder). Podeu veure aquest mecanisme descrit en la figura 1.

Figura 1. Xifratge i desxifratge d'un missatge en un criptosistema de clau pública



A més, l'usuari A podrà signar el seu missatge mitjançant la seva clau privada (només coneguda per ell), que acredita la seva identitat davant de l'usuari receptor del missatge. En el procés de verificació, el receptor (l'usuari B) emprarà la clau pública de l'usuari A, coneguda per tots els usuaris del criptosistema.

El criptosistema de clau pública més conegut és l'anomenat *RSA*, però n'hi ha d'altres com, per exemple, el criptosistema *digital signature algorithm* (*DSA*).

El criptosistema RSA va ser ideat per Rivest, Shamir i Adlerman l'any 1978.

Un avantatge molt important del criptosistema de clau pública és que permet la incorporació de **signatura digital**. Cada usuari podrà signar digitalment el seu missatge amb la seva clau privada i aquesta signatura podrà ser verificada més tard, de manera que l'usuari que l'ha originat no pugui negar que s'ha produït (**propietat de no-repudiació**).

El *digital signature standard* (DSS)...

... és un sistema de signatura digital adoptat com a estàndard pel NIST (National Institute of Standards and Technology). Utilitza l'algorisme DSA.

Certificat digital

A l'hora d'utilitzar la clau pública d'un usuari, com podem saber que és autèntica? Per resoldre aquest problema es requereix la participació d'una tercera part (anomenada **autoritat de certificació**) que confirmi l'autenticitat de la clau pública d'un usuari amb l'expedició d'un **certificat digital**. Aquest document, signat digitalment per un prestador de serveis de certificació, vincula unívocament unes dades de verificació de signatura al titular, que en confirma la identitat en qualsevol transacció telemàtica que es pugui fer.

2.3. Tractament i manteniment de fitxers de dades

Els sistemes informàtics, encarregats del tractament i del manteniment de dades, molt probablement gestionaran dades de caràcter personal. Quan ens trobem en aquesta situació, hem de complir la LOPDP. Com que el tractament es fa en fitxers de l'empresa, la llei ens diu en l'article 9.1, que hem de prendre les mesures necessàries per tal de garantir la seguretat de les dades de caràcter personal.

Les mesures, per tant, hauran d'incloure la seguretat de les dades en aspectes com la conservació, el robatori, l'alteració o l'accés no autoritzat, i també el tractament durant la seva vida útil. La LOPDP, en l'article 3, defineix el **tractament de dades**.

Article 3. Definicions

c) "Les operacions i els procediments tècnics de caràcter automatitzat o no, que permetin recollir, gravar, conservar, elaborar, modificar, bloquejar i cancel·lar, i també les cessions de dades que derivin de comunicacions, consultes, interconnexions i transferències."

Podeu trobar la LOPDP en català en la secció "Adreces d'interès" del web.

El tractament, per tant, comprèn qualsevol ús, des del moment de la recollida fins al moment de la cancel·lació. I hi ha moltes maneres de fer aquest tractament de dades: des del sistema d'emmagatzematge tradicional en suport paper, fins a les bases de dades més modernes distribuïdes, instal·lades en servidors en malla.

El tractament i el manteniment de dades, d'acord amb el que diu la LOPDP, es pot dividir en dues parts clarament diferenciades.

- **Tractament inicial**: de primer cal determinar el tipus de dades, crear el fitxer o els fitxers i declarar-los a l'**Agència de Protecció de Dades** i establir les mesures de seguretat adients.

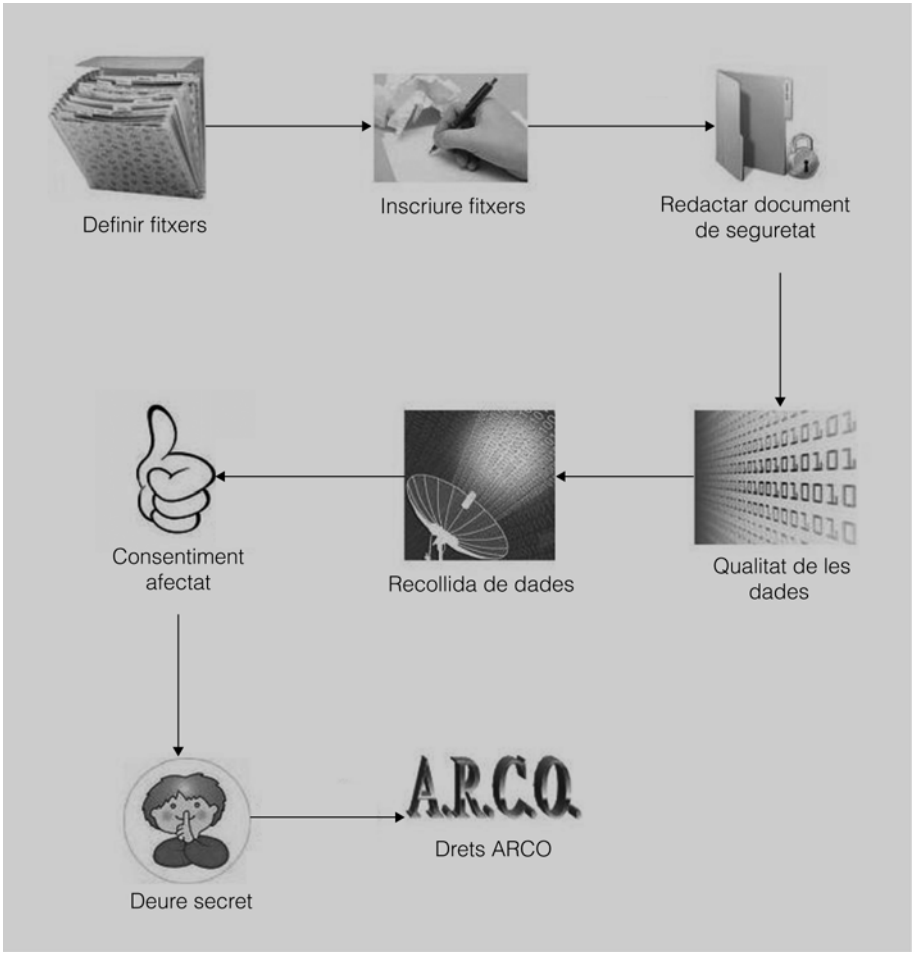
- **Manteniment**: tan bon punt tinguem el fitxer registrat, cal donar els permisos adients a les persones que necessitin tenir accés a la informació.

2.3.1. Tractament inicial

Els passos esquemàtics per dur a terme aquest tractament que ens permetrà fer un ús i un manteniment efectius de la informació són els que podeu veure en l'esquema de la figura 2.

En la secció "Annexos" del web trobareu un esquema amb una explicació breu dels passos que us pot ajudar a una comprensió millor.

Figura 2. Tractament inicial de les dades



1) Definició i establiment dels fitxers. La Llei identifica tres nivells de mesures de seguretat, **bàsic**, **intermedi** i **alt**, els quals hauran de ser adoptats en funció dels diferents tipus de dades personals.

- **Nivell bàsic***:* consisteix en la implantació de **mesures d'autenticació i control d'accés** per als usuaris que han d'accedir al fitxer amb contingut sensible, i també en l'elaboració de **protocols d'actuació** sobre el fitxer que permetin la identificació de possibles responsables en les incidències que es produeixin en la manipulació de les dades. Aquest nivell és exigible en la gestió de tots els fitxers que emmagatzemen dades de caràcter personal. Les mesures de nivell bàsic i el

Reviseu el subapartat "Mecanismes de control d'accés a informació personal emmagatzemada" d'aquesta mateixa unitat formativa.

tipus de dades que en podrien resultar afectades es recullen en la taula 1.

Taula 1. Mesures de seguretat de nivell bàsic

	Nivell bàsic
Tipus de dades	• Nom • Cognoms • Adreces de contacte (tant físiques com electròniques) • Telèfon (tant fix com mòbil) • Núm. de compte corrent • D'altres
Mesures de seguretat obligatòries	• Document de seguretat • Règim de funcions i obligacions del personal • Registre d'incidències • Identificació i autenticació d'usuaris • Control d'accés • Gestió de suports • Còpies de seguretat i recuperació

- **Nivell intermedi**: en aquest nivell de seguretat, l'administrador ha d'elaborar un **catàleg** sobre les mesures de seguretat genèriques que s'han de dur a terme i implementar **mecanismes d'autenticació remota** segurs. A més, aquestes mesures s'han de sotmetre, com a mínim cada dos anys, a una **auditoria externa** que certifiqui l'eficàcia de les mesures de seguretat que s'han pres. Són mesures exigibles per a tots els fitxers que emmagatzemin dades relatives a la comissió de delictes o infraccions administratives, Hisenda pública, serveis financers i els relatius a la solvència patrimonial i el crèdit. Les mesures de nivell intermedi i el tipus de dades que en podrien resultar afectades es recullen en la taula 2.

Taula 2. Mesures de seguretat de nivell intermedi

	Nivell intermedi
Tipus de dades	• Comissió d'infraccions penals • Comissió d'infraccions administratives • Informació d'Hisenda pública • Informació de serveis financers
Mesures de seguretat obligatòries	• Mesures de seguretat de nivell bàsic • Auditoria bianual • Mesures addicionals d'identificació i autenticació d'usuaris • Control d'accés físic • Mesures addicionals de gestió de suports • Registre d'incidències • Proves sense dades reals

- **Nivell alt**: per protegir els fitxers situats en aquest nivell cal l'ús de **mètodes criptogràfics** per evitar que les dades sensibles siguin intel·ligibles i no puguin ser alterades o capturades mentre circulen per una xarxa. Pertanyen a aquest nivell les dades relatives a ideologia, creences, origen racial, salut, vida sexual o les obtingudes amb finalitats policíaques. Les mesures de nivell alt i el tipus de dades que en podrien resultar afectades es recullen en la taula 3.

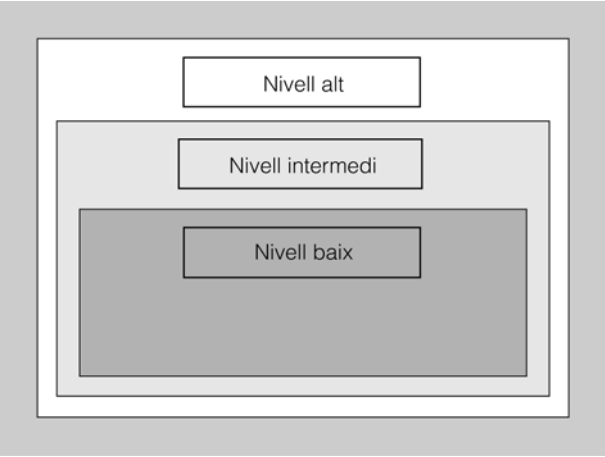
Taula 3. Mesures de seguretat de nivell alt

	Nivell alt
Tipus de dades	• Ideologia • Religió • Creences • Origen racial • Salut • Vida
Mesures de seguretat obligatòries	• Mesures de seguretat de nivell bàsic i intermedi • Seguretat en la distribució de suports • Registre d'accessos • Mesures addicionals de còpies de suport • Xifratge de telecomunicacions

Una vegada identificats els fitxers i el nivell al qual pertanyen, des del punt vista de la seguretat informàtica i la LOPDP, cal fer el **document de seguretat**. Aquest s'ha de veure com una part de la política de seguretat de l'organització, que estableix el conjunt de procediments i actuacions davant d'incidències que poden succeir en el sistema informàtic.

Les mesures de seguretat descrites en aquest apartat són **acumulatives** i, per tant, les podem veure segons el gràfic de la figura 3 (és a dir, les de nivell 3 també inclouen les de nivell 1 i 2, i les de nivell 2 les de nivell 1).

Figura 3. Nivells de mesures de seguretat previstos en la LOPDP



2) Inscripció de fitxers a l'Agència Espanyola de Protecció de Dades. L'Agència Espanyola de Protecció de Dades (AEPD) és l'autoritat de control independent que vetlla, al nostre país, pel compliment de la normativa sobre protecció de dades i garanteix i tutela el dret fonamental a la protecció de dades de caràcter personal.

A causa de la quantitat de tasques de coordinació i d'assessorament en matèria de LOPDP existent, també s'han creat les **agències de protecció de dades autonòmiques**.

Pel que fa al procés d'**inscripció de fitxers**, les competències de les agències autonòmiques es limiten al registre de fitxers del sector públic autonòmic i local, mentre que l'Agència Espanyola de Protecció de Dades té competències sobre els fitxers del sector privat i del sector públic estatal.

!!

Per tal de trobar més informació sobre l'Agència Espanyola de Protecció de Dades, consulteu la secció "Adreces d'interès" del web.

Agències Autonòmiques

A data d'avui no totes les comunitats autònomes han creat les seves agències de protecció de dades. Catalunya té la seva pròpia agència, anomenada *Agència Catalana de Protecció de Dades*.

Una vegada hem localitzat i determinat els fitxers de dades de caràcter personal, procedirem a la notificació a l'Agència de Protecció de Dades per a la seva inscripció.

El **responsable del fitxer** procedirà a la seva notificació mitjançant un model normalitzat (imprès) que es remetrà a l'Agència de Protecció de Dades per escrit, en suport informàtic o per Internet. L'Agència de Protecció de Dades inscriu el fitxer si la notificació s'ajusta al que disposa la Llei i, en cas contrari, pot demanar que es completin o se solucionin les dades notificades que estiguin incompletes o siguin incorrectes.

Transcorregut un mes des de la presentació de la sol·licitud d'inscripció del fitxer sense que l'Agència de Protecció de Dades hagi resolt res, s'entén inscrit el fitxer a tots els efectes legals.

3) Redacció del document de seguretat. Una vegada rebuda la confirmació de la inscripció, redactarem el document de seguretat.

El **document de seguretat** és un document que ha d'elaborar la figura del **responsable del fitxer**. Estableix i implanta les mesures de seguretat que s'han d'aplicar a les dades de caràcter personal i als sistemes d'informació. El contingut del document de seguretat serà diferent segons el nivell de seguretat que sigui aplicable en cada cas. És d'obligat compliment per a totes les persones que tinguin accés al fitxer de dades.

La mateixa Agència de Protecció de Dades facilita un model per a la creació del document de seguretat.

El responsable del fitxer no solament està obligat a elaborar el document de seguretat, sinó també a mantenir-lo constantment actualitzat, i a reflectir-hi qualsevol canvi rellevant que es produeixi en els sistemes d'informació.

S'ha de considerar el document de seguretat com una part molt important de qualsevol política de protecció de dades de caràcter personal. Conté les polítiques, les normes i els procediments pel quals s'ha de regir l'organització en el tractament de les dades. S'hi recullen totes les mesures de caràcter tècnic, jurídic i organitzatiu que una organització adopta per protegir i garantir la seguretat de les dades personals que hi pugui haver, tant en els seus sistemes d'informació com en els seus fitxers manuals o no automatitzats.

El document té dues parts. Un text que conté les obligacions del personal, obligacions generals, mesures que cal adoptar, etc., i un llibre en el qual es duu a terme el **registre d'incidents**. La Llei diu que és el responsable del fitxer (en el nivell bàsic) o el responsable de seguretat qui s'ha de cuidar del document de seguretat.

a) Contingut del document de seguretat. El contingut del document de seguretat varia una mica segons el nivell de seguretat. No obstant això, ser-

veix de guia (fins i tot per elaborar el document per als altres nivells), saber què ha de contenir el document en el nivell bàsic.

b) Àmbit d'aplicació del document de seguretat. El document de seguretat ha de definir el seu àmbit d'actuació i especificar amb detall els recursos protegits. Per fer-nos una idea, ha de contenir:

- Empresa/es, entitat/s o organització/ns de qualsevol tipus a què s'aplica el document de seguretat.

- Identificació del responsable del fitxer i la seva ubicació física dins de l'entitat.

- Identificació i ubicació de les persones que pel fet de tenir accés a les dades els siguin d'aplicació les mesures de seguretat que hi ha en el document.

c) Mesures, normes i procediments de seguretat. El document de seguretat ha d'incloure el conjunt de mesures, normes, procediments, regles i estàndards que ens garanteixin el nivell de seguretat exigit en el **Reglament de mesures de seguretat,** d'acord amb el nivell de seguretat aplicable.

- Descriurem el sistema informàtic emprat per accedir als fitxers de dades i indicarem els equips informàtics existents (aïllats o connectats en xarxa) i les seves característiques tècniques (sistema operatiu usat, sistemes de protecció com antivirus o tallafocs, etc.). Indicarem si hi ha connexions remotes, i també el tipus (ADSL, etc.). També descriurem els elements de xarxa (encaminadors, tallafocs, etc.) i les seves característiques tècniques.

- Documentarem les mesures de seguretat existents, tant les mesures de seguretat físiques del local on s'ubiquin els fitxers, com les mesures de seguretat de què disposi el sistema informàtic.

d) Funcions i obligacions del personal

- Es farà esment de totes les persones que tinguin accés a les dades incloses en el fitxer i s'indicaran les funcions i obligacions d'accés de cadascuna d'elles amb relació a les dades.

- També s'esmentarà qualsevol altra persona o empresa aliena a l'organització que tingui accés a les dades.

e) Estructura dels fitxers. El document de seguretat contindrà un apartat que descrigui l'estructura dels fitxers, i també una descripció dels sistemes d'informació que els tracten.

- Descriurem l'estructura dels fitxers que contenen les dades de caràcter personal, les seves característiques i finalitat.

- Descriurem els programaris informàtics utilitzats per al tractament de les dades.

f) Incidències. Hem de preveure un procediment de notificació, gestió i resposta enfront de les incidències. Voldrà dir tenir un **registre d'incidències** en què anotarem (com a mínim), el següent:

- Les incidències que es produeixin que afectin la seguretat de les dades.

- El moment en què s'han produït.

- La persona que ha notificat la incidència i la persona a qui es comunica la incidència.

- El procediment seguit, i també les mesures adoptades com a conseqüència de la incidència produïda.

g) Còpies de seguretat. Hi ha de ser descrit i previst el procediment de còpies de seguretat i recuperació de les dades.

- Descriurem el procediment per dur a terme les còpies de seguretat i el procediment per a la recuperació de les dades, i indicarem els mitjans tècnics (dispositius, cintes, etc.) i programaris que utilitzarem per fer aquestes tasques.

- Aquests procediments hauran de garantir la reconstrucció de les dades en l'estat en el qual es trobaven en el moment de la pèrdua o destrucció.

- Indicarem la periodicitat amb què es duran a terme les còpies de seguretat, que haurà de ser com a mínim d'una còpia per setmana.

h) Gestió de suports. Els suports informàtics que continguin dades de caràcter personal han de complir els requisits següents:

- Ser etiquetats de manera que permetin conèixer la informació que contenen.

- Ser inventariats.

- Ser emmagatzemats en un lloc al qual només tingui accés el personal autoritzat (ha de constar en el document de seguretat).

i) Identificació i autenticació. Per a una **identificació** i **autenticació** correctes dels usuaris haurem de preveure el següent:

- El responsable del fitxer mantindrà una llista actualitzada d'usuaris amb dret d'accés al sistema d'informació que contingui les dades personals.

- Establirà un sistema d'identificació (reconeixement de la identitat) i autenticació (comprovació de la identitat) d'aquests usuaris.

- Quan l'autenticació dels usuaris es basi en l'existència de contrasenyes, aquestes hauran de complir els requisits següents:

  – Establirem un sistema d'assignació, distribució i emmagatzemament de les contrasenyes que en garanteixi la integritat i confidencialitat.
  – Les contrasenyes s'emmagatzemaran de manera inintel·ligible.
  – Les contrasenyes es canviaran amb la periodicitat que assenyalem en el document de seguretat.

Vegeu el subapartat "Mecanismes d'autenticació d'usuaris" per saber quins sistemes d'identificació hi ha i com se'n pot gestionar la seguretat.

4) La qualitat de les dades. La Llei estableix en l'article 4 uns principis generals de qualitat que tendeixen a garantir un ús adequat de les dades, i fixa que les dades de caràcter personal:

Reviseu el subapartat "Principis bàsics de la LOPDP". La qualitat de les dades és un dels eixos fonamentals d'aquesta llei. Consegüentment, ha de formar part del tractament inicial.

- S'han d'adequar a la finalitat per a la qual van ser demanades.
- Han de ser exactes i actualitzades.
- No s'han de mantenir indefinidament sense justificació.
- Han d'haver estat recollides d'una manera lícita.

Per complir aquest apartat s'hauria de dissenyar un procediment de recollida de dades que s'adeqüi al que necessitem.

5) El dret d'informació en la recollida de les dades. La LOPDP estableix una **obligació prèvia** d'informar la persona afectada a l'hora de demanar-ne les dades personals d'una sèrie d'extrems, perquè pugui subministrar o no les dades amb el ple coneixement de l'abast del tractament que se'n farà.

S'ha d'informar la persona interessada d'una manera prèvia, expressa, precisa i inequívoca:

- De l'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.

- Del caràcter obligatori o facultatiu de la seva resposta a les preguntes que li siguin plantejades.

- De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.

- De la identitat i adreça del responsable del tractament o, si escau, del seu representant.

- De la possibilitat d'exercir els **drets d'accés, rectificació, cancel·lació i oposició** (drets ARCO, articles 15,16 i 17 de la LOPDP).

Aquests drets reflecteixen:

- **Accés***:* el ciutadà pot sol·licitar informació sobre les seves dades emmagatzemades al responsable del fitxer i obtenir la informació següent:

  – Informació sobre si les seves dades són objecte de tractament.
  – Finalitat del tractament que s'estigui duent a terme.
  – Informació sobre l'origen de les dades i les cessions fetes o previstes.

- **Rectificació***:* si les dades del ciutadà són inexactes, incompletes, inadequades o excessives, en pot exigir la modificació per reflectir la seva situació real.

- **Cancel·lació***:* el ciutadà pot exigir al responsable del fitxer la supressió d'algunes dades que poguessin ser inadequades o excessives.

- **Oposició:** és el dret del ciutadà a negar-se a que les seves dades personals siguin objecte de tractament en els casos en què:

  – No sigui necessari demanar consentiment i hi hagi motius legítims i fonamentats referits a una situació personal concreta, sempre que la Llei no disposi el contrari.
  – Que els fitxers tinguin per finalitat la realització d'activitats de publicitat i prospecció comercial.
  – Quan el tractament tingui per finalitat una decisió referida a la persona afectada i basada exclusivament en un tractament automatitzat de les seves dades personals.

Dret de cancel·lació

L'exercici del dret de cancel·lació molt possiblement provocarà un bloqueig de les dades. Són conservades únicament per administracions públiques, jutges i tribunals fins a la prescripció de la durada del fitxer. Després són eliminades.

6) Consentiment de la persona afectada. El **principi del consentiment** (article 6) és l'eix fonamental de la protecció de dades. El consentiment no és altra cosa que la manifestació de voluntat, lliure, inequívoca, específica i informada, mitjançant la qual la persona interessada consent el tractament de les seves dades personals.

7) El deure de secret. S'estableix un **deure de secret i de custòdia** a què es veuen subjectes les persones que participen en el procés de tractament de les dades de caràcter personal, deures que subsisteixen una vegada finalitzat el tractament de les dades.

Article 10. Deure de secret

El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardarles, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si escau, amb el seu responsable.

8) Drets ARCO. S'ha de **facilitar** als ciutadans l'exercici dels drets ARCO (l'existència dels quals ja ha estat prèviament informada).

Per complir aquest apartat caldrà crear els formularis corresponents, i també les clàusules necessàries per a informació de l'usuari.

2.3.2. Manteniment

Una vegada tenim els fitxers identificats i declarats a l'Agència de Protecció de Dades, seguidament cal adoptar un conjunt de mesures tècniques, normes i procediments que garanteixin el nivell de seguretat que ens exigeix la LOPDP.

El **nivell bàsic** conté les còpies de seguretat, el control d'accés i la gestió de suports. Aquests elements, per tant, seran presents en la resta dels nivells. Vegeu tot seguit com es poden dur a terme, ja que a més d'haver d'estar en el document de seguretat, són necessaris per al manteniment de la informació i la seva seguretat.

1) Còpies de seguretat i recuperació de dades. Per a la realització de les còpies de seguretat i recuperació de dades, s'ha de tenir en compte que:

- El **responsable del fitxer** (RF) s'encarrega de verificar, amb la col·laboració del **responsable de seguretat** (RS), l'aplicació correcta dels procediments utilitzats per a la realització de les còpies de seguretat i recuperació de dades.

- Els procediments de realització de còpies de seguretat o recuperació de dades han de garantir, en la mesura del que sigui possible, la reconstrucció de les dades en l'estat en el qual es trobaven en el moment de produir-se una pèrdua.

- Quan un procés de recuperació de dades afecti fitxers de nivell intermedi, serà necessària l'autorització de l'RF per a l'execució del procediment de recuperació.

- Les còpies de seguretat s'han de fer sobre suport extraïble i amb periodicitat setmanal (com a mínim). Aquest termini únicament podria ser ampliat en cas que en aquest període no s'hagi produït cap actualització o modificació de les dades.

- S'han de fer còpies de seguretat addicionals prèviament a la realització de qualsevol intervenció tècnica en els recursos informàtics (instal·lació o actualització d'aplicacions, instal·lació o substitució de maquinari, reparacions...).

- Verificació, prèvia a l'emmagatzemament de la còpia de seguretat, de la realització correcta, sense existència d'incidències o errors.

- Tot programari o aplicació utilitzada per al tractament de dades personals haurà de tenir la funció de realització de còpies de seguretat, o bé permetre la realització de còpies de seguretat de manera que es garanteixi la recuperació de dades.

- Tot procediment de recuperació de dades haurà de ser fet pel personal amb els coneixements tècnics necessaris. En cas que aquest procediment sigui fet per personal extern, l'RS ha de verificar que durant l'execució es mantingui la confidencialitat més estricta sobre les dades de caràcter personal dels fitxers.

2) Identificació, autenticació i control d'accessos

Com a norma general, que és senzilla de recordar, l'accés serà individualitzat i tot quedarà registrat. La implementació d'aquesta regla passa per crear un protocol per al control d'accessos, per a l'assignació de contrasenyes i l'emmagatzematge corresponent, i també per al registre d'ús dels fitxers i la gestió dels seus suports.

a) Control d' accessos

- Els sistemes informàtics que donen accés a fitxers que contenen dades de caràcter personal han de tenir sempre aquest accés restringit mitjançant un codi d'usuari i una contrasenya. Sense la introducció de la contrasenya no ha de ser possible accedir a les dades protegides.

- Només en els casos en què exclusivament un usuari accedeixi al sistema informàtic o als fitxers de dades es pot prescindir del codi d'usuari.

- Tots els usuaris autoritzats per a l'accés als fitxers han de disposar d'un codi d'usuari particular associat a una contrasenya que només ha de conèixer l'usuari.

- El codi d'usuari i la contrasenya han de ser absolutament personals i intransferibles; per això, els registres que s'efectuïn sobre operacions fetes sota un codi i contrasenya s'han d'atribuir, llevat de prova en contra, al seu titular i queden sota la seva responsabilitat personal.

- En els casos en els quals els fitxers continguin dades de nivell intermedi o alt, s'ha de limitar la possibilitat d'intentar reiteradament l'accés no autoritzat a un màxim d'intents fallits.

b) Assignació i canvi de codis d'usuari i contrasenyes

- Quan un usuari sigui donat d'alta, l'RS ha de confirmar amb l'RF el seu nivell d'accés als fitxers que continguin dades de caràcter personal.

Aquest nivell d'accés ha de ser l'estrictament necessari perquè l'usuari pugui desenvolupar les seves funcions i només podrà ser modificat prèvia consulta amb l'RF.

- L'RS ha d'assignar a l'usuari el codi d'usuari corresponent i una contrasenya, la qual haurà de ser modificada per l'usuari (si ho vol) en un termini màxim no superior a 24 hores, de manera que passarà a ser del seu coneixement exclusiu.

- Cada usuari és responsable de la confidencialitat de la seva contrasenya. Si adverteix o sospita que ha pogut ser coneguda fortuïtament o fraudulentament per persones no autoritzades, haurà de registrar-ho com a incidència i notificar-ho a l'RS, el qual haurà d'assignar una nova contrasenya a l'usuari.

- Quan un usuari sigui donat de baixa, l'RS haurà d'esborrar el seu identificador d'usuari sense que sota cap concepte pugui ser assignat a un altre usuari.

- Les contrasenyes han de tenir una longitud mínima de sis caràcters i no haurien de ser llegibles quan s'estiguin teclejant.

- El sistema haurà de sol·licitar la modificació de contrasenyes d'usuaris cada 45 o 60 dies màxims.

c) Emmagatzemament de contrasenyes

- L'arxiu en el qual quedin emmagatzemades les contrasenyes serà d'accés exclusiu per l'RF o l'RS amb l'autorització expressa d'aquest.

- L'arxiu haurà d'estar protegit i les contrasenyes s'emmagatzemaran de forma inintel·ligible.

d) Registre d'accessos (fitxers de nivell alt)

- En els casos en els quals els fitxers continguin dades de nivell alt i sigui necessari l'accés per més d'un usuari, es guarda un registre de cada accés en el qual consti la identificació de l'usuari, la data i l'hora d'accés, el fitxer accedit, el tipus d'accés i si va ser autoritzat o denegat. Si l'accés s'autoritza, es desa a més la informació que permeti identificar el registre accedit.

- L'RS ha de controlar directament els mecanismes establerts per al registre d'accessos, els quals no poden ser desactivats en cap cas.

- L'RS ha de revisar periòdicament la informació registrada.

- Les dades registrades s'han de conservar, com a mínim, durant dos anys.

3) Gestió de suports

En l'article 5 de LOPDP es defineix *suport* com un "[...] objecte susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar i recuperar dades".

Així doncs, és imprescindible una bona gestió dels suports, físics o informàtics, per poder dur a terme un tractament acurat de la informació.

- Els suports han d'estar clarament identificats amb una etiqueta externa, que indiqui el tipus d'informació que contenen, i també la data de creació.
- Els suports s'han d'emmagatzemar amb pany i clau, i se n'ha de restringir la utilització únicament a les persones amb accés autoritzat als fitxers.
- La sortida de suports fora dels locals (instal·lacions) on es trobin ubicats els fitxers l'haurà d'autoritzar, mitjançant la firma, l'RF i l'RS.
- S'ha de fer un inventari de suports que ha de contenir la informació relativa a cada suport inventariat: tipus de suport, data de creació, informació que conté i lloc on és emmagatzemat.

a) Per als fitxers de nivell intermedi

- En el cas de suports que s'hagin de llençar, s'ha de procedir a destruir-los o inutilitzar-los físicament, abans de la baixa en l'inventari, per impedir qualsevol recuperació posterior de la informació que contenen.
- Els suports que siguin reutilitzables s'hauran d'esborrar abans de reutilitzar-los, de manera que les dades que contenien no siguin recuperables.
- Si fos necessari que els suports surtin fora dels locals on són ubicats els fitxers com a conseqüència d'operacions de manteniment, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada.
- S'ha d'establir un sistema de registre d'entrada i de sortida de suports informàtics.
- La recepció de suports sempre ha de ser autoritzada per l'RS.
- L'RF ha d'arxivar els registres d'entrades i de sortides de suports.

2.4. Dades personals

El concepte de *dada de caràcter personal* de fet genera força confusions. Per determinar què és realment, ens hem de fixar en la LOPDP, en la qual es defineix com tota informació numèrica, alfabètica, gràfica, fotogràfica, acús-

tica o de qualsevol altre tipus susceptible de recollida, registre, tractament o transmissió, referida a una persona física identificada o identificable.

Així, doncs, quan parlem de *dada personal* ens referim a qualsevol informació relativa a una persona concreta. Les dades personals ens identifiquen com a individus i caracteritzen les nostres activitats en la societat, tant públiques com privades. El fet que diguem que les dades són de caràcter personal no vol dir que només tenen protecció les vinculades a la vida privada o íntima de la persona, sinó que les dades protegides són totes les que ens identifiquen o que en combinar-les permeten la nostra identificació.

Només les dades de persones físiques, i no les dades de persones jurídiques, com empreses, societats, etc., són dades de caràcter personal.

Tenen la consideració de dades personals:

- Nom i cognoms, data de naixement.
- Número de telèfon, adreça postal i electrònica.
- Dades biomètriques (empremtes, iris, dades genètiques, imatge, raça, veu, etc.).
- Dades sanitàries (malalties, avortaments, cirurgia estètica, etc.).
- Orientació sexual.
- Ideologia, creences religioses, afiliació sindical, estat civil...
- Dades econòmiques: bancàries, solvència, compres.
- Consums (aigua, gas, electricitat, telèfon...), subscripcions premsa, etc.
- Dades judicials (antecedents penals).

Dades personals

Dades com el correu electrònic o dades biomètriques també són dades personals, ja que permeten identificar la persona.

Fins i tot l'Agència de Protecció de Dades ha considerat la IP (Informe 327/2003) com una dada personal.

2.4.1. Dades personals sensibles

No totes les dades personals són igual d'importants. Algunes s'anomenen **sensibles** a causa de la seva transcendència per a la nostra intimitat, o a la necessitat d'evitar que siguin usades per discriminar-nos. No es tracta de preservar la nostra intimitat sinó d'evitar prejudicis per l'ús que es pugui fer d'aquestes dades.

Tenen la consideració de **dades sensibles** les que es refereixen a la nostra raça, a les preferències polítiques, a les conviccions religioses, a les afiliacions a partits polítics o a sindicats, a la nostra salut o orientació sexual, etc.

Les dades sensibles reben una protecció més intensa que la resta. Estan definides a l'article 7 de la LOPDP.

2.4.2. Drets dels titulars de les dades personals

La LOPDP dóna als usuaris un conjunt de drets que els permeten un control sobre les dades personals (en especial, si la persona detecta que estan fent un ús incorrecte de les seves dades). Els drets que la normativa dóna als usuaris són:

- **Drets ARCO**.
- **Dret de consulta**: qualsevol persona té el dret d'anar al **Registre General de Protecció de Dades** (registre públic i gratuït integrat en l'estructura

de l'Agència Espanyola de Protecció de Dades) per obtenir informació sobre els fitxers inscrits. Concretament, sobre els tractaments de dades de caràcter personal existents, les seves finalitats i la identitat del responsable del tractament.

- **Dret d'indemnització**: el ciutadà que, a causa d'un tractament il·legal de les seves dades, pateixi danys en els seus béns o drets té dret a ser indemnitzat per la persona, empresa o entitat (pública o privada) responsable d'aquests danys.

La persona interessada és assistida per altres drets; així, a més a més dels drets explicats, hi ha els drets d'informació i d'impugnació.

2.5. Infraccions i sancions

L'incompliment d'una normativa legal pot comportar sancions. En el cas de la LOPDP, el règim de responsabilitat previst és de caràcter **administratiu** (menys greu que el penal i que no pot representar sancions privatives de llibertat). El títol VII d'aquesta Llei estableix quines són les infraccions (lleus, greus i molt greus) que es poden cometre durant el tractament de les dades de caràcter personal, i també les sancions que es poden aplicar en cada cas. L'import de les sancions varia segons els drets personals afectats, volum de dades efectuats, beneficis obtinguts, grau d'intencionalitat i qualsevol circumstància que l'Agència estimi oportuna (vegeu la taula 4).

Taula 4. Infraccions i sancions de la LOPDP

Tipus d'infraccions	Característiques	Sancions
Infracció lleu	• No atendre per motius formals sol·licituds de rectificació o cancel·lació. • No proporcionar informació requerida per l'APD. • No inscriure fitxers en el Registre General de Protecció de Dades. • No complir el deure d'informació. • Vulnerar el deure de secret.	**De 600 a 60.000 €**
Infracció greu	• No demanar el consentiment dels titulars. • Mantenir dades inexactes. • No aplicar les mesures de seguretat corresponents. • Obstruir la tasca inspectora.	**De 60.000 a 300.000 €**
Infracció molt greu	• Recollir dades d'una manera enganyosa. • Comunicar dades sense requisits legals. • Tractar dades de nivell alt sense consentiment exprés / exprés i escrit.	**De 300.000 a 600.000 €**

Exemples d'infraccions de la LOPDP

Vegem alguns exemples d'infraccions de la Llei de protecció de dades:

- Ha estat objecte de sanció la inclusió no consentida de persones a llistes com a voluntaris en les eleccions del País Basc.

- Alguns webs que ofereixen la possibilitat d'enviar a un amic certa informació o de recomanar aquest web a un amic també han estat sancionats.

- Així mateix, diverses empreses d'assegurances i centres de salut que intercanviaven informació mèdica dels pacients sense el seu consentiment també han estat objecte de sanció.

- Tot i així, encara hi ha buits no resolts, com l'anomenat ***spam* telefònic**, és a dir, la realització de trucades comercials no consentides als domicilis dels particulars.

2.6. Legislació sobre els serveis de la societat de la informació, comerç, correu electrònic i signatura electrònica

Com a conseqüència de l'expansió enorme de les xarxes d'ordinadors i molt especialment d'Internet, fenòmens que abans eren habituals dins del món analògic o real, han acabat traspassant les fronteres per esdevenir freqüents en el món virtual (per exemple, el comerç electrònic). No podem esperar que el marc jurídic doni resposta als nous reptes provocats per l'ús de les tecnologies de la informació. Si bé els conceptes són antics, el seu trasllat al món virtual crea la necessitat d'expandir el marc jurídic (o fins i tot redefinir-lo dins de l'àmbit tecnològic) per donar resposta als buits legals que s'originen com a conseqüència de l'aplicació de la tecnologia. Aquesta regulació no solament ha d'evitar el mal ús de la tecnologia (per exemple, l'enviament de correu brossa [*spam*] o correu no consentit), sinó que ha de generar un entorn de confiança en el qual es delimitin clarament les responsabilitats i els deures de cadascú, sense el qual no seria possible l'establiment de transaccions, com ara el comerç electrònic.

El comerç electrònic o *e-commerce*...

... consisteix en la compra i venda de productes o serveis mitjançant xarxes d'ordinadors (com, per exemple, Internet).

Així, doncs, l'objectiu de la **Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i del comerç electrònic** (LSSICE, d'ara endavant) és la incorporació de la directiva comunitària sobre el comerç electrònic al marc jurídic espanyol. Aquesta normativa s'ha desenvolupat en diversos àmbits: europeu, estatal i autonòmic.

Podeu trobar la versió consolidada no oficial de la LSSICE (de data 31/12/07) en la secció "Adreces d'interès" del web.

2.6.1. Concepte de serveis de la societat d'informació

Segons el text de la mateixa LSSICE, el concepte de **servei de la societat d'informació** és realment divers i comprèn els àmbits següents:

- Contractació de béns i serveis per via electrònica.
- Subministrament d'informació per via electrònica (per exemple, els diaris digitals).
- Les activitats d'intermediació relatives al següent:
  - Provisió d'accés a la xarxa.
  - Transmissió de dades.
  - Realització de la còpia temporal de les pàgines d'Internet sol·licitades pels usuaris.
  - Allotjament de dades en els servidors d'informació.
  - Serveis o aplicacions facilitats per altres.
  - Provisió d'instruments de recerca.
  - Enllaços a altres llocs d'Internet.

- Qualsevol altre servei que es presti a petició individual dels usuaris (descàrrega d'arxius de vídeo o àudio...), **sempre que representi una activitat econòmica per al prestador**.

Els serveis de la societat d'informació són oferts pels operadors de telecomunicacions, els **proveïdors d'accés a Internet**, els portals, els motors de recerca o qualsevol altre subjecte que disposi d'un lloc a Internet per mitjà del qual digui a terme alguna de les activitats indicades, inclòs el comerç electrònic.

Proveïdors de serveis

Els operadors que ens proporcionen l'accés a Internet a les nostres llars són exemples del que la LSSICE entén per *proveïdors de serveis*.

2.6.2. Obligacions i responsabilitat dels prestadors de serveis

No solament per desenvolupar el ja esmentat marc de confiança, sinó també per poder perseguir les activitats il·lícites que es puguin desenvolupar a la Xarxa, la LSSICE determina quines són les **obligacions i responsabilitats dels prestadors de serveis**. No oblideu, però, que la LSSICE se situa dins del **marc jurídic extrapenal**. Així, doncs, les sancions que preveu aquesta llei no poden comportar penes privatives de llibertat. Per exemple, l'enviament de correu brossa o correu no consentit és una activitat sancionada per la LSSICE, però, en canvi, en si mateixa, no apareix reflectida en el Codi penal.

El correu brossa se sol confondre amb un delicte informàtic, tot i que no ho és.

Obligacions dels prestadors de serveis

Malgrat tot, les obligacions que tenen els prestadors de serveis, descrites en la LSSICE, possibiliten la persecució dels delictes relacionats amb la xarxa Internet.

La llei imposa el **deure de col·laboració dels prestadors de serveis d'intermediació** per impedir que determinats serveis o continguts il·lícits es continuïn divulgant, i també el **deure de retenció de dades de trànsit relatives a les comunicacions electròniques, durant un període màxim de dotze mesos.**

Són activitats d'intermediació la transmissió, la còpia, l'allotjament i la localització de dades a la Xarxa.

Així, doncs, i sempre mitjançant una resolució judicial motivada, els prestadors de serveis hauran de col·laborar amb els jutges, i hauran de posar a la seva disposició les dades que els siguin requerides. Per exemple, si una investigació criminal descobreix un lloc d'Internet que allotja pornografia infantil o programaris **pirates**, els proveïdors de serveis hauran de lliurar al jutge encarregat de la investigació els fitxers de registre que enregistrin l'activitat de l'usuari que ha allotjat el contingut il·lícit en el lloc investigat.

Un aspecte molt important que cal tenir en compte és que, segons la llei, els fitxers de registre només s'emmagatzemaran com a molt durant dotze mesos. Atès que no hi ha una durada mínima del temps de preservació dels registres, els proveïdors els podrien emmagatzemar durant poc temps (per exemple, només uns dies o unes hores), amb la qual cosa és necessari, davant el coneixement d'un delicte relacionat amb la Xarxa, actuar amb molta prestesa per no perdre la informació valuosa dels registres.

Un altre aspecte destacable amb relació a la preservació dels registres és la consideració de la IP com una dada personal (tot i que no identifica directament una persona, sí esdevé un mitjà per identificar-la). Això implica que els responsables de les pàgines web que emmagatzemin les IP dels usuaris que les consulten hauran d'inscriure el fitxer a l'Agència Espanyola de Protecció de Dades.

Com podíem esperar, les dades que enregistra el proveïdor de serveis s'hauran d'emmagatzemar garantint els drets constitucionals i amb les mesures determinades per la Llei de protecció de dades. Només poden retenir les dades imprescindibles per identificar l'**origen de la connexió** des de la qual s'ha efectuat l'acció il·lícita i el **moment en què s'inicià la prestació del servei.** En cap cas la preservació de les dades no pot atemptar contra el secret de les comunicacions.

Règim de responsabilitats dels prestadors de serveis

Els prestadors de serveis de la societat de la informació estan subjectes a la **responsabilitat civil, penal i administrativa**. Per determinar el tipus de responsabilitat que recau sobre ells caldrà diferenciar les situacions següents:

Vegeu els diferents tipus de responsabilitat en la secció "Annexos" del web.

a) El prestador és l'autor (creador) directe de la informació, o bé desenvolupa tasques de control sobre els continguts que es transmeten a la Xarxa. Per exemple, el gestor d'una llista de distribució de correu electrònic (*mailing list*) o el moderador d'un fòrum de discusió. En tots dos casos, el prestador pot tenir coneixement de la informació que s'introdueix a la Xarxa i en pot exercir el control. Per tant, la seva responsabilitat és inqüestionable.

Una *llista de correu*...

... és un conjunt de noms i adreces de correu electrònic, emprades per un usuari o organització per enviar informació a múltiples destinataris.

Una *fòrum de discussió*...

... és una aplicació web que permet que diferents usuaris expressin les seves opinions en línia, normalment entorn d'una qüestió proposada per un moderador.

b) Quan no hi ha la participació activa del prestador amb relació als continguts il·lícits allotjats, la determinació de la responsabilitat ja no és tan evident i consta de les exempcions següents:

- Si el servei consisteix en la mera **transmissió de les dades** proveïdes pel destinatari del servei, o en proporcionar l'**accés a la Xarxa**, s'entén que els proveïdors desconeixen els continguts transmesos i no seran res-

ponsables de la informació que s'hagi pogut transmetre, sempre que no es produeixin les situacions següents:

– Que els prestadors no hagin originat la transmissió.
– Que no hagin modificat ni seleccionat les dades.
– Que no hagin seleccionat el destinatari.

- Els prestadors solen emmagatzemar en els servidors còpies automàtiques i temporals de les dades facilitades pel destinatari del servei (*caching*). També en aquest cas, els proveïdors no són responsables del contingut d'aquestes dades, sempre que no hagin modificat la informació.

Caching

El *caching* és una tècnica emprada pels anomenats **servidors intermediaris**, els quals (entre altres activitats) emmagatzemen la resposta a la sol·licitud d'un usuari (una pàgina web) per poder-la oferir directament quan un altre usuari la sol·liciti, sense necessitat de contactar novament amb la pàgina demanada.

- En el cas dels proveïdors de serveis que allotgen o emmagatzemen dades, aplicacions o serveis (hostatge), no hi haurà responsabilitat en els casos següents:

  – Quan els prestadors no tinguin **coneixement efectiu** que l'activitat o la informació és il·lícita o que pot lesionar béns o drets d'un tercer susceptible d'indemnització.

  – En cas que en tinguin coneixement, no tenen cap responsabilitat si retiren amb prestesa les dades o hi impossibiliten l'accés.

Coneixement efectiu

Els prestadors de serveis tenen el *coneixement efectiu* quan:

- L'autoritat competent hagi declarat que les dades són il·lícites, n'hagi ordenat la retirada o demanat que s'impossibiliti l'accés.
- Quan s'hagi declarat l'existència d'una lesió i el prestador conegui la resolució corresponent.

Cal dir que, en aquest sentit, molts proveïdors ofereixen als usuaris la possibilitat de valorar els continguts i marcar-los en cas que el contingut no sigui lícit o lesioni els drets d'una persona. En aquests casos, els proveïdors supervisen els continguts marcats i determinen si cal o no cal eliminar-los. No obstant això, la Llei no exigeix als prestadors l'obligació de supervisió, ni la realització de recerques de continguts il·lícits.

És el cas del portal YouTube. Els mateixos usuaris poden determinar i marcar els continguts que no són idonis.

- Finalment, quan el prestador faciliti enllaços (*links*) amb continguts, o bé inclogui instruments de recerca, no és responsable de la informació redirigida pels enllaços, sempre que es produeixin els requisits d'exempció, ja esmentats en l'apartat d'allotjament:

  – Quan els prestadors no tinguin **coneixement efectiu** que l'activitat o la informació és il·lícita o que pot lesionar béns o drets d'un tercer susceptible d'indemnització.

– En cas que en tinguin coneixement, no tenen cap responsabilitat si retiren amb prestesa les dades o hi impossibiliten l'accés.

Obligacions de les empreses que fan comerç electrònic

Com a possibles usuaris del comerç electrònic, convé que sapigueu les obligacions d'informació que tenen totes les empreses que es dediquen a aquest tipus d'activitats. El portal web hauria de mostrar, entre d'altres, la informació següent:

- La denominació social, NIF, domicili i adreça de correu electrònic o fax.
- Els codis de conducta als quals s'adhereixin.
- Preus dels productes o serveis que ofereixen, amb indicació dels impostos i despeses d'enviament.
- Si escau, les dades relatives a l'autorització administrativa necessària per a l'exercici de l'activitat, dades de col·legiació i títol acadèmic dels professionals que exerceixin l'activitat.

En cas que l'empresa faci contractes en línia també caldrà que ofereixi la informació següent, amb caràcter previ a la contractació del servei:

- Tràmits que cal seguir per fer la contractació en línia.
- Si el document electrònic del contracte s'arxivarà i si serà accessible.
- Mitjans tècnics per identificar i corregir errors durant el procés d'introducció de dades.
- Idioma o idiomes en els quals es pot formalitzar el contracte.
- Condicions generals del contracte.

A més, l'usuari ha de rebre un acusament de rebut de la comanda feta.

Amb relació als usuaris d'Internet, els titulars de pàgines personals que no percebin cap ingrés econòmic pel seu web no estan subjectes a la Llei. No obstant això, si guanyen diners (per exemple, gràcies a la inclusió de bàners publicitaris en la seva pàgina), hauran de mostrar informació bàsica (nom, residència, adreça de correu electrònic, telèfon o fax i NIF) i respectar les normes de publicitat incloses en la Llei:

- L'anunciant s'ha d'identificar clarament.
- El caràcter publicitari de la informació ha de resultar inequívoc.

2.6.3. Regulació de comunicacions publicitàries (*spam*)

El correu brossa consisteix en l'enviament no consentit (pels receptors) de missatges de correu electrònic a una multitud de destinataris, amb finalitat merament comercial.

Si bé aquesta conducta s'associa freqüentment a l'esfera del mal anomenat *delicte informàtic*, tot i que és susceptible de ser sancionada, no apareix recollida en el Codi penal.

Això no obstant, dins de l'àmbit extrapenal, aquestes accions apareixen recollides de la manera següent:

- La LOPDP determina el consentiment de la persona interessada en el cas del tractament de dades amb finalitats de publicitat i de prospecció comercial.

- La LSSICE també prohibeix l'enviament de comunicacions publicitàries per correu electrònic (o mitjans electrònics equivalents), si no han estat prèviament autoritzats de manera expressa pels destinataris.

L'incompliment d'aquesta prohibició pot constituir una **infracció greu**, que es pot castigar amb una **multa de 30.001 fins 150.000 euros**, o bé una **infracció lleu**, punible amb **una multa de fins 30.000 euros**, segons els casos. En cap cas, però, pot generar responsabilitat penal perquè no és cap conducta constitutiva de delicte.

En general, pel que fa a la publicitat, cal que recordeu que qualsevol usuari té dret a conèixer la identitat de l'anunciant, a no rebre publicitat no sol·licitada i deixar de rebre la que ha autoritzat (però que vol deixar de rebre).

De manera similar a la LOPDP, les infraccions de la LSSICE també poden ser lleus, greus i molt greus.

2.6.4. Legislació sobre signatura electrònica

Tots els serveis de la societat de la informació, i molt especialment tots els relacionats amb el comerç electrònic, es basen en l'establiment de relacions de confiança en un entorn gairebé anònim i intangible per definició. Per aquest motiu, sorgeix la necessitat d'incorporar mesures que permetin conferir seguretat a les comunicacions per Internet. Aquesta és, doncs, la motivació essencial de la **signatura electrònica**.

La signatura manuscrita (o hològrafa)...

... autentica la identitat de la persona que signa i certifica el consentiment de la informació continguda en un document.

Tot i que sovint es parla indistintament de **signatura digital** i **signatura electrònica**, ambdós termes no són exactament sinònims. Mentre que el primer es refereix a mètodes criptogràfics (i, per tant, és una definició tècnica), el segon és de natura legal i té un abast més ampli que no pas la signatura digital. La definició de *signatura electrònica* no inclou la tècnica subjacent que cal emprar per desenvolupar-la. Per exemple, la signatura electrònica es podria haver desenvolupat a partir de l'aplicació d'altres

Per tal de comprendre millor els conceptes de *criptografia* i *signatura digital*, vegeu el subapartat "Protecció de dades" d'aquesta mateixa unitat formativa.

mètodes diferents dels basats en la criptografia. No obstant això, a efectes pràctics, podeu considerar anàlegs els dos conceptes.

La **signatura digital**, basada en la criptografia de clau pública, permet que un emissor pugui enviar missatges a un receptor de manera que se satisfacin les tres propietats següents:

- **Autenticitat**: la signatura d'un missatge per l'emissor permet que el receptor estigui segur de la identitat del remitent.

- **Integritat**: aquesta propietat al·ludeix a la impossibilitat que el missatge no s'hagi pogut modificar durant la transmissió.

- **No-repudiació**: l'emissor d'un missatge no pot repudiar o negar que l'ha enviat (per exemple, podria argumentar que l'ha enviat una tercera persona). La inclusió d'una signatura digital al missatge evita aquesta possibilitat.

Aquestes tres propietats són essencials perquè, efectivament, la signatura digital gaudeixi de prou confiança en un entorn tan intangible com Internet. Si volem fer qüestions tan delicades, com, per exemple, signar un contracte via Internet o participar en unes votacions electròniques, és imprescindible que les tres propietats abans esmentades es puguin garantir. Observem que moltes vegades l'entorn en què se signa de manera **manuscrita** un document ofereix, en realitat, menys garanties que la robustesa proporcionada pels criptosistemes de clau pública.

Moltes vegades, les operacions que es puguin fer per la Xarxa són qüestionades perquè l'usuari no les acaba d'entendre o perquè impliquen la traducció al món virtual d'operacions perfectament tangibles del món real. Suposem, per exemple, la participació en unes votacions electròniques. En el món real, el votant introdueix físicament una papereta de vot dins de l'urna electoral. Pot veure com cau dins de l'urna i **confia** que l'urna només serà oberta, al final del procés, per les persones autoritzades i que el seu vot serà comptabilitzat correctament. Malgrat tot, aquest procés té tantes baules, punts febles i possibles errors humans, que, en el fons, podria ser tan qüestionat (o més fins i tot) com el seu homòleg electrònic.

Tots els criptosistemes de clau pública requereixen una **autoritat de certificació** que acrediti la identitat d'un usuari. En l'àmbit de la signatura digital, aquestes entitats reben el nom de **prestadors de serveis de certificació**. La seva tasca consisteix a expedir **certificats electrònics** que relacionen les eines de signatura digital, en poder de cada usuari, amb la seva identitat personal.

Podeu veure la necessitat de l'existència d'una tercera part o autoritat de certificació en el subapartat "Protecció de dades".

Una vegada vistos els elements tècnics de la signatura digital, definirem què entén la llei per **signatura electrònica**. Recordeu que aquest és un con-

cepte més ampli, de natura legal, que no especifica com s'ha de desenvolupar tècnicament la signatura.

La llei (Llei 59/2003, de 19 de desembre, de signatura electrònica) reconeix dos tipus de signatura electrònica: la **signatura electrònica avançada** i la **signatura electrònica reconeguda**.

La **signatura electrònica avançada** permet identificar la persona que signa i detectar qualsevol modificació que s'hagi pogut efectuar en les dades signades.

La **signatura electrònica reconeguda** és la signatura electrònica avançada, basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura (els prestadors de serveis de certificació). S'equipara a la signatura manuscrita.

El tractament de les dades personals que necessitin els prestadors de serveis de certificació s'ha d'efectuar d'acord amb la Llei orgànica de protecció de dades, els quals hauran de lliurar la identitat dels signants quan ho sol·licitin els òrgans judicials.

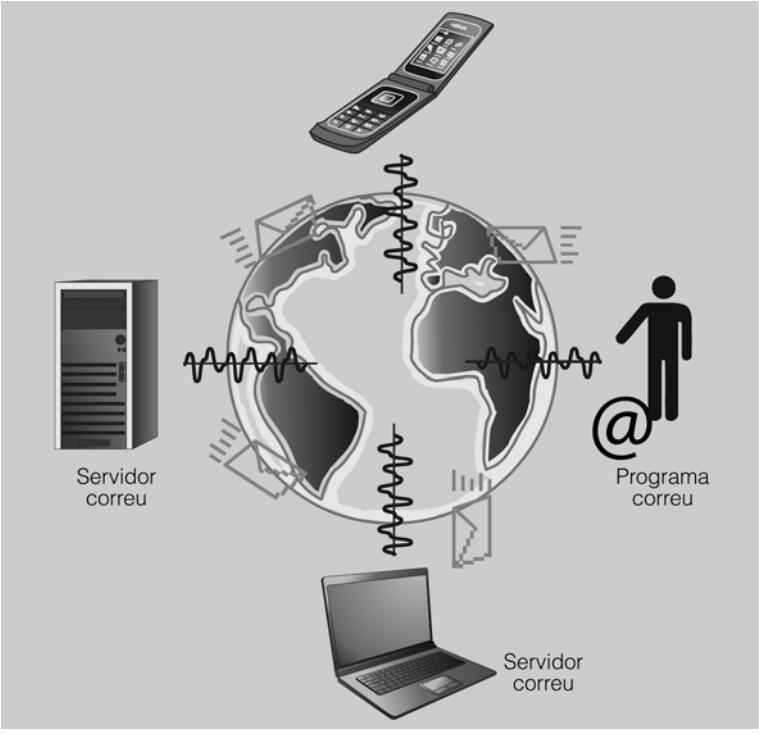
El DNI electrònic (DNIe)...

... permet acreditar, físicament i telemàticament, la identitat d'una persona, i també efectuar tot tipus de transaccions telemàtiques gràcies a les claus criptogràfiques que emmagatzema.

2.7. Configuració de programes client de correu electrònic per al compliment de normes sobre gestió de seguretat de la informació

El correu electrònic, perquè funcioni correctament, necessita els elements descrits en la figura 4.

Figura 4. Elements que intervenen en l'enviament del correu electrònic



!!

En la secció "Annexos" del web trobareu una explicació detallada de com es pot configurar un correu electrònic (Thunderbird) per enviar i rebre missatges usant criptografia de clau pública.

- **Adreça de correu**: per poder enviar un correu electrònic és necessari que tinguem nosaltres i la persona que ha de rebre el correu una adreça (ambdós hem de tenir adreça). L'adreça (que l'ha de subministrar un proveïdor de correu) es divideix en dues parts: el nom de l'usuari (a l'esquerra del símbol @), i que usualment correspon a la persona, i el domini en que està (a la dreta del símbol @).

- **Servidor de correu:** per poder enviar i rebre un correu electrònic en un servidor cal estar registrat (el servei pot ser gratuït o de pagament). El registre permet tenir una adreça de correu personal única i s'hi accedeix amb un nom d'usuari i una contrasenya.

Un proveïdor de correu és alguna entitat que té un servidor de correu i dóna servei, gratuït o de pagament, de correu.

- **Client de correu**: els clients de correu electrònic són programes per gestionar els missatges rebuts i per poder-ne escriure de nous. Habitualment, amb els paràmetres necessaris que subministra el proveïdor (tipus de connexió –POP o IMAP–, adreça del servidor de correu, nom d'usuari i contrasenya), el programa pot obtenir i descarregar el nostre correu. També pot enviar els nous missatges que enviem.

  Un programa de correu descarrega tots els nostres missatges del servidor al nostre ordinador i, després, sense necessitat d'estar connectats a Internet, els podem llegir, ja que estan enregistrats al nostre ordinador. Així mateix, també és possible usar el correu web, és a dir, accedir al servidor de correu mitjançant una interfície web per consultar i enviar correu. Alguns del programes de correu més coneguts són Mozilla Thunderbird, Outlook Express i Eudora.

- **Missatge:** un missatge de correu és un fitxer amb un format molt ben definit. Cal tenir present que llegir els correus d'altres persones és senzill, ja que aquests viatgen "despullats" (en clar) per la Xarxa. Un correu electrònic es pot assimilar a una targeta postal sense sobre, que pot ser llegit per qualsevol. Per tant, la millor manera de protegir-ne el contingut i preservar la intimitat és l'ús d'eines criptogràfiques.

L'estructura del missatge de correu és definida en l'RFC 822.

Així, doncs, podem trobar informació personal en els servidor de correu i ens els programes clients de correu. Per tant, l'ús dels sistemes de correu electrònic comporta algunes qüestions relatives a la protecció de dades personals, que s'han de tenir en compte.

En el servidor de correu cal mantenir la LOPDP i en els clients, la privadesa.

Molts aspectes de la nostra vida són regulats d'una manera o d'una altra per la legislació. El correu electrònic no n'és una excepció. La normativa aplicable és:

- **Constitució (art. 18)**: s'estableixen les garanties per a l'honor i la intimitat i es garanteix el secret de les comunicacions.

- **Codi penal (art. 197. 1)**: protegeix la intimitat de la persona. En aquest sentit, expressa que és un acte delictiu obtenir missatges de correu electrònic d'una altra persona sense el seu consentiment.

- **Estatut dels treballadors (art. 20.3)**: concedeix a l'empresari les mesures que estimi oportunes de vigilància i control per verificar que el treballador compleix les seves obligacions i els seus deures legals.

Mentre els treballadors no notifiquin ni acceptin els controls sobre el correu, ni tampoc els mecanismes sancionadors (en cas d'incompliment), el correu es pot considerar equiparat al correu paper, és a dir, **privat i no controlable**.

2.7.1. Servidors de correu i LOPDP

Els mecanismes d'intercanvi d'informació poden afectar les dades de caràcter personal. El correu electrònic és un dels mecanismes d'intercanvi d'informació més habituals. Quan pensem en dades de caràcter personal, tendim a pensar ràpidament en els servidors de bases de dades o en els servidors de fitxers. Però, què és el **servidor de correu electrònic** sinó una base de dades (tot i que no relacional, però un sistema d'emmagatzemament al cap i a la fi)? Per tant, també està subjecte a la LOPDP.

Aplicarem, consegüentment, tot el que hem vist amb relació als fitxers i a les seves mesures tècniques i organitzatives.

2.7.2. Correu electrònic i intimitat

En el cas dels programes de correu electrònic, és necessari algun mecanisme de transmissió dels correus que mantingui la intimitat de l'usuari. En aquest sentit, és una opció de l'usuari i, per tant, la configuració de l'aplicació (o les decisions de l'organització sobre la configuració), és la que determinarà el nivell de privadesa del programa.

És extremament important en un programa de correu electrònic evitar que puguin observar els nostres missatges (enviats i/o rebuts) i que puguin obtenir contrasenyes i/o fer-se passar per nosaltres per enviar correus en el nostre nom. (!!)

Algunes de les indicacions bàsiques per evitar aquest tipus de problemes són:

- **Utilitzeu sempre l'última versió del programari**: contínuament apareixen nous forats en els navegadors i en el programari associat (Java, Ja-

vaScript, ActiveX, CGI, en el programaris de correu, etc.). Utilitzarem, per tant, l'última versió disponible, que representa que és més segura que les anteriors.

- **Esborreu la informació compromesa**: cal que sigueu conscients de tota la informació residual que hi pot haver en el vostre disc dur (inclosa la paperera de reciclatge): correus antics, galetes (*cookies*), els llocs web visitats darrerament, els últims documents que heu obert, etc. En general, un ordinador és un llibre obert per a qualsevol persona malintencionada que el vulgui llegir.

Hi ha utilitats com Without a Trace o Zero Trace (programari gratuït) que esborren tota la informació residual del disc dur.

- **Useu diferents comptes de correu**: si voleu enviar correus confidencials des de la feina, utilitzeu un compte amb un proveïdor d'Internet (o millor feu-ho des de casa), però sense usar el vostre nom real. Podeu utilitzar serveis gratuïts (com, per exemple, HotMail).

- **Xifreu i signeu els correus confidencials**: si no voleu que qualsevol persona pugui llegir els vostres correus, però al mateix temps us interessa conservar la vostra identitat, xifreu els correus i signeu-los. Així, el destinatari estarà segur que ningú més no llegeix els missatges i que només vosaltres els envieu. Si només accepteu com a vàlids els correus signats no us exposeu que algú suplanti la personalitat (falsejament d'identitat o *spoofing*) d'un altre i us enganyi.

- **No reveleu dades personals innecessàriament**: sovint, en navegar per la Xarxa, us trobareu formularis que us demanen certes dades personals. Empleneu només els que penseu que són rellevants per al servei que s'ofereix. No és el mateix explicar que teniu un encaminador ADSL que dir l'import de la vostra factura del gas o quants membres viuen a casa vostra.

2.7.3. Correu segur

Tal com hem vist en l'apartat anterior, el correu és inherentment insegur. Ens interessa preparar el programa de correu per tal de tenir les màximes garanties de privadesa, tant en l'enviament com en la rebuda del programa de correu. És el que genèricament s'anomena **correu segur**. Aquest ha de complir les propietats següents (de manera similar a les propietats exigides en la signatura digital):

- **Xifratge**: volem que el nostre missatge viatgi per la Xarxa amb la garantia que no podrà ser vist per ningú més que el destinatari.

- **Integritat**: volem que el nostre missatge arribi intacte al destinatari i que, si hi ha hagut alguna manipulació, aquesta sigui detectada.

- **Identitat del remitent**: volem saber amb certesa qui ens envia el missatge.
- **No-repudiació**: volem que qui rep el missatge no pugui dir que no l'ha rebut, o bé que l'emissor no pugui dir que no ha estat ell qui l'ha enviat.

Aquestes propietats s'aconsegueixen instal·lant elements addicionals en el client de correu.

La millor manera de preservar la intimitat en els missatges de correu electrònic és amb l'ajuda de:

- La **signatura digital**, la qual permet que el destinatari del nostre correu comprovi que el missatge no ha estat modificat i que el que el llegeix és exactament el que nosaltres hem redactat.
- El **xifratge**, el qual permet ocultar el contingut del missatge perquè només el destinatari final el pugui llegir.

Cada usuari ha de disposar d'un parell de claus, la clau pública i la clau privada. La clau pública la donarem a tothom que vulguem que rebi correus nostres i permetrà que la gent verifiqui la nostra firma i creï missatges xifrats que vagin adreçats a nosaltres.

Com que els algoritmes de clau pública són molt ineficaços, el que es fa quan s'han de xifrar documents llargs (o els missatges de correu) és emprar funcions resum (*hash*), de manera que en lloc de signar un document se'n signa el resum.

Funció resum (*hash*)

És una funció matemàtica que fa correspondre una representació de mida fixa a un missatge *m* de mida variable. Aquesta representació té de 128 a 160 bits –els nous algorismes poden arribar als 256, 384 i 512 bits– i s'anomena *valor resum del missatge*. A efectes pràctics podem considerar que el resum és una mena d'empremta digital (o DNI) per a cada fitxer. És a dir, donat un fitxer qualsevol, és "difícil", en termes computacionals, trobar un altre fitxer amb el mateix valor resum.

És important tenir present...

... que la clau privada no la donarem a ningú, ja que ens permetrà signar el nostres correus i desxifrar els que vagin adreçats a nosaltres.

Els passos que cal seguir són els següents:

1) L'usuari A genera un resum del missatge que s'ha d'enviar.

2) L'usuari A xifra el resum amb la clau privada i signa, consegüentment, el missatge.

3) L'usuari A envia el missatge i el resum signat a l'usuari B, l'usuari receptor.

4) L'usuari B genera un resum del document rebut de l'usuari A, usant la mateixa funció resum (per exemple, els algorismes MD5 o SHA-1). Des-

més, desxifra amb la clau pública de l'usuari A el resum signat. Si el resum signat coincideix amb el resum que ha generat, la signatura és vàlida.

Així, s'ofereixen conjuntament els serveis de **no-repudiació**, ja que ningú excepte A no podria haver signat el document, i d'**autenticació**, ja que si el document és signat per A, podem estar-ne segurs de la identitat, ja que només ell l'ha pogut signar. Finalment, mitjançant la signatura digital es garanteix la **integritat** del document. En el cas de ser modificat, seria impossible fer-ho de manera que es generés la mateixa funció de resum amb què s'havia signat.