Seguretat física, lògica i legislació

Josep Maria Arqués Soldevila, Miquel Colobran Huguet, Ivan Basart Carrillo, Carles Caño Valls, Jordi Masfret Corrons, Josep Pons Carrió i Jordi Prats Català

Seguretat i alta disponibilitat

Índex

Introducció

Actualment, les tecnologies de la informació han esdevingut un actiu imprescindible en la gestió de tota mena d'activitats. Com a conseqüència, ens trobem davant d'un augment del volum d'informació emmagatzemat en els sistemes informàtics. Algunes d'aquestes dades, molt probablement, contindran informació relacionada amb l'esfera personal o íntima de treballadors o clients.

El creixement d'Internet com a mitjà de comunicació ha comportat que aquesta informació pugui ser vista per persones alienes a l'organització. Per tant, s'ha de protegir de possibles intents d'accés no autoritzat. Cal tenir present que l'obtenció d'informació per mitjans no autoritzats pot ser un comportament que contravingui la llei (accions il·legals) i pot comportar sancions (multes).

En aquest mòdul es treballen 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 la 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 es troben 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 "Seguretat informàtica" s'expliquen els elements relacionats amb el concepte de seguretat informàtica i amb la seva vulneració. Entendre'ls us permetrà conèixer com s'ha d'enfocar la seguretat en cada sistema. Es descriuen també els mecanismes per preservar la informació i s'explica què cal fer en cas que es produeixi un incident de seguretat.

En l'apartat "Legislació sobre seguretat, protecció de dades i Codi Penal" s'analitzen els elements jurídics relacionats amb la informàtica i les accions que poden ser constitutives de delicte. El fet de conèixer-les us permetrà prevenir-les, detectar-les i evitar-les. S'estudien també aspectes relatius a la protecció de dades i se'n justifica la importància. Es desenvolupa la normativa existent i s'analitza com aquesta afecta a l'operativa diària, tant des del punt de vista informàtic com des del punt de vista de l'organització. Veureu algunes regles que us ajudaran a detectar situacions en les quals la normativa no s'aplica correctament i com es poden millorar aquests escenaris.

Al llarg de la unitat anireu entenent que les dades personals (econòmiques, mèdiques, domicili, sociològiques…) s'han de gestionar amb una cura especial. També veureu que la legislació ha estat conscient d'aquest problema i que, per aquest motiu, existeixen moltes normes, com per exemple la Llei Orgànica de protecció de dades personals i garantia dels drets digitals (LOPDGD), que regulen aquesta qüestió.

Aquesta unitat tracta qüestions essencials de l'àmbit de la seguretat informàtica. D'una banda, descriu les mesures de prevenció de la pèrdua d'informació, i de l'altra, explica com la informàtica s'interrelaciona amb el seu entorn, així com les obligacions que persones i organitzacions han de seguir per adequar-se a les normes establertes. És una unitat tant teòrica com pràctica. Per assimilar adequadament aquests continguts és convenient anar fent les activitats i els exercicis d'autoavaluació, així com llegir els annexos.

Resultats d'aprenentatge

En finalitzar aquesta unitat formativa, l'alumne/a:

1. Adopta pautes i pràctiques de tractament segur de la informació, reconeixent les vulnerabilitats d'un sistema informàtic i la necessitat d'assegurar-lo.
    - Valora la importància d'assegurar la privadesa, coherència i disponibilitat de la informació en els sistemes informàtics.
    - Descriu les diferències entre seguretat física i lògica.
    - Classifica les principals vulnerabilitats d'un sistema informàtic, segons la tipologia i origen.
    - Contrasta la incidència de les tècniques d'enginyeria social en els fraus informàtics.
    - Adopta polítiques de contrasenyes.
    - Valora els avantatges que suposa la utilització de sistemes biomètrics.
    - Aplica tècniques criptogràfiques en l'emmagatzematge i la transmissió de la informació.
    - Reconeix la necessitat d'establir un pla integral de protecció perimètrica, especialment en sistemes connectats a xarxes públiques.
    - Identifica les fases de l'anàlisi forense enfront d'atacs a un sistema.
2. Reconeix la legislació i normativa sobre seguretat i protecció de dades valorant-ne la importància.
    - Descriu la legislació sobre protecció de dades de caràcter personal.
    - Determina la necessitat de controlar l'accés a la informació personal emmagatzemada.
    - Identifica les figures legals que intervenen en el tractament i el manteniment dels fitxers de dades.
    - Contrasta l'obligació de posar a disposició de les persones les dades personals que els concerneixen.
    - Descriu la legislació actual sobre els serveis de la societat de la informació i de comerç electrònic.
    - Contrasta les normes sobre gestió de seguretat de la informació.
    - Comprèn la necessitat de conèixer i respectar la normativa legal aplicable.

1. Seguretat informàtica

El concepte de seguretat informàtica és difús i pràcticament inabastable, per la qual cosa ens centrarem en el que podríem anomenar **fiabilitat**, entesa com a garantia de qualitat de servei d'un sistema informàtic. La fiabilitat es pot veure compromesa de moltes maneres, no només en la mesura que tots els components d'un sistema informàtic tenen vulnerabilitats inherents, sinó també per l'acció d'elements externs al propi sistema (des de catàstrofes naturals, fins a l'acció d'intrusos). Malgrat l'aparent feblesa extrema dels sistemes informàtics, el cert és que l'administrador disposa de molts recursos i eines que l'ajuden a assegurar i mantenir la fiabilitat del sistema, així com a detectar les seves mancances de seguretat. Finalment, en cas que es produeixi un problema de seguretat, existeix una disciplina de creació recent, la **informàtica forense**, que pot ser determinant per saber, una vegada produït l'incident, què ha passat i qui n'ha estat l'autor.

1.1 Conceptes de seguretat informàtica: fiabilitat, confidencialitat, integritat i disponibilitat

Encara que sigui d'una manera intuïtiva, tots entenem que un sistema informàtic es considera **segur** si es troba lliure de tot risc o dany. Tot i que no resulta gaire senzill formalitzar el concepte de **seguretat informàtica**, entendrem com a tal la implantació d'un conjunt de mesures tècniques que determinen que els accessos als recursos d'un sistema informàtic siguin duts a terme exclusivament pels elements autoritzats a fer-ho. Atès que és impossible garantir la seguretat o inviolabilitat absoluta d'un sistema informàtic, és preferible fer servir el terme **fiabilitat** en lloc de l'inabastable concepte de seguretat.

En general, doncs, direm que un sistema informàtic és fiable quan se satisfan les tres propietats següents:

- **Confidencialitat:** només poden accedir als recursos que integren el sistema els elements autoritzats a fer-ho. Per recursos del sistema no s'entén solament la informació, sinó qualsevol recurs en general: impressores, processador, etc.
- **Integritat**: els recursos del sistema només poden ser modificats o alterats pels elements autoritzats a fer-ho. La modificació inclou diverses operacions, com ara l'esborrament i la creació, a més de totes les possibles alteracions que es puguin fer sobre un objecte.
- **Disponibilitat**: els recursos del sistema han de romandre accessibles als elements autoritzats.

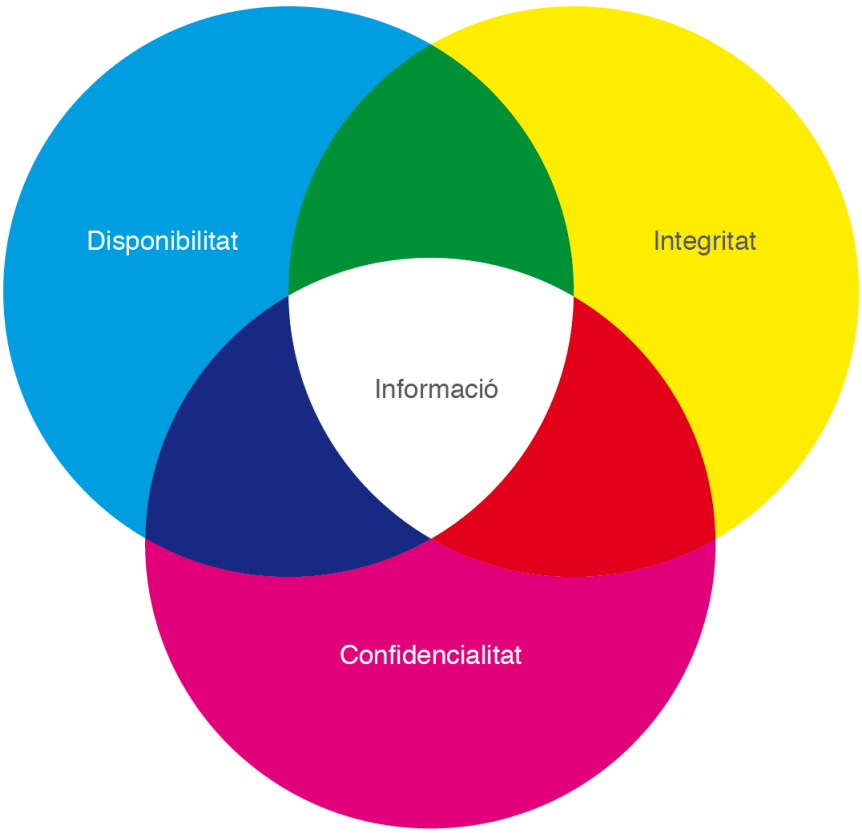
Com podem suposar, és difícil trobar un sistema informàtic que maximitzi les tres propietats. Normalment, i segons l'orientació del sistema, se'n prioritzarà alguna. Per exemple, en un sistema que emmagatzemi dades de caràcter policial, l'element que cal prioritzar és la confidencialitat de la informació (és a dir, mantenir el seu caràcter "secret" o confidencial), tot i que també cal tenir molt en compte la preservació (en la mesura que es pugui) de la integritat i la disponibilitat. Observem que no serveix de res garantir la confidencialitat mitjançant algun mètode criptogràfic si permetem que un intrús pugui esborrar fàcilment la informació emmagatzemada en el disc dur del servidor (atac contra la integritat). D'altra banda, és absolutament necessari que les dades contingudes en una base de dades policial puguin ésser disponibles en el decurs d'una actuació policial, per la qual cosa tampoc podem descuidar la propietat de disponibilitat en un sistema d'aquestes característiques.

En general, cal entendre que la seguretat total no és possible i que les polítiques de gestió sempre són un compromís entre el nivell de seguretat que hom pot o vol assumir i el cost econòmic que això implica.

Vegeu l'apartat "Seguretat lògica" d'aquesta unitat, per conèixer més sobre la criptografia.

La **criptografia** és un mètode secret d'escriptura.

Figura 1.1. La seguretat informàtica com a compromís entre disponibilitat, integritat i confidencialitat



Segons la norma ISO/IEC 27001, estàndard elaborat per la International Organization for Standardization (ISO) i per la International Electrotechnical Comission (IEC), la **seguretat informàtica** consisteix en la implantació d'un conjunt de

mesures tècniques destinades a preservar la confidencialitat, la integritat i la disponibilitat de la informació, abastant altres propietats, com l'autenticitat, la responsabilitat, la fiabilitat i el no repudi (no poder negar la intervenció en una operació o comunicació).

1.2 Elements vulnerables: maquinari, programari i dades

Sabem que és necessari protegir el nostre sistema informàtic, la pregunta que ens podem formular és: quins són els elements del sistema que ens cal protegir? A grans trets, és fàcil adonar-se que qualsevol component d'un sistema informàtic ha de pertànyer a un dels grups següents: maquinari, programari i dades.

- Maquinari: són els elements tangibles o físics del nostre sistema. L'ordinador, els perifèrics, els dispositius d'emmagatzemament, els cables...

- Programari: són els elements lògics del sistema. El sistema operatiu, però també els programes, sense els quals el maquinari no seria funcional.

- Dades: estan constituïdes per aquella informació lògica que processen els programes (elements lògics) fent ús del maquinari (elements físics) com, per exemple, una base de dades de clients.

Existeix una altra categoria, els recursos fungibles, és a dir, aquells que s'usen i es gasten, com ara tòners, CD, cintes de còpia de seguretat... Tot i que no formen part, pròpiament parlant, del sistema informàtic, cal tenir present la seva seguretat. Per exemple, cal decidir on s'han d'emmagatzemar (i a quines mesures de seguretat s'han de sotmetre), elements fungibles tan importants com els suports informàtics que contenen les còpies de seguretat.

Ara bé, de tots aquests recursos o **actius**, quins són els més crítics, és a dir, aquells que necessiten un major grau de protecció? Si bé les inversions en maquinari i programari poden representar despeses milionàries per a una empresa, aquests elements són, al cap i a la fi, normalment substituïbles, a diferència de les dades. Per exemple, què passaria si una gran empresa perdés, sense possibilitat de recuperació, totes les dades relatives als seus treballadors? Com podem comprendre fàcilment, aquesta pèrdua tindria conseqüències catastròfiques per a l'empresa, i per això es diu que **els actius més crítics d'un sistema informàtic són les dades**. Sortosament, qualsevol organització té, avui en dia, polítiques adequades de generació i de recuperació de còpies de seguretat (*backup*), que minimitzen l'impacte d'una pèrdua eventual.

1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic

Extrapolant les definicions anteriors, s'arriba fàcilment a determinar què és una **vulnerabilitat**. És qualsevol punt feble que pugui posar en perill la seguretat d'un sistema informàtic. Aquesta feblesa s'ha d'entendre com una qüestió interna. Pot ser aprofitada per un atacant per violar la seguretat del sistema informàtic, o simplement pot provocar danys de manera no intencionada (per exemple, un error de programació pot fer que un programari tingui comportaments insospitats).

Una **vulnerabilitat** és qualsevol punt feble *intern* que pugui posar en perill la seguretat d'un sistema informàtic. En canvi, les **amenaces** exploten les vulnerabilitats i, per tant, poden ser considerades com a *exteriors* al sistema.

En general, segons el seu origen, les vulnerabilitats es poden classificar de la manera següent:

Exemple de vulnerabilitat d'origen físic

Cal evitar que els dispositius d'emmagatzematge que contenen la informació siguin fàcilment accessibles, o qualsevol usuari en podria extreure les dades de manera no autoritzada.

- **Vulnerabilitats d'origen físic**. Es relacionen amb l'accés físic a les instal·lacions que contenen el sistema informàtic. Si l'organització no manté una bona política d'accés al sistema, provocaria l'aparició d'una vulnerabilitat que podria ser aprofitada per una persona que, sense tenir cap accés autoritzat, en podria extreure dades o provocar danys.

- **Vulnerabilitats d'origen natural**. El caràcter imprevisible i inevitable dels fenòmens naturals fa que difícilment puguem evitar-ne les conseqüències. Si més no, cal intentar minimitzar el seu impacte i disposar de mitjans per recuperar, en la mesura del possible, l'estat original del sistema informàtic. Aquestes vulnerabilitats són conseqüència de no haver pres les mesures adequades davant de la possibilitat que es produeixin fenòmens meteorològics o catàstrofes naturals. Si, per exemple, l'organització es troba ubicada en un lloc on sovint es pateixen inundacions, és clar que si no s'ha pres cap mesura les pluges poden provocar danys molt importants al sistema informàtic.

- **Vulnerabilitats que tenen l'origen en el maquinari**. Estan relacionades amb el mal funcionament dels elements físics del sistema, el qual pot tenir diverses causes: mal disseny dels components, desgast, mal ús, errors de fabricació... Com a conseqüència, el sistema informàtic pot deixar de ser operatiu o funcionar de forma inesperada. Un atacant podria aprofitar aquesta vulnerabilitat per malmetre el sistema.

- **Vulnerabilitats que tenen l'origen en el programari**. Aquestes són les més evidents i conegudes. Es basen en errors de programació o de disseny tant de sistemes operatius com de programes.

- **Vulnerabilitats que tenen l'origen en la xarxa**. Les xarxes són elements molt vulnerables, ja que estan constituïdes per una suma de maquinaris i programaris interconnectats (que, a més, poden presentar vulnerabilitats físiques i naturals). Els principals problemes que poden sorgir arran de les vulnerabilitats en una xarxa són la intercepció de la informació circulant,

així com l'accés no autoritzat a un sistema informàtic (o a diversos) a través de la xarxa. Un element molt condicionant en l'aparició de vulnerabilitats és la tria de la topologia de la xarxa (segons quina es triï serem més sensibles a unes o altres amenaces).

- **Vulnerabilitats que tenen l'origen en el factor humà**. Sol ser la baula més feble i més incontrolable de totes. Ja sigui per manca de formació, de conscienciació o per mala fe, l'element humà és difícilment controlable. No tenim cap poder de decisió sobre les persones que volen cometre atacs contra sistemes informàtics (robatori d'informació, eliminació de fitxers, destrucció de dispositius físics...), però, en canvi, sí és possible, mitjançant una política adequada de formació i conscienciació, evitar moltes conductes causades per la desinformació que podrien posar en perill la seguretat del sistema informàtic d'una organització (per exemple, una bona política de gestió de contrasenyes d'accés).

Les vulnerabilitats del programari es troben directament relacionades amb l'aparició de les **amenaces de programari**, les quals es veuran a l'apartat, "Amenaces", d'aquesta mateixa unitat.

Una de les maneres d'explotar les vulnerabilitats d'origen humà és l'anomenada **enginyeria social**. Consisteix a obtenir informació confidencial manipulant els usuaris legítims.

Exemple d'enginyeria social

Algú que es fa passar per l'administrador del sistema informàtic truca un treballador i li sol·licita, amb qualsevol pretext, la contrasenya d'accés al sistema.

Mals hàbits

Usar contrasenyes fàcils d'esbrinar, tipus "1234", o deixar-les anotades en una etiqueta adhesiva penjada al monitor de l'ordinador.

Una de les formes més conegudes d'enginyera social és la **pesca electrònica** (*phishing*). Aquest tipus de frau es basa en l'enviament de correus electrònics fraudulents (aparentment enviats des d'un origen fiable) en els quals se sol·liciten dades sobre targetes de crèdit, codis d'accés per operar amb comptes bancaris o altres tipus d'informació personal.

1.4 Seguretat física i ambiental

L'adopció de mesures de seguretat **externes** (*físiques* i *ambientals*) és essencial a l'hora de protegir l'actiu més important de qualsevol organització: les dades. Aquestes mesures també ens han de servir per protegir l'element habitualment més car de tot sistema informàtic: el maquinari. Les mesures que es veuran proporcionen protecció davant de fenòmens meteorològics i davant d'incidents amb component humà, com ara robatoris o sabotatges.

Les mesures de seguretat física són uns dels aspectes que més es descuida, però cal anar amb molt de compte, ja que una persona no autoritzada que accedeix al sistema pot causar pèrdues enormes per a l'organització: robatori d'ordinadors, introducció de programari maliciós en el servidor (per exemple, un cavall de Troia o un *keylogger*), destrucció de dades...

Un **enregistrador de teclat** o *keylogger* és un programa o equip que enregistra l'activitat d'un teclat d'una estació de treball.

Cavalls de Troia

Els **cavalls de Troia** són fragments de codi inserits 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.

1.4.1 Ubicació física i condicions ambientals dels equips i servidors

No tots els components d'un sistema informàtic tenen la mateixa rellevància i, per tant, hauran d'estar sotmesos a diferents mesures de seguretat, segons la seva importància i funcionalitat. Per exemple, una **estació de treball** pot ésser fàcilment reemplaçable i pot no allotjar programari o dades gaire rellevants. No obstant això, podria esdevenir una porta d'entrada a tot el sistema informàtic. En aquest cas, doncs, convé que els accessos físics a l'estació només puguin ésser duts a terme pel personal autoritzat. En canvi, els **servidors** es troben contínuament en funcionament i són l'eix central del sistema informàtic. Cal, doncs, protegir especialment els seus accessos físics, així com garantir les condicions ambientals en les quals aquests components han de funcionar.

Per tant, sembla lògic que els servidors s'ubiquin en llocs especialment protegits i específicament dissenyats per treballar en unes condiciones ambientals determinades (temperatura, humitat, altitud, interferències electromagnètiques, vibracions...). Aquests espais (normalment sales grans o edificis sencers) reben el nom de **centres de processament de dades** (CPD) i concentren al seu interior els recursos informàtics necessaris per al processament de les dades d'una organització.

Entre les mesures de control ambiental de què han de disposar els CDP destaquen els sistemes contra incendis i inundacions (extintors, portes ignífugues, drenatges i vies d'evacuació) i els sistemes de control de temperatura (no s'haurien de superar els 30º).

Sistemes d'alimentació ininterrompuda

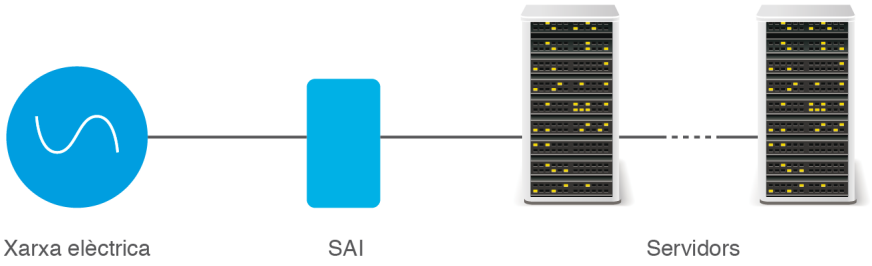
El **sistema d'alimentació ininterrompuda** (SAI) protegeix els servidors de talls de corrent i d'altres problemes relacionats amb la tensió.

Els sistemes d'alimentació ininterrompuda són un altre element especialment important en relació al servidor.

La importància d'un bon corrent per als servidors es deu al fet que un tall de corrent no li permetrà aturar-se correctament. Això farà que les memòries intermèdies (*cache*) es perdin, no s'actualitzin en el disc i quedin fitxers oberts. Així, és possible que quan es torni a posar en marxa el sistema no es pugui engegar correctament i es perdi informació o fitxers. Si algun d'aquests fitxers és una base de dades, les conseqüències poden ser desastroses: s'ha de recuperar de la còpia de seguretat, tenint en compte però, que es perdrà la informació introduïda des que es va fer la còpia fins al moment en què s'ha produït el tall.

Un SAI subministra corrent quan la xarxa elèctrica no en proporciona, de manera que l'ordinador continua funcionant correctament, sense veure's afectat pel fet que no hi ha subministrament elèctric general. Això permet apagar els sistemes amb seguretat.

Figura 1.2. Esquema de xarxa amb SAI



Les característiques més rellevants d'un SAI són les següents:

- **Potència que cal subministrar**. És la potència en watts que pot proporcionar el SAI quan no hi ha corrent d'entrada. Determina el nombre de servidors que s'hi poden connectar.

- **Temps de durada de les bateries**. Els SAI porten bateries que es carreguen amb el corrent elèctric i són les que després proporcionen electricitat quan falla el corrent general. El nombre de bateries determina el temps que podran subministrar corrent abans d'exhaurir-se.

- **Temps de vida de les bateries**. Un SAI serveix de ben poc si falla quan hauria de funcionar. Les bateries tenen una vida útil determinada. Després d'aquest temps, no hi ha garanties que funcionin i responguin correctament quan sigui necessari. És el fabricant del SAI qui determina cada quants anys s'han de canviar les bateries.

- **Avís al servidor**. Actualment, els SAI porten una línia (USB o sèrie) que arriba a l'ordinador. D'aquesta manera, quan entra en funcionament, és capaç d'enviar un senyal al servidor que, amb el programari adient (subministrat amb el SAI), sap que es manté amb l'alimentació elèctrica del SAI. S'estableix un diàleg que informa de l'estat de les bateries del SAI i de la seva durada. Quan falta poc per a esgotar la càrrega de les bateries, el SAI n'informa al servidor i pot procedir a enviar missatges als usuaris i a fer una aturada correcta, ordenada i automàtica de l'ordinador. Els servidors acostumen a estar preparats per arrencar sols, sense intervenció de l'administrador, per la qual cosa quan es restableixi el subministrament elèctric normal, el servidor s'engegarà i tot tornarà a funcionar correctament.

1.4.2 Protecció física dels sistemes informàtics

Les mesures de protecció física abasten el control d'accessos, no només pel que fa a la identificació dels usuaris, sinó també al control físic dels accessos, així com diverses mesures de caire preventiu.

Pel que fa al control físic dels accessos, podem parlar de la utilització de diverses mesures, relativament allunyades del món informàtic, per la qual cosa no se'n farà gaire esment: personal de seguretat, detectors de metalls... Algunes d'aquestes mesures es poden combinar amb la identificació de l'usuari mitjançant mètodes informàtics, els quals sí que ens interessen, per la qual cosa s'explicaran detalladament. No obstant això, abans veurem diverses mesures de prevenció que poden ser d'utilitat a l'hora de configurar la seguretat física de l'edifici:

- 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 a protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància (cal tenir present la normativa que en regula la instal·lació).
- Triar una topologia de xarxa adequada a les nostres necessitats.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Proveir mecanismes d'autenticació als usuaris que volen accedir al sistema.

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

De mecanismes d'autenticació n'hi ha de molts tipus diferents, des dels 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 els que més s'ajustin a les nostres necessitats. També cal tenir en compte que molts d'aquests mecanismes són complementaris i es poden utilitzar alhora.

Mecanismes d'autenticació d'usuaris

Podem classificar els mecanismes d'autenticació d'usuaris de la manera següent:

- Sistemes basats en elements coneguts per l'usuari.

- Sistemes basats en elements que té l'usuari.
    1. Sistemes basats en targetes intel·ligents i testimonis (*tokens*) de seguretat.
    2. Sistemes biomètrics.

1. Sistemes basats en elements coneguts per l'usuari

Els principals mecanismes dins d'aquest tipus d'autenticació són els sistemes basats en contrasenyes. És un dels mètodes que es fan servir més sovint per autenticar els usuaris que volen 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 emprant múltiples tècniques.

Xifra

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 la clau de xifratge.

Tot i que l'ús de contrasenyes s'ha de basar en el sentit comú, no és sobrer fer les recomanacions següents:

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No usar 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, per idiomes, de temes concrets com esports... Aquestes tècniques reben el nom d'*atacs de diccionari*.
- Evitar utilitzar dades que puguin ésser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el mateix nom que l'identificador, el DNI, la data de naixement, el número de mòbil...).
- 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 (!, *, ?...).
- No enviar contrasenyes per SMS o correu ni dir-les per telèfon.
- No utilitzar seqüències de teclat del tipus "qwerty" o "1234" (són seqüències que s'assagen en els atacs de diccionari).
- Fer servir sistemes mnemotècnics per recordar les contrasenyes (per exemple, "Cada dia al matí canta el gall quiquiriquic" donaria lloc a la contrasenya "CDAMCEGC").

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

Molts sistemes informàtics forcen els usuaris a escollir contrasenyes amb un cert nivell de robustesa: obliguen a canviar la contrasenya cada cert temps, que tingui un cert nombre de caràcters, només ofereixen un cert nombre d'intents...

2. Sistemes basats en elements que té l'usuari

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

PIN

El PIN (*Personal Identification Number*) és una contrasenya numèrica, sovint formada per quatre xifres, com, per exemple, el codi numèric que ens demana el 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 compten amb un microprocessador (i memòria) que les dota de les capacitats següents:

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

Per comprendre millor els conceptes de **criptografia** i **signatura digital**, vegeu l'apartat "Seguretat lògica", d'aquesta mateixa unitat.

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.

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

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

Un altre mecanisme d'autenticació, força popular en el sector empresarial, és 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 sessió o cada cert temps). També poden emmagatzemar claus criptogràfiques com, per exemple, la signatura digital o mesures biomètriques.

RFID

RFID (*Radio Frequency Identificatio*n identificació per radiofreqüència) és un sistema d'emmagatzematge 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 en qualsevol altre objecte) amb finalitats d'autenticació.

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 manual). Com a avantatge principal, 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 això encara no es fan servir gaire, tot i que alguns d'aquests mètodes ofereixen un alt nivell de fiabilitat a un preu raonable

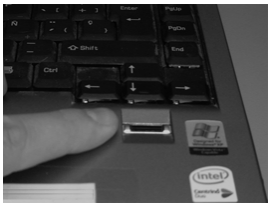
(per exemple, el reconeixement dactilar). Entre les característiques que es poden utilitzar per identificar un usuari mitjançant mesures biomètriques destaquem les següents:

Mesures biomètriques

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

- Veu
- Escriptura i signatura
- Empremtes dactilars
- Patrons de la retina o de l'iris
- Geometria de la mà
- Estructura facial (2D i 3D)
- Traçat de les venes

Els sistemes biomètrics es componen de dos mòduls no interconnectats:



Lector d'empremtes dactilars incorporat en un ordinador portàtil.

- **Mòdul d'inscripció**. A partir de les dades proporcionades pels sensors, s'extreuen els trets característics de la mesura biomètrica de l'usuari (per exemple, una empremta dactilar) i s'emmagatzemen en una base de dades. L'usuari només haurà de fer aquesta operació una vegada.
- **Mòdul d'identificació**. Quan l'usuari es vol autenticar, els sensors extreuen els trets característics de l'usuari i es compara el patró obtingut amb les dades emmagatzemades pel mòdul d'inscripció. Si el patró obtingut coincideix amb l'emmagatzemat, l'usuari és identificat positivament.

Un dels problemes més importants dels sistemes biomètrics és la generació de falsos positius, és a dir, persones que tot i no estar autoritzades pel sistema, són identificades positivament i, per tant, són autoritzades a entrar en el sistema. Aquest és, òbviament, un problema greu. Per solucionar-ho, es pot incrementar la sensibilitat del sistema biomètric, però aleshores també es produirà un increment dels falsos negatius, és a dir, de les persones que tot i estar autoritzades, no són identificades correctament i no poden entrar al sistema. En termes generals, no és possible minimitzar els falsos positius sense incrementar els falsos negatius, de manera que cal arribar a una solució de compromís a l'hora d'ajustar la sensibilitat del sistema biomètric.

Una altra qüestió important pel que fa a l'ús de les mesures biomètriques és el possible rebuig social que puguin patir: per exemple, les persones poden ser reticents a enregistrar el seu ull en un control d'accessos, no només pel fet en si mateix, sinó també per la incertesa de l'ús que podria tenir la recollida de dades tan sensibles com aquestes.

1.5 Seguretat lògica

En contraposició a la **seguretat física** (externa), la **seguretat lògica** fa referència a totes aquelles mesures tècniques i administratives, i, per tant, de caire intern, que hom pot adoptar amb l'objectiu de mantenir la fiabilitat del sistema informàtic.

1.5.1 Criptografia i funcions hash

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 els anomenats mètodes criptogràfics.

Amb la criptografia es pretenen evitar els atacs contra la confidencialitat.

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

S'anomena **criptografia** a 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).

1.5.2 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 només si coneix la clau amb la qual l'emissor ha xifrat el missatge.

Notem que aquests criptosistemes permeten enviar missatges confidencials (per exemple, un correu electrònic) entre un emissor i un receptor, el qual només podrà desxifrar el missatge si coneix la clau amb què ha estat xifrat, però a més, també permeten que un únic usuari emmagatzemi, de forma xifrada, informació en un disc dur, de manera que aquesta només pugui ser recuperada (desxifrada) emprant la clau amb què va ser xifrada.

Un exemple molt entenedor és el **xifratge de substitució** basat en la taula 1.1.

TAULA 1.1. Xifratge de l'alfabet mitjançant una taula de conversió

	A	**B**	**C**	**D**	**E**
A	A	B	C	D	E
B	F	G	H	I	J
C	K	L	M	N	O
D	P	Q	R	S	T
E	U	V	X	Y	Z

Les lletres de l'alfabet es disposen dins de la taula, de manera que cada caràcter del text que es vulgui xifrar se substituirà pel parell (fila i columna) de la lletra en qüestió. Per exemple, la paraula AVUI quedaria codificada com AAEBEABD (és a dir, AA-EB-EA-BD). Naturalment, si emissor i receptor comparteixen aquesta taula, els serà molt senzill xifrar i desxifrar missatges. A la pràctica, els criptosistemes reals són molt més complexos i no és gens senzill desxifrar-los, ni tan sols amb l'ajut dels ordinadors més potents.

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 o Blowfish. 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.

1.5.3 Criptosistemes de clau pública

A diferència dels criptosistemes de clau privada, molt intuïtius però 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.

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

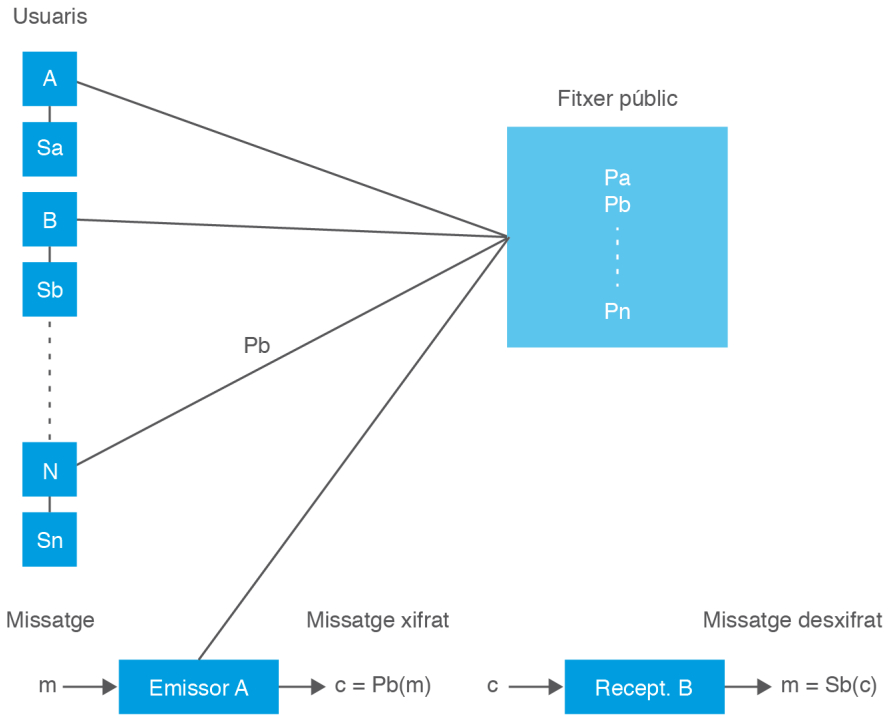
Criptosistemes de clau pública

Donada qualsevol clau del parell <*Pu*, *Su*>, 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), *Pu*, no és possible obtenir la clau privada

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, convenientment protegida). Podeu veure descrit aquest mecanisme en la figura 1.3.

Figura 1.3. Xifratge i desxifratge d'un missatge en un criptosistema de clau pública



A: usuari A

Sa: clau secreta de l'usuari A.

Sb: clau secreta de l'usuari B.

Pa: clau pública de l'usuari A.

Pb: clau pública de l'usuari B.

m: missatge a enviar

Pb(m): el resultat d'aplicar el xifratge al missatge m, usant la clau pública de l'usuari B. S'obté un nou missatge c, xifrat, que necessita de la clau secreta de B per a poder ser llegit.

Sb(c): el resultat d'aplicar el desxifratge al missatge c, usant la clau privada de l'usuari B. S'obté el missatge original, m. Ara ja pot ser llegit.

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

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

Un avantatge molt important del criptosistema de clau pública és que permet la incorporació d'una **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-repudi**).

DSS

El **Digital Signature Standard (DSS)** és un sistema de signatura digital adoptat com a estàndard pel National Institute of Standards and Technology (NIST). 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.

Les funcions hash o funcions resum

Una **funció *hash*** o funció resum 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 512 bits (segons la funció que s'empri) i s'anomena *valor resum del missatge*.

Per exemple, el que es pot veure a continuació és el resultat d'aplicar una funció resum a un fitxer anomenat Hola.txt:

Hola.txt 89736DF30DC47A7D5AC22662DC3B5E9C

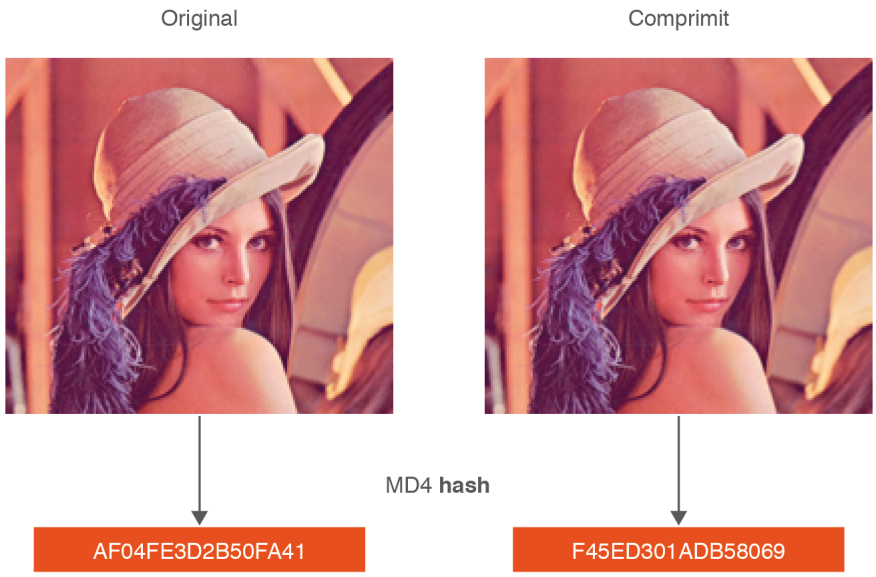
El valor *hash* identifica, pràcticament de manera unívoca, un fitxer qualsevol. Podríem dir, doncs, que exerceix de codi ADN de fitxers. No obstant això, cal fer una matisació important: existeix una probabilitat, encara que molt petita, que dos fitxers **diferents** tinguin el mateix valor *hash* (**col·lisió**). A la pràctica, les col·lisions observades pels matemàtics s'han produït, no pas de manera accidental, sinó que s'han cercat de manera expressa.

Els algorismes **MD5** (*Message Digest*, desenvolupat per Ron Rivest i amb resums de 128 bits, qüestionat des de l'any 2004) i **SHA-1** (*Secure Hash Algorithm*, desenvolupat per la NSA (*National Security Agency*) agència de seguretat nord-americana i amb resums de 160 bits) són els que més es fan servir per implementar les funcions resum. Malgrat el problema de les col·lisions i certes vulnerabilitats que pateix la funció MD5, és ràpida i encara útil a efectes de verificació.

Una característica molt important de les funcions *hash* és que qualsevol canvi que es produeixi sobre el fitxer comporta un canvi total i impredictible del valor *hash*. Així, doncs, n'hi ha prou canviant un únic píxel d'una fotografia perquè el valor *hash* canviï completament. Per tant, si, per exemple, obrim qualsevol fotografia amb el programa Paint del sistema operatiu Windows i el sobreescrivim amb el mateix programa, el seu valor *hash* es veurà completament alterat a causa de les dades que el programa afegeix a la fotografia en el moment de sobreescriure-la. Qualsevol alteració en un fitxer comporta el canvi radical del valor *hash*. Això vol dir que continguts idèntics poden estar representats per valors *hash* diferents.

En l'exemple següent (figura 1.4) podem observar el càlcul del valor *hash* (MD4) d'una fotografia i de la seva equivalent comprimida (la compressió, com qualsevol canvi, també provoca una variació del valor *hash)*.

Figura 1.4. Càlcul del valor hash (MD4) d'una imatge i de la imatge comprimida



1.5.4 Llistes de control d'accés

La confidencialitat vetlla perquè només les persones autoritzades accedeixin als recursos. Això es fa usant llistes de control d'accés.

Control d'accés

Una de les qüestions fonamentals en el disseny de l'entorn de l'usuari és aconseguir que aquest accedeixi únicament a allò que necessiti. Aquesta regla s'anomena *principi de privilegi mínim*. Quan un usuari necessita accedir a un recurs del sistema informàtic, primer de tot s'identifica (s'autentica). Una vegada s'ha identificat, el sistema controla (autoritza) l'accés als recursos del sistema informàtic tot registrant (auditant) com s'utilitza cada recurs. En la figura 1.5 es pot veure de manera gràfica.

Principi de privilegi mínim

Consisteix a atorgar a l'usuari el conjunt de privilegis més restrictiu (l'autorització més baixa) necessari perquè pugui dur a terme la seva tasca.

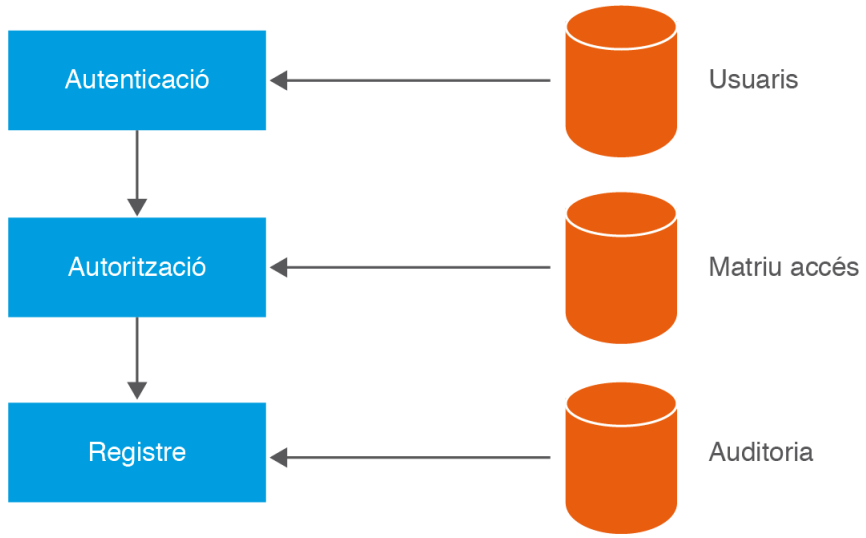
- **Autenticació**: mecanisme de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic. Habitualment es fa mitjançant nom de l'usuari i contrasenya o testimoni (*token*) del procés.
- **Autorització**: procés mitjançant el qual el sistema autoritza a l'usuari identificat a accedir als recursos d'un sistema informàtic. L'autorització determina quin accés es permet a cada entitat. L'autenticació és el procés de verificar la identitat d'una persona, mentre que l'autorització és el procés

de verificació, que una persona determinada té l'autoritat per realitzar certa operació. L'autenticació, per tant, ha de precedir l'autorització.

- **Registre**: informació de registre (*log*) de l'ús que l'usuari fa dels recursos del sistema informàtic.

El **control d'accés**, per tant, determina quins privilegis té un usuari dins del sistema informàtic i a quins recursos té accés.

Figura 1.5. Procés de validació



Matriu de control d'accés

Els recursos als quals té accés una entitat es determinen mitjançant la **matriu de control d'accés o matriu d'accés**. És un model formal de seguretat computacional (usat en sistemes informàtics) que inventaria els drets de cada subjecte respecte als objectes del sistema. Els objectes són entitats que contenen informació, poden ser físics o abstractes. Els subjectes accedeixen als objectes, i poden ser usuaris, processos, programes o altres entitats.

Els drets d'accés més comuns són l'accés de lectura (L), l'accés d'escriptura (E) i l'accés d'execució (X).

Taula 1.2. Matriu de control d'accés

Objecte Domini	Fitxer	Directori
D1	Lectura	Lectura Escriptura Execució
D2	Execució	Lectura Escriptura
D3	Execució	Lectura

Les files de la matriu representen dominis (o subjectes) i les columnes representen objectes. Les entrades de la matriu consisteixen en una sèrie de drets d'accés. Per exemple, l'entrada corresponent al domini D2 sobre un directori de la taula 1.2

defineix el conjunt d'operacions que un procés, executant-se en el domini D2, pot invocar sobre un objecte O situat dins del directori.

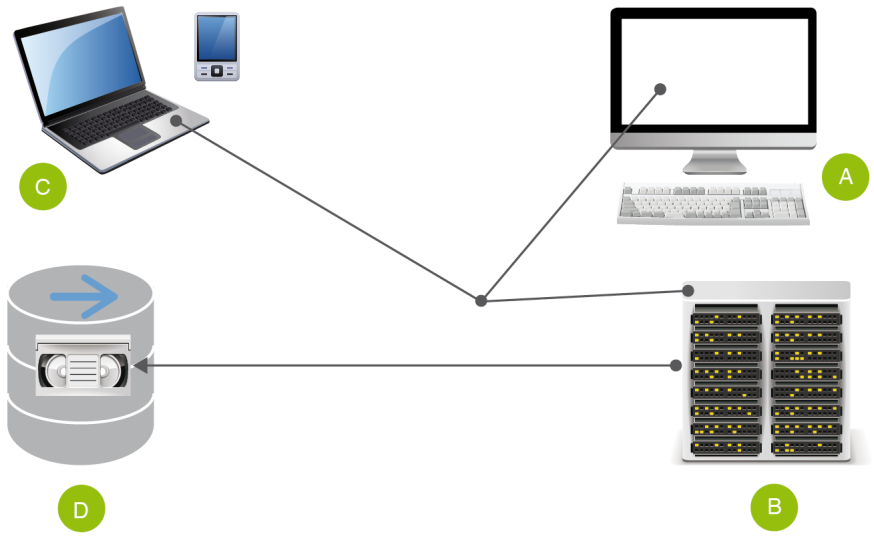
Llista de control d'accés (ACL)

Els sistemes informàtics no acostumen a guardar la matriu, ja que pot ser molt gran. Gran part dels dominis no tenen cap accés a la majoria dels objectes, de manera que l'emmagatzematge d'una matriu enorme gairebé buida seria un malbaratament d'espai de disc. El que es fa és associar a cada objecte una llista (ordenada) amb tots els dominis que poden tenir-hi accés i la forma de fer-ho. Aquesta llista s'anomena *llista de control d'accés* (ACL).

1.5.5 Polítiques d'emmagatzematge

Per poder mantenir d'una manera segura i eficaç els sistemes d'emmagatzematge és important especificar quines són les polítiques que tots els usuaris han de seguir per evitar que augmenti l'ús de la capacitat d'emmagatzematge de manera desordenada, amb la conseqüent manca de control o pèrdua d'informació. Així, tal i com es pot veure a la figura 1.6, existeixen quatre polítiques bàsiques d'emmagatzematge, depenent d'on siguin les dades.

FIGURA 1.6. Ubicació de les dades en un sistema informàtic



(A) Polítiques d'emmagatzematge local en els equips de treball.

(B) Política d'emmagatzematge a la xarxa corporativa.

(C) Política sobre l'ús de dispositius externs.

(D) Política de còpies de seguretat.

Polítiques d'emmagatzematge local en els equips de treball

S'estableixen unes normes d'emmagatzematge per als equips de treball de l'empresa (equips de sobretaula, equips portàtils, telèfons i altres dispositius) que els usuaris han de complir. Aquesta política inclou almenys els aspectes següents:

- Quin tipus d'informació es pot emmagatzemar en els equips locals.
- Quant de temps ha de romandre aquesta informació en els equips.
- Permanència de la informació en la xarxa local un cop transmesa als servidors corporatius.
- Ubicació dins de l'arbre de directoris de l'equip.
- Utilització de sistemes de xifratge d'informació en els documents empresarials.
- Normativa d'emmagatzematge de documents personals, fitxers de música, fotografies..., i en concret relativa a fitxers protegits per drets d'autor.

Política d'emmagatzematge a la xarxa corporativa

A la xarxa corporativa és necessari distingir entre la informació de l'empresa que han d'utilitzar tots els usuaris i la informació dels treballadors emmagatzemada en aquesta xarxa:

- Els servidors d'emmagatzematge disponibles a la xarxa corporativa estan configurats per poder emmagatzemar i compartir la informació de l'empresa que ha de ser utilitzada pels treballadors. Els controls d'accés són definits per la direcció i el responsable de sistemes, amb l'objectiu de destriar qui pot accedir i on, mentre que el contingut de la informació emmagatzemada es determina mitjançant una política d'ús específica que ha de cobrir almenys els aspectes següents:
  - Tipus d'informació emmagatzemada, moment de l'emmagatzematge i ubicació dins dels directoris del sistema.
  - Persones encarregades de l'actualització d'aquesta informació en cas de modificació.
- Els treballadors poden disposar de bústies o carpetes personals dins de la xarxa corporativa. En aquestes carpetes s'emmagatzema informació que, si bé té relació amb el seu treball, no és necessàriament compartida per altres membres de l'equip. Per controlar aquesta informació s'han d'especificar polítiques que determinin els mateixos aspectes que en el cas de l'emmagatzematge local.

Política sobre l'ús de dispositius externs

Especialment important són les normes relatives a l'ús d'equips externs que, connectats als equips de treball, permeten l'emmagatzematge extra d'informació per tal de transportar-la a una altra ubicació o simplement de disposar d'una còpia de seguretat personal. Aquesta política inclou almenys els aspectes següents:

- Si està permès o no l'ús d'aquests dispositius.
- En cas afirmatiu, quin tipus d'informació no es permet emmagatzemar en cap cas, com, per exemple, dades personals de clients.
- Quins mètodes d'esborrat s'han de fer servir quan aquesta informació ja no es necessita.

Política de còpies de seguretat

Una còpia de seguretat, també coneguda com a *backup*, és un duplicat de fitxers o aplicacions contingudes en un ordinador que es realitza per recuperar les dades en el cas que el sistema d'informació pateixi danys o pèrdues accidentals de les dades emmagatzemades. Tot pla de contingència d'una empresa ha de comptar amb una planificació adequada de les còpies de seguretat que es realitzen, ja que la pèrdua de dades pot posar en perill la continuïtat del negoci.

Alguns dels requisits que ha de complir la planificació de còpies de seguretat són:

- Identificar les dades que han de ser preservades. Són aquelles la pèrdua de les quals afectaria la continuïtat del negoci.
- Establir la freqüència amb què es faran les còpies. Aquesta freqüència influeix en la quantitat d'informació que es pot perdre pel que fa a la font original. Aquest paràmetre és molt important i requereix una anàlisi exhaustiva.
- Per exemple, si es realitza una còpia cada nit i el suport s'espatlla a les dotze del migdia tota la informació generada des de la nit anterior fins a les dotze no serà a la còpia de seguretat.
- Disposar el magatzem físic per a les còpies. Aquest magatzem es determina en funció de la seguretat que requereix la informació. Pot ser un magatzem situat al mateix edifici o en un edifici extern. Per exemple, si es produeix un incendi a l'edifici de l'empresa, la informació emmagatzemada en un magatzem remot segueix estant disponible.
- Cercar la probabilitat d'error mínima. Assegurar-se que les dades són copiades íntegrament de l'original i en uns suports fiables i en bon estat. No s'han d'utilitzar suports que estiguin al final de la seva vida útil per evitar que fallin quan s'intenti recuperar la informació.
- Controlar els suports que contenen les còpies. Guardar-los en un lloc segur i només permetre'n l'accés a les persones autoritzades.

- Planificar la restauració de les còpies:
  - Formar els tècnics encarregats de realitzar-les.
  - Disposar de suports per restaurar la còpia diferents dels de producció.
  - Establir els mitjans per disposar d'aquesta còpia en el menor temps possible.
- Provar el sistema exhaustivament per comprovar la seva correcta planificació i l'eficàcia dels mitjans disposats.
- Definir la vigència de les còpies establint un període en què aquesta còpia deixa de tenir validesa i s'ha de substituir per una informació més actualitzada.
- Controlar l'obsolescència dels dispositius d'emmagatzematge. Per al cas d'aquelles còpies que emmagatzemen informació històrica de l'organització, per exemple projectes ja tancats, s'ha de tenir en compte el tipus de dispositiu en el qual s'ha realitzat la còpia, per evitar que en el moment que es requereixi la restauració de aquesta informació ja no existeixin lectors adequats per al dispositiu.
- Quan es rebutgin els suports d'emmagatzematge perquè hagin arribat al límit de vida útil fixat en la política de còpies de seguretat, és important realitzar un procés d'esborrat assegurança o destrucció per assegurar que la informació que conté no podrà ser recuperada posteriorment.

1.5.6 Còpies de seguretat i imatges de suport

Una bona política de còpies de seguretat és clau per tenir segura la informació de l'organització. Alguns motius per fer còpies de seguretat són els següents:

- Protegir la informació contra una fallada del sistema o algun desastre natural.
- Protegir la informació dels usuaris (els fitxers) contra esborraments accidentals.
- Protegir la informació dels usuaris i de l'organització contra atacs per part de tercers.
- Duplicar la informació dels usuaris per a casos d'ús incorrecte que la deixin inconsistent o la modifiquin incorrectament.
- Possibilitar el traspàs de la informació quan s'actualitza o es reinstal·la el sistema.

Tipus de còpies de seguretat

Depenent de la quantitat de fitxers que es guardin, podem distingir els tipus de còpia de seguretat següents:

- **Còpia de seguretat completa**: també es coneix amb el nom de *còpia de seguretat total* o *còpia 'full dump'*. Es fa una còpia de tota la partició del disc en cinta (generalment es fa així, tot i que no és l'únic suport possible). Sovint, la còpia es fa atenent a l'estructura del dispositiu i sense tenir en compte el sistema de fitxers, ja que només cal conèixer la taula de particions del disc i en quina part hi ha la partició per duplicar-la en un dispositiu de cinta. En aquests casos, la restauració no pot ser selectiva: s'ha de restaurar tota la partició i no es pot seleccionar només un fitxer. Es pot fer també una còpia de seguretat completa del sistema de fitxers, la qual sí que és pot restaurar selectivament.

- **Còpia de seguretat incremental**: en aquest cas es guarden només els fitxers que s'han modificat des de l'ultima còpia de seguretat que s'ha fet. Les còpies de seguretat incrementals s'utilitzen conjuntament amb les còpies de seguretat completes en el que s'anomenen *polítiques de còpies de seguretat*.

- **Còpia de seguretat selectiva**: també és possible fer una còpia de només uns fitxers determinats. Normalment això es duu a terme amb fitxers de comandes.

- **Còpia de seguretat diferencial**: aquest sistema realitza una còpia de tots els fitxers que s'han modificat des de la darrera còpia total. Així, si realitzem una còpia total cada dissabte i diferencial la resta de dies, la còpia de divendres contindrà tots els fitxers modificats des de dissabte.

La còpia diferencial té diversos avantatges respecte de la còpia total. El primer és que requereix menys espai, i el segon, associat al primer, és que redueix el temps o finestra de còpia.

Respecte a la còpia incremental aporta l'avantatge que en el procés de recuperació només necessitarem l'última còpia total i l'última còpia diferencial. Tanmateix, a partir del segon dia, la còpia diferencial requerirà més espai i més temps de còpia. La diferència entre la còpia de seguretat incremental i diferencial es pot veure a la figura 1.7 i a la figura 1.8.

Figura 1.7. Copia de seguretat incremental

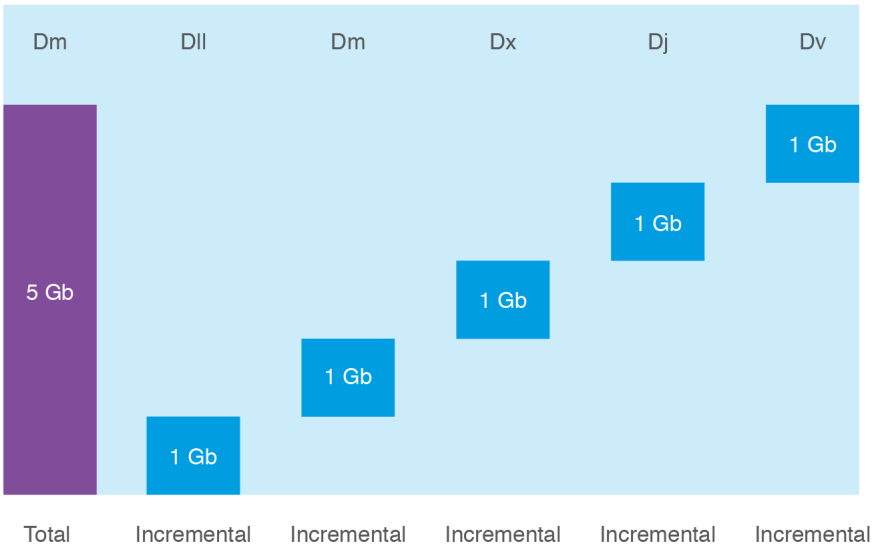
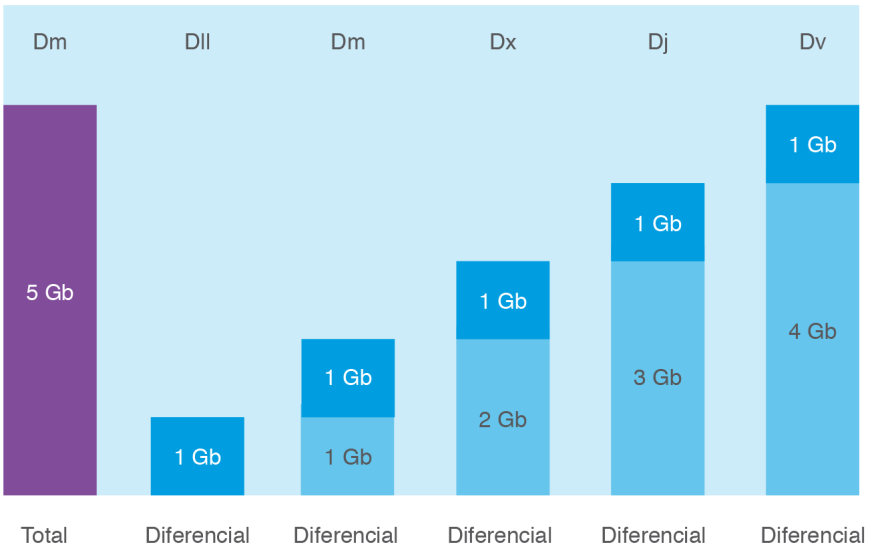


Figura 1.8. Copia de seguretat diferencial



Polítiques de còpies de seguretat

L'estratègia de les còpies de seguretat és crítica per garantir que el procés es faci correctament i que la informació es pugui restaurar quan calgui.

La necessitat d'elaborar estratègies de còpia de seguretat deriva del fet que actualment en els servidors els discos tenen molta capacitat i contenen molta informació, que no cap en un sol dispositiu de sortida (en una sola cinta, per exemple). A més, la transferència pot durar hores i, per tant, s'han de buscar solucions per optimitzar el procés.

Analitzem la variabilitat de la informació. A primera vista podem adonar-nos que

no sembla gaire encertat copiar-ho tot diàriament. En conseqüència, hem de fer una classificació de la informació:

- Informació que varia diàriament
- Informació no variable

1. **Informació que varia diàriament.** Cal fer una còpia diària de la informació que varia cada dia. Aquesta informació es pot trobar en els servidors o distribuïda per tota l'organització. En aquest escenari, guardarem la primera còpia total de cada mes. D'aquesta manera, sempre és possible recuperar les dades de mesos anteriors. Això té uns avantatges:
   - La còpia és ràpida perquè no hi ha còpies totals diàriament i les incrementals només copien els fitxers modificats durant el dia, que són pocs.
   - S'estalvien cintes, ja que les còpies incrementals ocupen poc en relació amb les totals.

     Però també presenta alguns problemes:
   - Recuperar un fitxer requereix temps, perquè s'ha de passar pel conjunt de cintes que van des de l'ultima còpia total i per totes les incrementals fins al fitxer de la data que es busca.
   - Si falla una cinta incremental no es pot recuperar cap dada de les còpies incrementals posteriors.
2. **Informació no variable.** Hi ha informació que es modifica molt poc al llarg del temps. Aquesta informació necessita uns altres criteris de valoració pel que fa a la còpia de seguretat. L'estratègia que s'acostuma a seguir és la següent:
   - Informació de sistema. La informació de sistema dels servidors (les particions amb els operatius) es considera essencial. Perdre-la implica una fallada crítica de l'estructura informàtica. Per tant, com que els fitxers de registre també varien, s'acostumen a considerar informació variable i se'n fa una còpia diària.
   - Aplicacions. Les aplicacions dels usuaris no són dades que variïn amb gaire freqüència, per la qual cosa fer-ne una còpia diària carregaria molt el sistema. Per tant, normalment només se'n fa una còpia manual (controlada pels administradors) quan hi ha modificacions en el contingut.
   - Estacions de treball. També tenen informació de sistema, dades i aplicacions. Normalment, la informació de sistema (el sistema operatiu) i d'aplicacions és pràcticament igual en totes les estacions. Fer-ne una còpia diària desbordaria el sistema de còpies i col·lapsaria la xarxa per guardar pràcticament la mateixa informació. En cas de desastre es pot recórrer a la restauració a partir d'imatges de les estacions de treball. A més, en principi a les estacions no hi hauria d'haver informació, però si n'hi ha ja es fa, com s'ha explicat en el

punt anterior, una còpia diària exclusivament d'aquesta informació de l'estació de treball.

Hi ha informació de la qual no cal fer còpia de seguretat (els fitxers temporals, per exemple).

Aquí teniu algunes recomanacions sobre on guardar les còpies de seguretat:

- Sempre hi ha d'haver una còpia de seguretat fora de l'organització. La freqüència en què cal actualitzar-la dependrà de la política de còpia de seguretat implementada. Pot estar en una caixa forta d'un banc o en mans d'alguna persona de la direcció, per exemple. En cas de desastre tindrem bona part de la informació, no s'haurà perdut tot.
- En cas que l'organització tanqui en alguns períodes com, per exemple, durant les vacances o, en general, en períodes en què la seguretat global de l'edifici es relaxa, és molt important que hi hagi una còpia fora de l'organització per prevenir un desastre.
- Actualment hi ha empreses que es dediquen a emmagatzemar còpies de seguretat seguint protocols de seguretat i acords de confidencialitat pactats amb els seus clients. És una opció que pot ser útil per a algunes organitzacions.

1.5.7 Mitjans d'emmagatzematge

Guardar la informació sempre ha estat un problema. Per aquest motiu els mitjans d'emmagatzematge han variat considerablement al llarg de la història de la informàtica. Els principals sistemes usats han estat els següents:

Targetes perforades al tèxtil

Les targetes perforades han estat utilitzades també per Joseph Marie Jacquard en els telers. De fet, la informàtica va agafar la idea de les targetes perforades de la indústria tèxtil.

- **Targetes perforades**. És una cartolina rectangular amb un codi binari fet amb perforacions en llocs concrets. Aquests van ser els primers mitjans utilitzats per introduir informació i instruccions en sistemes informàtics cap als anys 1960 i 1970.
- **Cintes perforades**. És el pas lògic següent a les targetes perforades. És una tira llarga de paper en la qual es realitzen forats per emmagatzemar les dades.
- **Cintes magnètiques.** És un suport d'emmagatzematge de dades en què es grava sobre una banda plàstica amb un material magnetitzat (generalment òxid de ferro). El tipus d'informació que es pot emmagatzemar en les cintes magnètiques tant pot ser analògic (àudio o vídeo) com digital (dades o programes). Actualment aquest sistema d'emmagatzematge és molt usat com a mitjà per guardar còpies de seguretat. Existeix una gran varietat de cintes magnètiques:

- **DAT**. Els DAT (Digital Audio Tape) són molt habituals, generalment són SCSI (Small Computers System Interface), i n'hi ha de diverses capacitats, que poden arribar fins a uns 20 GB per cinta.
- **DLT**. Les cintes DLT (Digital Linear Tape) també són generalment SCSI i n'hi ha de diferents capacitats, que poden anar dels 20 als 100 GB (sense compressió), fent servir SDLT (Super DLT).
- **AIT**. Les cintes AIT (Advanced Intelligent Tape) també són generalment SCSI i poden tenir entre 25 i 100 GB de capacitat (amb AIT3). La capacitat depèn de la generació de cinta i tecnologia de compressió.
- **LTO**. Les cintes LTO (Linear Tape Open) són una nova tecnologia desenvolupada per Hewlett-Packard, IBM i Seagate. Aquests tipus de cintes han anat evolucionant ràpidament. Mentre que a l'any 2000 parlàvem de LTO 1, que permetia fins a 100 GB de còpia per cinta, actualment la capacitat de les cintes LTO4 arriba fins a 800 GB sense compressió (1,6 TB amb compressió). La seva velocitat de còpia pot arribar a 120 Mb/s, i ja estan planificades les versions LTO5 i LTO6, que permetran emmagatzemar fins a 3,2 TB a una velocitat de 270 Mb/s.

Quan es parla de capacitat de les unitats de cinta ens referim a capacitat sense compressió. Aplicant compressió, la capacitat es pot duplicar o més.

Hi ha altres cintes magnètiques, com per exemple l'Hexabyte, però aquestes quatre són les més esteses.

Tendències

Gràcies a la proliferació de xarxes SAN (Storage Area Network) o dispositius NAS (Network Attached Storage), que ofereixen una gran quantitat d'espai per emmagatzemar, s'utilitzen cada cop més els discos com a dispositiu de còpia. Els mateixos proveïdors de maquinari ofereixen eines específiques que permeten fer aquestes còpies sense interrompre el normal funcionament del sistema .

- **Discos magnètics o disquets**. Estan composats per una peça circular de material magnètic, fina i flexible (d'aquí en ve la denominació) tancada en una coberta de plàstic quadrada o rectangular. Ja no s'utilitzen. N'hi havia de varies mides (3, 3 1/2, 5 1/4 i 8 polzades).
- **Discs durs**. És un dispositiu d'emmagatzematge de dades. Utilitza un sistema de gravació magnètica per emmagatzemar dades digitals. Està fabricat amb un o més discos rígids (anomenats plats), units per un mateix eix que gira a gran velocitat dins d'una caixa metàl·lica segellada. En cadascuna de les cares de cada plat (superior i inferior) hi ha un capçal de lectura/escriptura que sura sobre una fina làmina d'aire generada per la rotació dels discos (efecte Bernoulli).
- **Discs durs externs**. És un disc dur que és fàcilment transportable arreu sense necessitat de consumir energia elèctrica o bateria. Es connecten als ordenadors personals pel port USB (bus sèrie universal).
- **Discs òptics o CD**. Suport digital òptic utilitzat per emmagatzemar diferents tipus d'informació (àudio, imatges, vídeo, dades, programes). Els CD estàndard tenen un diàmetre de 12 centímetres i poden emmagatzemar fins a 80 minuts d'àudio (o 700 MB de dades).
- **DVD**. És, com el CD, un suport digital òptic. L'emmagatzematge es pot fer de diverses maneres. Així, trobem el DVD-ROM (dispositiu només de lectura), DVD-R i DVD + R (només es possible escriure-hi una vegada), DVD -RW i DVD + RW (permeten gravar i esborrar dades les vegades que es vulgui).

- **Blu-ray**. És un nou format de disc òptic. El Blu-ray és un disc de la mateixa mida que un DVD (12 cm) i amb una capacitat de 25 GB per cara (50 GB en total a una velocitat de 36 Mbit/s). Existeixen ja el BD-R i el BD-RE (gravable i regravable respectivament).

- **Memòria Flash**. És un sistema d'emmagatzematge digital basat en semiconductors. Té moltes similituds amb la memòria RAM, però el seu contingut (informació) no es destrueix quan manca corrent. Per la seva elevada velocitat, durabilitat i baix consum d'energia, la memòria Flash s'usa en càmeres digitals, telèfons mòbils, impressores, PDA, ordinadors portàtils i dispositius que emmagatzemen i reprodueixen so, com els reproductors d'MP3. Aquest tipus de dispositiu no utilitza elements mecànics. Aquest factor n'augmenta molt la velocitat i la vida útil i disminueix considerablement el consum d'energia. Existeixen diversos formats de targetes de memòria, com Compact Flash, Secure Digital (anomenades SD), Memory Stick, MMC (MultimediaCard) o xD Picture Card. La diferència entre ells (a part d'aspectes mecànics com l'encapsulat o els connectors) rau en la velocitat de transferència.

- **Discs d'estat sòlid (SSD)**. És l'evolució natural dels dispositius d'emmagatzematge de dades perquè no utilitza components mecànics. La seva capacitat és comparable a les dels discs durs mecànics amb una velocitat de transferència més elevada.

- **Llibreries de còpia**. Ens podem trobar que la nostra organització manipuli quantitats de dades que ocupin diverses cintes de còpia al dia. En aquest cas, una sola persona es passaria el dia fent còpies de seguretat i no acabaria mai. Quina és la solució per a aquests volums d'informació tan grans? Hi ha uns dispositius anomenats *llibreries de còpia*. Són externs, disposen de braços articulats i contenen de 20 a 2.000 cintes de còpia de seguretat. Són com robots.

Còpia disc a disc

En sistemes crítics, i més tenint en compte el cost i la capacitat actual d'aquests dispositius, no s'ha de descartar la possibilitat de fer una còpia de seguretat (o fins i tot de copiar tota la informació) en un altre disc dur només dedicat a aquesta funció. L'estratègia és fer una primera còpia de seguretat en un disc dur (es pot fer amb un procediment automàtic i diverses vegades al dia, si cal), i d'aquest disc, posteriorment, fer-ne una còpia de seguretat en un altre dispositiu (que pot ser una cinta).

Amb el programari adient, l'usuari veu, per exemple, una unitat de 400 TB de capacitat. El programa sap en quina cinta està emmagatzemada la còpia i quines cintes estan plenes, i executa la política de substitució de cintes. Les llibreries de còpia només tenen sentit per a organitzacions de grans dimensions o bé que gestionen quantitats d'informació molt grans.

Llibreries de còpia comercials

Hi ha diverses fabricants de maquinari que comercialitzen llibreries de còpia en col·laboració amb marques de programari, perquè puguin funcionar correctament amb els servidors en què s'instal·lin. Algunes d'aquestes marques són Qualstar, Adic, Hewlett-Packard, StorageTek o Quantum (ATL).

1.6 Amenaces

Les **amenaces** són esdeveniments externs que poden causar danys al sistema informàtic. A diferència de les vulnerabilitats, que són factors interns, les amenaces representen accions malicioses que poden provocar danys. Així, una amenaça pot explotar una determinada vulnerabilitat per causar dany al sistema. Les **contramesures** són les accions que es poden dur a terme per evitar una amenaça determinada.

1.6.1 Amenaces físiques

La **humitat relativa** és el percentatge de la humitat total (quantitat de vapor d'aigua) que pot contenir l'aire a la temperatura a la qual ens trobem.

Les amenaces físiques tenen a veure amb els factors ambientals en els quals operen els equipaments informàtics. Podem esmentar els següents:

- **Temperatura ambiental.** Els ordinadors haurien de funcionar en ambients que tinguin temperatures entre els 10 i els 35 ºC. Cal garantir, doncs, que els ordinadors estiguin adequadament ventilats i que les condicions ambientals (pel que fa a la temperatura) no siguin extremes. En cas contrari, alguns xips poden deixar de funcionar.

- **Humitat**. L'excessiva humitat també pot provocar danys a l'ordinador (curt-circuits, corrosió dels components metàl·lics, degradació de les propietats dels components interns...). Els aparells d'aire condicionat poden ajudar a mantenir un nivell acceptable d'humitat a les zones de treball (una humitat relativa del 20-80%). També pot ser útil instal·lar humidificadors.

- **Pols i partícules diverses**. Aquestes partícules poden interferir en el funcionament dels components mecànics de l'ordinador. Per exemple, si hi ha pols a la unitat lectora de CD, en pot dificultar el funcionament, l'acumulació de pols pot produir problemes de ventilació...

- **Altitud**. Els components elèctrics poden funcionar malament si l'altitud en què ens trobem és excessiva (ara bé, aquest problema és molt difícil que el trobem a la pràctica).

- **Impactes i vibracions**. Els impactes directes poden malmetre de manera evident un ordinador, tant pel que fa a la seva aparença externa, com als components interns que, a causa del cop, es poden desprendre o espatllar-se. També cal tenir en compte les vibracions a què està sotmès contínuament un ordinador en funcionament.

- **Descàrregues electrostàtiques** (en anglès, *electrostatic discharge* o ESD). Es produeix quan una persona que té una càrrega elèctrica estàtica toca un component d'un ordinador. Pot passar en ambients secs, amb humitats relatives menors al 50%, i pot produir danys en xips i fins i tot en discs durs

(si els manipulem amb les mans). Per evitar aquest problema hi ha diverses solucions, una de les qual és l'ús de braçalets antiestàtics.

- **Interferències electromagnètiques i de radiofreqüència**. Aquestes interferències es poden produir pels dispositius que hi ha al voltant del nostre sistema (o bé, per exemple, per una antena en un edifici proper), i poden ocasionar el funcionament defectuós d'algun component de l'ordinador mentre dura la interferència (per exemple, alteracions de la imatge en el monitor). I a la inversa, el nostre sistema informàtic també pot produir interferències sobre altres dispositius, com ara telèfons mòbils o aparells de televisió. Per solucionar-ho cal mantenir, en la mesura del possible, la separació d'aquests dispositius amb l'ordinador que les provoca, emprar cables blindats per connectar perifèrics, i fer funcionar l'ordinador amb la coberta instal·lada.

- **Magnetisme**. Cal tenir present que les superfícies magnètiques dels plats giratoris dels discs durs són susceptibles de patir alteracions arran de les seves propietats magnètiques (per exemple, si han de passar per sota de l'arc de seguretat d'un jutjat).

Solid State Drive

Una **unitat d'estat sòlid** (SSD o *Solid State Drive*) és un dispositiu d'emmagatzematge de dades que utilitza una memòria per a emmagatzemar dades, en lloc dels plats giratoris que es troben als discs durs convencionals. Tècnicament no són discs durs, tot i que sovint els anomenen d'aquesta manera.

1.6.2 Amenaces lògiques

En aquest apartat considerem tots aquells programaris que, amb independència de la voluntat amb què van ser creats, poden produir danys en un sistema informàtic. Es poden classificar de la manera següent:

- **Virus**. És una seqüència de codi que s'insereix en un fitxer executable (anomenat amfitrió o *host*). El virus no es pot executar per si mateix (no és un programa independent), de manera que necessita l'amfitrió per executar-se i, quan ho fa, normalment replica el codi viral (o una modificació) en altres programes, que van estenent la infecció arreu. És, per tant, molt semblant a un virus biològic, del qual en rep el nom.

- **Cuc** (*worm*). La principal característica dels cucs és la seva capacitat de duplicació i difusió a través de la xarxa. Poden ser relativament inofensius i només consumir, per exemple, molta amplada de banda de la xarxa, però també es poden programar per produir danys, com per exemple, llançar un atac de denegació de servei (*denial of service* o DoS) o instal·lar un virus en el sistema atacat.

- **Cavall de Troia**. Programari que, aparentment, realitza una tasca útil per l'usuari, però que en realitat realitza altres funcions que van en detriment del sistema afectat, com ara donar el control remot del sistema a un usuari no autoritzat o enviar dades a l'exterior. A diferència dels virus, les activitats dels quals solen ser ben visibles per l'usuari, els cavalls de Troia solen romandre inadvertits. Es basen en una estructura client-servidor i en moltes

ocasions s'instal·len amb tècniques d'enginyeria social o es descarreguen d'Internet, camuflats com a aplicacions útils.

- **Codi maliciós** (*malware*). És el nom genèric que designa tots aquells programes que poden provocar efectes nocius en el sistema informàtic que els allotja. El nom prové de l'abreviació de les paraules angleses (*malicious software*). Els virus, cucs i cavalls de Troia són exemples típics de codis maliciosos.

- ***Exploit***. Programa maliciós que aprofita una vulnerabilitat (coneguda o no) d'un programa informàtic, conseqüència d'un error de programació. No existeix un *exploit* general, sinó que cada programari, a causa dels gairebé inevitables errors de programació, té les seves peculiars vulnerabilitats, les quals poden ser hàbilment aprofitades o explotades pels programadors experimentats (si bé a Internet es poden trobar *exploits* per violar la seguretat de tota mena d'aplicacions i sistemes operatius sense necessitat de tenir coneixements de programació).

- **Bomba lògica**. Tipus de *malware* similar als cavalls de Troia caracteritzat per activar-se, amb efectes nocius per al sistema afectat, en certes condicions (per exemple, en una data determinada).

- **Porta del darrere** (*backdoor*). Codi en un programa que permet, a qui en coneix l'existència i funcionament, evitar els mecanismes d'autenticació (per exemple, existia el rumor que el conegut programari de xifratge PGP tenia un *backdoor*). Pot permetre l'accés remot il·lícit a un sistema informàtic.

- **Programa espia** (*spyware*). Programa que recull informació sobre els hàbits dels usuaris sense el seu consentiment. Aquesta recaptació es pot dur a terme amb finalitat publicitària o per obtenir informació personal per a qualsevol ús.

- **Programari de publicitat** (*adware*). Programari que mostra publicitat. Per exemple, les versions de demostració d'alguns programes poden ensenyar publicitat diversa (d'aquí ve que siguin gratuïtes o de demostració).

- **Falsa alarma** (*hoax*). Missatge que es difon per mitjà del correu electrònic en el qual s'adverteix de l'existència (falsa) de virus o *malware* similar en el sistema. Per exemple, rebem un correu en què se'ns demana que esborrem un fitxer del nostre sistema perquè és un virus molt perillós. En realitat, aquest presumpte nom de virus podria correspondre a un arxiu necessari pel bon funcionament del sistema operatiu, per la qual cosa la seva eliminació podria produir danys importants en el sistema.

- **Enregistrador de teclat** (*keylogger*). Captura les pulsacions del teclat de l'ordinador infectat. Es pot utilitzar, per exemple, per obtenir informació d'accés a un compte bancari.

- **Eina d'intrusió** (*rootkit*). El terme prové d'unir la paraula anglesa "root" (nom assignat a Unix al compte de màxims privilegis) i "kit" (que significa conjunt d'eines o programes). És una eina informàtica, normalment

emprada amb finalitats malicioses (com ara l'obtenció d'informació), que permet l'accés al sistema per part d'un atacant remot. Fa servir tècniques per ocultar la seva presència i la d'altres processos que puguin estar realitzant accions malicioses sobre el sistema. Els *rootkits* poden atorgar privilegis d'administrador a l'atacant i, per tant, són molt perillosos perquè li cedeixen el control del sistema.

Existeixen molts tipus d'*exploits*: *buffer overflow*,*race condition*, *cross-site scripting*, *SQL injection*...

1.7 Anàlisi forense en sistemes informàtics

La generalització de l'ús de les tecnologies de la informació ha incrementat el valor de la informació digital, la qual cosa ha generat, al seu temps, la necessitat de protegir-la davant d'atacs malintencionats o atribuïbles al desconeixement d'aquestes noves tecnologies. En qualsevol cas, les empremtes que podrien revelar la realització d'un fet determinat (amb independència de si és o no constitutiu de delicte) es troben emmagatzemades en suports digitals i s'anomenen genèricament evidències digitals.

Definició d'evidència

En la comissió d'una conducta delictiva, s'anomena evidència a tot aquell element que proporciona informació que condueix a alguna conclusió relacionada amb el fet que s'investiga.

L'evidència digital presenta, bàsicament, les propietats següents:

- Es pot modificar o eliminar fàcilment.
- És possible obtenir una còpia exacta d'un fitxer sense deixar cap empremta d'aquesta acció.
- L'obtenció de l'evidència digital pot suposar l'alteració dels suports digitals originals.

Fragilitat de l'evidència digital

Encara que obrim un fitxer de text per veure'n el contingut i no hi fem cap modificació, l'atribut de darrer accés al fitxer s'actualitza amb la data i hora en què s'ha efectuat aquesta operació.

L'anàlisi forense informàtic va aparèixer a causa de la necessitat d'aportar elements rellevants en els processos judicials en què les noves tecnologies de la informació hi tenien un paper destacat, ja fos com a objecte final (per exemple, una intrusió amb danys en un sistema informàtic) o com a mitjà (per exemple, l'enviament d'amenaces per correu electrònic a un personatge públic). La finalitat d'aquesta anàlisi, en qualsevol cas, segueix la clàssica línia argumental policíaca: buscar respondre *què*, *quan*, *on*, *qui*, *com* i *per què*.

Preguntes clau:

- *Què* s'ha comès?
- *Quan* ha passat?
- *On* s'ha comès?
- *Qui* ho ha comès?
- *Com* s'ha dut a terme?
- *Per què* s'ha comès?

Més precisament, es podria definir l'anàlisi forense informàtica com el procés d'aplicar el mètode científic als sistemes informàtics amb la finalitat d'**identificar, recollir, adquirir, preservar i analitzar** l'evidència digital, de manera que sigui acceptada en un procés judicial.

L'estàndard **ISO/IEC 27037** defineix aquestes etapes, tot i que hi ha bibliografia diversa en què les etapes difereixen de les indicades en aquest text.

Naturalment, la informàtica forense va més enllà dels processos judicials i, en moltes ocasions, els informes elaborats pels experts analistes no tindran com a objectiu final la seva presentació davant dels tribunals, sinó que romandran en l'àmbit de l'empresa privada (aprenentatge, auditoria...). No obstant això, el cas judicial és el més restrictiu i el que més mesures de preservació exigeix, per la qual cosa pot ser extensible a qualsevol tipus d'anàlisi informàtica.

1.7.1 Assegurament de l'evidència digital

La fase d'identificació conté una sèrie d'**accions prèvies** que, al més pur estil policial, permeten **protegir l'escena de l'incident**, de manera similar a com caldria protegir l'escena d'un crim. Les recomanacions següents permeten preservar l'evidència digital i facilitar-ne l'anàlisi:

- Identificar l'escena on s'ha produït el fet i establir un perímetre de seguretat.
- Realitzar una llista amb els equips involucrats en el succés.
- Restringir l'accés de persones i equipaments informàtics a l'interior del perímetre.
- Fotografiar o enregistrar en vídeo l'escena del succés També pot ser útil representar esquemàticament la topografia de la xarxa d'ordinadors.
- Desconnectar les connexions de xarxa.
- Comprovar i desconnectar les connexions sense fils, ja que podrien permetre connexions remotes als equips objecte d'investigació.
- Si hi ha impressores en funcionament, permetre que acabin la impressió.
- Anotar la data i hora del sistema abans d'apagar-lo. Aquestes dades també es poden fotografiar o enregistrar en vídeo.
- Etiquetar cables i components. Cal tenir present que alguns dispositius requereixen d'un cablatge específic, sense el qual no serà possible analitzar l'aparell en el laboratori, ja que no es podrà posar en funcionament.

1.7.2 Identificació de l'evidència digital

S'anomena *identificació de l'evidència digital* al **procés d'identificació i localització de les evidències** que s'han de recollir per ser analitzades posteriorment. Hi

ha fonts d'evidència digital que ens resulten evidents, com per exemple, un disc dur, però n'hi ha d'altres que no ho són tant: càmeres de vídeo, enregistradors de veu o de vídeo (càmeres de seguretat), dispositius GPS, impressores (moltes ja contenen discs durs, susceptibles d'ésser analitzats), telèfons mòbils...

A més, el procés d'identificació no és tan trivial com pot semblar a primera vista, ja que tot sovint l'expert es trobarà configuracions de sistemes complexos amb molts dispositius (cas de locutoris o empreses, per exemple) o, simplement, usuaris que guarden molts suports susceptibles de ser analitzats (per exemple, un particular addicte a emmagatzemar qualsevol programari descarregat d'Internet en milers de CD i DVD). En conseqüència, l'analista haurà de trobar una solució de compromís entre la qualitat de les evidències que pugui obtenir, el valor de la prova i el temps de què disposa per recollir-les.

En primer lloc, l'expert haurà d'identificar el sistema informàtic (un únic PC, una xarxa local, un sistema IBM AS/400, un RAID...) amb la finalitat de saber on es poden trobar les evidències digitals que poden ser d'utilitat per a l'anàlisi. Aquestes poden estar en ordinadors locals, en suports com CD, DVD o dispositius USB, en servidors remots i fins i tot en la memòria RAM dels equips en funcionament. Aquest darrer tipus d'evidències, les **volàtils** (en essència, aquelles que desapareixen en absència d'alimentació elèctrica), són les que haurà d'intentar preservar en primera instància.

El contingut de la RAM pot ser d'interès per esbrinar la contrasenya d'un fitxer determinat (s'hi emmagatzema en text en clar).

En aquesta primera instància també convindrà valorar la possibilitat de realitzar una **anàlisi in situ** a la recerca d'evidències que d'altra forma es perdrien en aturar el sistema (per exemple, els processos en execució). No obstant això, cal tenir present que aquesta mena d'anàlisi pot comportar la pèrdua d'altres evidències, així com la invalidació de la prova en un procediment judicial, ja que l'anàlisi in situ implica la manipulació del dispositiu original, i si no es fa amb les eines forenses adients es pot alterar l'evidència.

La manipulació de l'evidència en el lloc dels fets se sol realitzar en presència de terceres parts, normalment notaris o secretaris judicials.

1.7.3 Recollida de les evidències digitals

En la fase de recollida de les evidències digitals es produeix la recollida dels dispositius físics (de la seva localització original) que poden contenir l'evidència digital, documentant tots els dispositius recollits i els passos realitzats. L'evidència digital pot ser fàcilment destruïda si la recollida no s'efectua amb prou cura.

Recollida d'ordinadors en funcionament

En general, la manera més segura d'actuar pel que fa a un ordinador en funcionament és **desendollar el cable de corrent**. No obstant això, si l'evidència que cerquem es troba visible a la pantalla de l'ordinador (per exemple, un document de text amb contingut rellevant) o pot estar en la memòria (processos en execució, connexions de xarxa actives, contingut de la memòria RAM...), cal mantenir l'ordinador en funcionament i documentar (fotografiar la pantalla, per exemple) o obtenir les evidències (extreure la memòria RAM, per exemple).

El protocol de recollida d'altres dispositius com, per exemple, telèfons mòbils pot diferir del protocol aplicat als ordinadors.

Malgrat tot el que hem exposat, en les situacions següents **no seria recomanable desendollar el cable de corrent**:

- Quan hi ha sospites o hi ha activitat en la pantalla que indica que la informació s'està esborrant o sobreescrivint.
- Quan hi ha algun procés que indica que s'està destruint algun dispositiu d'emmagatzematge (format d'un disc dur, execució de programaris d'esborrament segur o *wipe*...).
- Quan sospitem que l'ordinador, quan efectua el procediment d'aturada normal, pot iniciar un script de format de disc dur o similar.

Recollida d'ordinadors apagats

En aquest cas, cal dur a terme les accions següents:

- Documentar i fotografiar l'equip, totes les seves connexions i perifèrics.
- Desendollar el cable de corrent des de la part posterior de l'ordinador. Si es tracta d'un ordinador portàtil, també cal extreure la bateria. Alguns portàtils s'encenen en aixecar la tapa. L'extracció de la bateria evita que el dispositiu es pugui posar en funcionament de manera accidental.
- Desendollar la resta de connexions, tot indicant-les en la documentació adjunta.
- Documentar el model i el número de sèrie de l'ordinador.
- Precintar l'ordinador.

1.7.4 Obtenció i preservació d'evidències digitals

Atesa la facilitat amb la qual les evidències digitals es poden modificar o eliminar, aquesta fase es converteix en la baula més crítica de tot el procediment. És evident que és impossible obtenir una "instantània" completa de tot un sistema informàtic en un moment concret, encara que, sortosament per a l'analista, en la gran majoria d'ocasions les proves determinants es troben emmagatzemades en el sistema de fitxers, el qual continuarà conservant les evidències malgrat la manca d'alimentació elèctrica. A diferència d'altres proves (per exemple, una anàlisi biològica d'ADN), l'evidència digital es pot duplicar o clonar de manera exacta (a nivell de bits), incloent els fitxers ocults, eliminats i no sobreescrits, i fins i tot l'espai dels clústers que queda sense utilitzar a l'hora de desar-hi els fitxers, l'anomenat "'espai desaprofitat" (*file slack*), al qual ens referirem posteriorment, possibles particions ocultes, o l'espai no assignat del disc dur. En virtut d'aquesta característica, i també com a garantia de preservació de la prova, l'analista actuant acabarà realitzant un clon de l'evidència, ja sigui en l'escena del succés o en les dependències del laboratori.

A primera vista resulta temptador ajornar la clonació dels suports informàtics al moment en què aquests arribin al laboratori (ja que és on es podrà fer el procés amb tota mena de garanties i sense presses), però això no sempre és possible. Si, per exemple, les evidències es localitzen en el servidor d'una empresa, no és possible precintar l'equipament perquè aleshores l'empresa hauria d'aturar la seva activitat. En aquests casos és preferible aturar momentàniament l'activitat de l'empresa i obtenir un clon allà mateix, per reprendre tot seguit l'activitat empresarial, o bé realitzar una anàlisi in situ, amb els inconvenients que ja s'han explicat.

Recordem que la mera observació del contingut d'un disc dur pot alterar o eliminar evidències (sobreescriptura de fitxers eliminats, alteració dels atributs de darrer accés dels fitxers...).

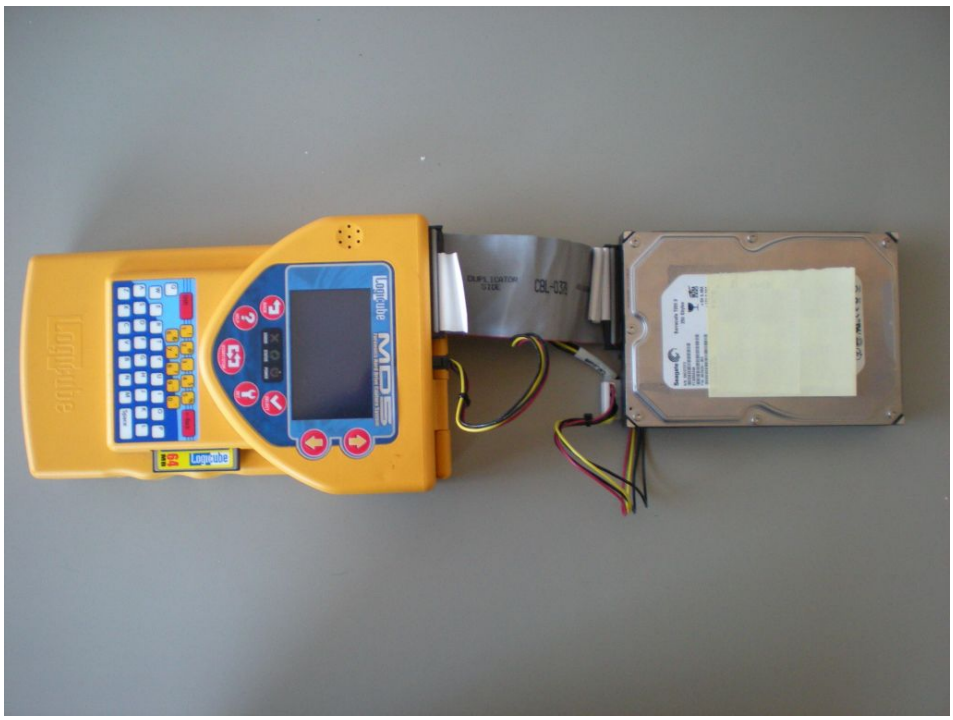
La còpia o clon s'efectuarà, normalment, en dispositius (DVD, discs durs...) aportats per l'analista. L'elecció d'un o altre mitjà (normalment es fa sobre discs durs) dependrà de la quantitat d'informació continguda en els suports originals. Finalment, el programari o maquinari emprat per a l'obtenció del clon calcularà un valor *hash* que haurà de ser el mateix per al disc dur d'origen que per al de destinació, garantint d'aquesta manera que el procés de còpia s'ha fet correctament.

Cada vegada més, les evidències es poden trobar en núvol (per exemple, al servidor de Dropbox) o en altres elements de la xarxa.

La clonació es pot fer amb programes específics (Linen, l'ordre ***dd*** d'Unix...), tot i que també hi ha dispositius de maquinari que la poden realitzar, com per exemple, el que mostra la figura 1.9.

Recordeu la definició de la funció *hash* de l'apartat "Criptografia i funcions *hash*", d'aquesta mateixa unitat.

Figura 1.9. Dispositiu de clonació



La imatge mostra un dispositiu de clonació: el disc dur de destinació es col·loca dins de l'aparell, mentre que el disc dur original és que el podem veure a l'exterior. El disc dur de destinació ha d'haver estat esborrat mitjançant procediments d'esborrament segur (*wipe*) per evitar que pugui contenir informació latent d'altres casos anteriors, o bé ha de ser un disc dur nou, específicament comprat per a l'ocasió.

Una vegada obtingut el clon, el suport original romandrà precintat i protegit, i el clon és el dispositiu que s'analitzarà, mitjançant eines específiques que permetran el seu estudi sense necessitat d'alterar-ne el contingut. Sovint, es genera un segon clon, que és el que realment s'empra per a l'anàlisi, mentre que el primer clon serveix perquè, en cas de necessitat, es pugui generar un nou clon idèntic a l'original. Sovint, el suport original es manté protegit i precintat en dipòsit (per exemple, en seu judicial), d'on es podrà reclamar en cas que es desitgi efectuar una prova contrapericial.

A més de l'adquisició de l'evidència, en aquesta etapa també cal documentar qui ha preservat l'evidència, on i com s'ha fet i quan. Tot seguit cal empaquetar les evidències, identificant-les de manera inequívoca. Aquest procés es duu a terme embalant els paquets amb material protector que protegeixi les evidències de cops, pluja o qualsevol altre element que les pugui malmetre. Aquesta fase acabarà amb el transport de les evidències a un lloc segur o a les dependències del laboratori on hagin de ser analitzades. L'embalatge i el transport de les evidències és l'inici de la denominada **cadena de custòdia**, la qual permet garantir la integritat de les proves, des de la seva obtenció fins a la seva disposició a l'autoritat judicial o al laboratori on hagin de ser analitzades. La documentació de la cadena de custòdia permet saber en qualsevol moment del procés on han estat emmagatzemades les evidències i qui hi ha tingut accés.

1.7.5 Anàlisi de les evidències digitals

En aquesta fase, l'expert haurà de respondre les preguntes "policials" introduïdes a l'inici d'aquest capítol. Aquest estudi es fonamenta, sobretot, en l'anàlisi del contingut dels fitxers (***dades***) i de la informació sobre aquests fitxers (***metadades***).

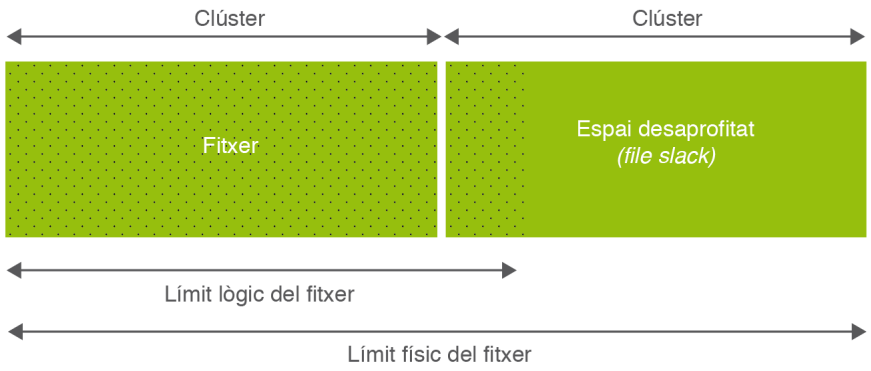
Un exemple de metadada podria ser, per exemple, el camp "Autor" d'un fitxer DOC.

Normalment no es fan anàlisis exhaustives dels suports objecte d'interès (seria una tasca inabastable), sinó que els informes pericials es limiten a respondre aquells extrems plantejats en l'anàlisi.

Bàsicament hi ha quatre categories diferents de dades susceptibles de ser analitzades:

- **Dades lògicament accessibles.** Són les dades contingudes en fitxers directament accessibles. Aquesta anàlisi pot ser complicada a causa de la dificultat de discriminar la informació rellevant entre molts milers de fitxers, o, entre altres raons, a causa de l'existència de fitxers xifrats.
- **Dades situades en l'anomenat *ambient data***. És a dir, aquelles dades que apareixen en localitzacions no directament visibles i que requereixen l'ús de programes específics per ser recuperades. Un bon exemple d'aquest tipus de dades és la informació residual que es pot trobar en clústers no assignats a cap fitxer, o aquella informació localitzada en l'espai desaprofitat del darrer clúster assignat a un fitxer (*file slack*), és a dir, l'espai entre el final lògic i el final físic d'un fitxer. Vegeu la figura 1.10.

FIGURA 1.10. Representació gràfica de l'espai desaprofitat (file slack)



- **Dades que han estat esborrades o eliminades**, però que encara no han estat sobreescrites per altres fitxers i que, per tant, són susceptibles de ser recuperades.

Per fer l'anàlisi de les evidències es poden emprar diverses eines. Una de les més conegudes és possiblement Encase, de codi propietari, que abasta, amb una interfície molt amigable, totes les fases de l'anàlisi forense, des de l'adquisició dels suports originals i l'anàlisi fins a la generació automàtica de l'informe final. Una altra eina molt coneguda és l'eina de font pública The Sleuth Kit (TSK), i el seu frontal web gràfic Autopsy.

The Sleuth Kit i Autopsy es poden trobar en moltes distribucions forenses gratuïtes, com Caine, DEFT o Backtrack, per exemple.

1.7.6 Presentació i informe

En l'informe elaborat per l'expert es presentaran les evidències relacionades amb el cas, la justificació del procediment emprat i, el més important, les conclusions. En moltes ocasions, l'informe serà ratificat en presència del jutge o bé serà lliurat a empreses i advocats. No obstant això, en cap cas els destinataris de les anàlisis pericials han de disposar necessàriament de coneixements informàtics per comprendre l'informe en profunditat. Per tant, en general no s'ha d'emprar un llenguatge gaire tècnic i, quan calgui fer-ho, serà necessari afegir notes explicatives a peu de pàgina o redactar glossaris tècnics, que es poden afegir a l'annex de l'informe. En els casos en què els informes hagin de ser defensats davant del jutge, l'analista, a més de tenir rigor tècnic, ha de ser prou hàbil per comunicar el resultat de l'anàlisi de manera concisa i clara.

2. Legislació sobre seguretat, protecció de dades i Codi Penal

La seguretat informàtica es relaciona de forma natural amb aspectes legislatius que, sovint, sorprenen els informàtics. Efectivament, no n'hi ha prou amb el coneixement de les disciplines tècniques, sinó que cal saber que hi ha lleis que protegeixen l'accés a les dades personals dels nostres sistemes (pensem que moltes d'aquestes dades són estrictament confidencials i poden revelar aspectes molt íntims de la nostra personalitat), o bé que ens permeten denunciar als cossos policials els danys que hagi pogut patir el nostre sistema com a conseqüència d'accions nocives que algú hagi pogut produir. També és molt important que, com a informàtics, sapiguem que el desconeixement d'una norma jurídica no ens eximeix de responsabilitat i que no perquè una acció sigui tècnicament possible de fer ha d'estar necessàriament ajustada a la norma jurídica.

2.1 Marc jurídic penal

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. 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.

Definició de delicte

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

2.1.1 El "delicte informàtic"

El delicte informàtic no apareix explícitament definit en l'actual Codi Penal (1995), ni en les reformes posteriors (Llei 15/2003 i Llei 5/2010) que se n'han fet i, per tant, no es pot 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 com a objectiu d'aquesta activitat (per exemple, una intrusió en un sistema informàtic).

Límits tècnics i legals

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

Una **intrusió** és un accés no autoritzat a 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 relacionades amb el sentit comú que amb la normativa complexa que es va generant entorn de l'aplicació de les noves tecnologies.

El vessant tecnològic o científic dels estudis d'informàtica sovint deixa de banda el vessant social de l'aplicació dels avenços en aquestes disciplines. Conseqüentment, els usuaris i tècnics d'un sistema informàtic poden ser molt competents en la seva feina, però és probable que tinguin molts dubtes a l'hora d'abordar situacions com les 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 el lloc 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 d'alguna manera?
- Puc penjar a Internet un lloc web amb les fotografies i logotips del meu grup de música preferit?
- Puc descarregar lliurement qualsevol fitxer de música de la xarxa?

Segurament, cap dels exemples descrits no us suposa cap 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. Així, doncs, haureu de ser 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 situacions, 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.

2.1.2 El Codi Penal i les conductes il·lícites relacionades amb 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 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 espanyola (1978) relacionats amb la pràctica informàtica (tant des del punt de vista tècnic com del simple usuari) és l'article 18, que 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.

Article 18 de la Constitució

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 consultar la Constitució aneu a la secció "Adreces d'interès" del web.

2.1.3 Delictes contra la intimitat

Una part molt important dels delictes relacionats amb la informàtica entra dins de la tipificació de **delictes contra la intimitat**. Sovint, els autors 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. 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 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) i, com a norma general, mai no s'ha de llegir cap correu electrònic que no vagi adreçat a nosaltres (ni tan sols si el nostre cap, dins de l'àmbit laboral, ens ho demana).

En el cas de la intercepció del correu electrònic en l'àmbit empresarial, se sol argumentar que els treballadors no poden fer ús dels mitjans de l'empresa per a qüestions personals. Algunes 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

Les activitats personals abracen, 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. Igualment, una bona estratègia consisteix a emprar noms de comptes de correu corporatiu en lloc de noms personals (per exemple: nom_empresa@proveidor.cat, en lloc de el_meu_nom@proveidor.cat). 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 nombre de bytes transmesos o rebuts per un usuari concret (per exemple, si un usuari descarrega fitxers 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 a 200 del Codi Penal 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 en suports informàtics, electrònics o telemàtics, sempre que aquestes conductes les facin persones no autoritzades Aquestes conductes s'anomenen, 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 el **Reglament General de Protecció de Dades** (RGPD).

Vegeu l'RGPD i una definició més detallada de *dada personal* en l'apartat "Marc jurídic extrapenal" d'aquesta unitat.

El Codi Penal considera un agreujant que l'objecte del delicte siguin dades de caràcter personal que revelin ideologia, religió, creences, salut, origen racial o vida sexual. Altres circumstàncies agreujants són que la víctima sigui un menor d'edat o incapacitat o que la persona que comet el delicte sigui 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 del Codi Penal**
>
> 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.

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

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 que tenim l'obligació de mantenir el secret i que no podem cedir a ningú.

Podeu consultar el Codi Penal en la secció "Adreces d'interès" del web.

Delicte d'intrusió

A la modificació de l'any 2010 es va incloure en el Codi Penal el delicte d'intrusió, és a dir, l'accés no autoritzat a un sistema informàtic (siguin dades o programes).

Cal dir que si bé fins a aquella data la intrusió no era constitutiva de delicte, aquests tipus d'accions se solen trobar vinculades a altres conductes que sí que ho eren (i ho continuen essent), com, per exemple, els danys en un sistema informàtic o els mitjans que s'hagin utilitzat per dur a terme l'accés no autoritzat.

Arran d'aquesta modificació del Codi Penal (apartat 3 de l'article 197), la intrusió directa, encara que no provoqui danys, i encara que no "trenqui" o descobreixi cap contrasenya d'accés, pot ser considerada una conducta constitutiva de delicte.

És interessant observar que, tot i que, com ja s'ha dit, el "delicte informàtic" no es troba definit en el Codi Penal, la intrusió en un sistema informàtic pot ser considerada com a tal, a causa de la seva especificitat i a la desvinculació de la resta de conductes il·lícites contingudes en el Codi Penal.

2.1.4 Delicte de frau informàtic

En l'article 248.2 del Codi Penal es castiga la conducta de qui, emprant qualsevol mètode informàtic, 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 ser, a tall d'exemple, la fabricació, la facilitació o simplement la mera possessió de programes específics destinats a la comissió del delicte de frau informàtic.

Per exemple, el **descaminament** (*pharming*) és una de les tècniques que es poden englobar dins d'aquesta tipificació. Aquesta tècnica permet que un atacant pugui redirigir un nom de domini a una màquina diferent. Així, 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 descaminament està molt relacionat amb un altre delicte, la **pesca electrònica** (*phishing*). En aquest darrer cas, però, no estarem parlant d'una tècnica informàtica, sinó d'una estratègia d'enginyeria social que usa la suplantació de correus electrònics o llocs web per obtenir 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 ho fa en un portal diferent, amb una adreça diferent de la real. En el cas del desencaminament, en canvi, l'usuari introdueix l'adreça real del portal d'Internet, però es produeix una redirecció a una màquina diferent.

Definició d'enginyeria social

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 del Codi Penal, aquesta acció es pot assimilar a un delicte de falsificació de moneda.

2.1.5 Delicte de danys

Els delictes de danys, juntament amb els delictes contra la intimitat i contra la propietat intel·lectual, són, amb diferència, els més freqüents. Com passa amb els delictes contra la intimitat de les persones, sovint els autors d'aquestes accions no són conscients de les conseqüències que poden comportar els seus actes.

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

Arran de la modificació del Codi Penal de l'any 2010, aquest delicte també inclou els **atacs de denegació de servei** (DoS). Així, doncs, l'obstaculització o interrupció del funcionament d'un sistema informàtic o fer inaccessibles dades informàtiques de manera no autoritzada són conductes recollides en el Codi Penal.

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

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

Alguns danys produïts en un sistema informàtic es poden valorar. És essencial, en aquest cas, 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 abastar diferents aspectes: cost de restauració d'un lloc web, pèrdues en conceptes de publicitat no emesa (**lucre cessant**), o per serveis que no s'han pogut prestar... A tall d'exemple, l'alteració d'una pàgina web (*defacement*) 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 divertida, des del punt de vista dels pirates), pot comportar pèrdues de milers d'euros.

2.1.6 Delictes contra la propietat intel·lectual

El delicte contra la propietat intel·lectual és una de les qüestions que més interès suscita en 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 propietat intel·lectual i l'ús de programaris d'intercanvis de fitxers en xarxes d'igual a igual (anomenades també P2P o *peer-to-peer*).

Xarxes d'igual a igual

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 usuaris, els continguts dels quals poden ser (o no) protegits per les lleis de propietat intel·lectual. Sens dubte, el programari P2P més conegut (i objecte de molta controvèrsia) és l'**eMule**, basat en la xarxa **eDonkey** (2002).

Segons l'**article 270 del Codi Penal**, 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) està protegida per uns drets de propietat intel·lectual que cal respectar.

Permís dels titulars

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

Exemples de delictes contra la propietat intel·lectual

Els delictes contra la propietat intel·lectual es poden produir de manera molt diversa, tal com es pot veure en els exemples següents:

- Reproducció íntegra de programes i venda al marge dels drets de llicència.
- Instal·lació de còpies no autoritzades de programes en un ordinador en el moment de la compra.
- Publicació del codi font de programes (o el programa mateix), o altres fitxers (MP3, llibres...) a Internet, al marge dels drets de llicència d'aquestes obres.
- Utilització d'una llicència de programa per a només un sol ordinador per donar servei a tota la xarxa.
- Trencament dels mecanismes de protecció que permeten el funcionament correcte del programa (motxilles o *dongles*, contrasenyes i altres elements de seguretat). Aquestes tècniques reben el nom genèric de *cracking*. Així, el terme *cracker* es refereix 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 programes.

El mateix article 270 del Codi Penal 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 programes que permeten "saltar" les proteccions anticòpia de CD o DVD).

Llicència de programari

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

Tot i els esforços d'alguns països de la Unió 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 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 programa) dissenyat per anul·lar la protecció de programes sí que és susceptible de ser sancionada.

Pel que fa a la **creació de programari**, també cal fer algunes consideracions. Segons el tipus de contracte al qual es trobi subjecte el treballador, el programari que desenvolupi per a una organització determinada 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.

La còpia privada

És un límit al dret de reproducció d'una obra que posseeixen els titulars dels drets de propietat intel·lectual de l'esmentada obra, és a dir, les persones que les han accedit legalment. Aquest límit no permet que la còpia obtinguda es pugui emprar de manera col·lectiva o bé amb ànim de lucre.

Per pal·liar el perjudici econòmic que origina la còpia privada, s'ha creat una compensació (anomenat **cànon per còpia privada** o **cànon digital**) que han d'assumir els fabricants i els importadors d'equips i suports de reproducció d'obres.

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 s'hi val a argumentar el desconeixement com a eximent.

Llicències de programari no lliure
Amb la finalitat d'emprar adequadament les llicències caldrà estudiar de quins tipus n'hi ha per poder-les adquirir segons les nostres necessitats i el pressupost de què disposem. Vegem-ne algunes:

- **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 programa com a part integrant d'un equip informàtic nou (programari preinstal·lat). Així, doncs, aquest programari no es pot vendre aïlladament, sinó juntament amb el maquinari que l'incorpora. Solen no disposar de l'embalatge de la versió normalitzada del producte. No es poden vendre ni cedir a tercers separats del maquinari.
- ***Retail***. Consisteix en les versions de venda normalitzades d'un programari, amb els embalatges que se solen veure a les botigues d'informàtica. A diferència de les versions OEM, es poden vendre independentment del maquinari on s'integren 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.

Llicències de programari lliure

Segons la Free Software Foundation (fundació pel programari lliure), el programari lliure ha de complir les quatre condicions següents:

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

Free Software Foundation

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.

En resum, 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 millores que permetin als futurs usuaris gaudir de les mateixes llibertats a què hem fet referència.

Notem que, si bé el tema de les llicències de programari no està recollida al Codi Penal, és una qüestió de l'àmbit informàtic relacionada amb els drets d'autor, i per això la tractem.

Programari descatalogat (abandonware)

El programari descatalogat sol ser programari antic, els drets d'autor del qual han caducat. Es pot trobar a la xarxa en webs dedicats i no té cap altra via de distribució.

El fet que un programari sigui lliure no vol pas dir que sigui **gratuït**. Per exemple, el programari gratuït pot tenir certes restriccions que fan que no s'adapti a la definició de programari lliure (un programari pot ser gratuït, però podria no incloure el codi font, tal com estableix la definició de programari lliure). D'altra banda, sovint trobem a la venda CD de **distribucions de Linux** (programari lliure). En aquest cas, però, el comprador pot copiar el CD i distribuir-lo.

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 (comercial o no) i la modificació, però amb la condició que totes les versions modificades del programari es continuïn mantenint sota els termes més restrictius de la llicència GNU GPL. Això implica que si un programa té parts amb llicència no GPL, el programa final ha de tenir forçosament llicència GPL.

Projecte GNU (GNU is Not Unix)

El projecte GNU va ser iniciat per Richard Stallman amb l'objectiu de crear un sistema operatiu totalment lliure, anomenat sistema GNU. El projecte es va iniciar l'any 1983.

L'any 1991 Linus Torvalds va començar a escriure el nucli del sistema operatiu Linux, que va distribuir amb llicència 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 és un sistema operatiu derivat de l'Unix creat 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 (encara que el codi font modificat o copiat amb MPL ha de mantenir aquest tipus de llicència). 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 endogàmica a causa de l'obligació que el producte final fos també llicenciat en GPL. Aquestes llicències són més restrictives que les BSD i, en definitiva, es poden considerar a mig camí entre aquestes i les GPL.

- **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 amb qualsevol de les llicències estudiades, sense que això afecti les llicències *copyleft* ja atorgades. L'autor també pot retirar una llicència *copyleft*, però sense efectes retroactius, ja que l'autor no té dret a retirar el permís d'una llicència que encara es troba vigent. Es pot aplicar no només a programes, sinó a tota mena de creacions artístiques (música, vídeo...).

2.1.7 Delicte de revelació de secrets d'empresa

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

Segons l'article 278.1 del Codi Penal, fa **revelació de secrets d'empresa** qui, amb la finalitat de descobrir un secret d'empresa, intercepti qualsevol tipus de telecomunicació o utilitzi artificis tècnic d'escolta, transmissió, gravació o enregistrament de so, imatge o qualsevol altre senyal de comunicació. Notem la semblança que hi ha entre aquest forma de delicte i els delictes contra la intimitat.

2.1.8 Altres delictes i la investigació dels delictes informàtics

A més dels delictes que s'han descrit, és evident que n'hi ha molts més, 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". Ens referim, entre d'altres, a aquests:

- Amenaces i coaccions (per mitjà de xats o correus electrònics).
- Falsedat documental: alteracions i simulacions de documents públics o privats.
- Tinença i difusió de pornografia infantil a Internet.
- Defraudació dels interessos econòmics dels prestadors de serveis: facilitació a tercers de l'accés a serveis interactius o audiovisuals (com, per exemple, els canals de televisió de pagament), sense el permís dels prestadors d'aquests serveis.

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

- **Els fitxers o registres locals**. Els sistemes operatius i els programaris que s'executen en els 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 deixa, si l'atacant no és gaire hàbil, empremtes en diversos fitxers del sistema. La informació que contenen aquests fitxers (per exemple, l'adreça IP de l'atacant) és la primera baula que els investigadors analitzen per arribar a establir l'origen de l'atac.
- **Els registres 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 conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions** (com a màxim 12 mesos, a partir de la data de comunicació de reserva, encara que es pot ampliar o reduir), les quals només poden ser cedides als investigadors per ordre judicial. Així, doncs, un cop que 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 una ordre perquè 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 investigació) per continuar el procés i identificar l'usuari que ha emprat la connexió sospitosa.

Proveïdor de serveis (PSI)

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 la Llei de serveis de la societat de la informació (LSSI) en l'apartat "Marc jurídic extrapenal", d'aquesta mateixa unitat (subapartat "Legislació sobre els serveis de la societat de la informació, comerç i el correu electrònic").

Si l'administrador d'un sistema informàtic és víctima de qualsevol d'aquests delictes o descobreix, per exemple, que el sistema que administra és utilitzat

com a plataforma de distribució de còpies de programari no autoritzades, ho ha de denunciar immediatament a la comissaria de policia més pròxima, tenint en compte el protocol d'actuació següent:

1. Adjuntar els fitxers de registre (registres locals del sistema) relacionats amb el delicte comès. Aquests fitxers han de reflectir, en cas que hagin quedat registrats, la IP de l'atacant i les accions produïdes en el sistema investigat.
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...). Moltes de les aplicacions amb 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.

2.2 Marc jurídic extrapenal

La Constitució vol protegir d'una manera molt curosa una sèrie de drets inherents a tota persona: els anomenats **drets fonamentals**. Entre aquests destaca el **dret a la intimitat**. A més de les conseqüències penals que pot comportar la vulneració d'aquest dret, hi ha altres lleis que protegeixen la privacitat de la persona, 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...).

La legislació té molta cura de la protecció de les dades perquè contenen informació personal que ha d'ésser protegida adequadament. Això afecta de manera negativa els sistemes informàtics, la gestió de 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: un nivell de seguretat de les dades adequat, juntament amb una protecció suficient de la intimitat, i permetre a les empreses operar amb la informació de manera eficient.

2.2.1 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 són més conscients de la protecció de què ha de gaudir la seva informació personal.

La situació actual és producte, d'una banda, de la normativa en matèria de protecció de dades i, de l'altra, de 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).

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

Veurem a continuació com han anat evolucionant les lleis; la primera en aparèixer va ser la **Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD)**. Aquesta norma tenia per objecte garantir i protegir, en relació amb el tractament de dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i en especial el seu honor, intimitat i privacitat. La LOPD va crear els anomenats drets ARCO:

Agències autonòmiques

A data d'avui no totes les comunitats autònomes han creat les seves agències de protecció de dades. Catalunya sí que en té: és l'Agència Catalana de Protecció de Dades, consulteu la secció "Adreces d'interès" del web.

- Dret d'**Accés**: Reconeix als ciutadans la potestat de defensar la seva privacitat controlant per si mateixos l'ús que es fa de les seves dades personals.
- Drets de **Rectificació** : La LOPD també regula els drets de rectificació i cancel·lació: quan les dades personals d'un ciutadà resulten ser incompletes, inexactes, excessives o inadequades aquest pot requerir al responsable del fitxer la seva rectificació o cancel·lació.
- Dret de **Cancel·lació**: El ciutadà pot exigir al responsable del fitxer la supressió de dades que consideri inadequades o excessives.
- Dret d'**Oposició**: Consisteix en el dret dels titulars de les dades per dirigir-se al responsable del fitxer perquè deixi de tractar les seves dades sense el seu consentiment per a fins de publicitat o prospecció comercial.

Posteriorment, amb el desenvolupament i popularització d'Internet i l'aparició de comerços online va aparèixer al 2002 la llei de serveis de la societat de la informació i comerç electrònic, coneguda per les seves sigles com LSSI.

Al 2003 apareix la llei de la firma electrònica per regular els certificats digitals i donar validesa jurídica a aquesta firma. Al 2003 també s'aprova el Reglament que desenvolupa la llei de protecció de dades de caràcter personal de 1999. El 2007 s'aprova la llei de conservació de dades a les comunicacions electròniques i a les xarxes públiques de comunicacions.

El 27 d'abril de 2016 s'aprova el **el Reglament General de Protecció de dades (RGPD)**, que no va entrar en vigor fins al Maig del 2018, per donar un marc Europeu. Aquest reglament, entre altres coses, amplia els drets ARCO.

El 5 de desembre de 2018 s'aprova la llei orgànica 3/2018, **Protecció de Dades Personals i Garanties dels Drets Digitals** (LOPDGD), que adapta l'RGPD a la normativa espanyola. Amb LOPDGD i l'RGPD es deroga l'antiga LOPD.

A continuació teniu un llistat d'aquestes lleis :

- Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD).
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic (LSSICE) o, habitualment (LSSI).
- Llei 59/2003, de 19 de desembre, de firma electrònica.
- Llei Orgànica 15/2003, de 25 de novembre, per la qual es modifica la Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal.
- Reial Decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a las comunicacions electròniques i a les xarxes públiques de comunicacions.
- Llei Orgànica 5/2010, de 22 de juny, per la qual es modifica la Llei Orgànica. 10/1995, de 23 de novembre, del Codi Penal.
- Reglament General de Protecció de dades (RGPD) del 27 d'Abril de 2016.
- Llei orgànica 3/2018 Protecció de Dades Personals i Garanties dels Drets Digitals (LOPDGD) del 5 de desembre de 2018.

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

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

El Reglament General de Protecció de dades (RGPD)

Aquest reglament és una norma d'àmbit europeu que protegeix les dades personals de tots els residents a la Unió Europea i garanteix el flux de dades entre els països de la Unió Europea. Per tant, els països necessiten **integrar** aquest reglament a les seves legislacions.

Aquest reglament estableix l'obligació de les organitzacions d'adoptar mesures destinades a garantir la protecció d'aquestes dades que afecten sistemes informàtics, fitxers, suports d'emmagatzematge, demanar el consentiment per usar

les dades de caràcter personal i procediments operatius. Aquestes mesures han d'adoptar-les totes les organitzacions que operen amb residents a la Unió Europea, encara que no hi tinguin la seva seu.

En el Capítol 7 d'aquest reglament es crea el Comitè Europeu de protecció de dades per supervisar el Reglament i la seva aplicació als diferents països d'Europa. En el Capítol 11, *Disposicions finals*, s'estableix com a màxim el 25 de maig del 2020 per fer una primera avaluació i revisió del reglament per tal d'anar-lo actualitzant als nous temps. Posteriorment, aquesta revisió es repetirà cada 4 anys.

Els fitxers que han de satisfer mesures de seguretat no són tan sols aquells als quals es pot accedir a Internet, sinó tots els que continguin dades personals.

L'RGPD és aplicable a qualsevol informació sobre persones físiques identificades o identificables (nom i cognoms, edat, sexe, dades d'identificació fiscal, estat civil, professió, domicili, dades biomètriques...) enregistrada en qualsevol suport físic (inclòs el paper), que en permeti el tractament manual o automatitzat i ús posterior pel sector públic o privat. Traspassat a l'àmbit de les empreses, s'ha d'interpretar que l'RGPD 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 treballadors com dels seus clients o proveïdors (persones físiques), la qual cosa obliga les empreses, institucions, professionals i, en general, totes les persones jurídiques o físiques que operin amb fitxers de dades de caràcter personal, al compliment d'una sèrie d'obligacions legals. Cal tenir present, però, que al considerand 18, diu: "El reglament no s'aplica al tractament de dades de caràcter personal dut a terme per una persona física en el curs d'una activitat exclusivament personal o domèstica, és a dir sense cap connexió amb una activitat professional o comercial".

Què és una dada de caràcter personal?

Segons el Reglament General de Protecció de dades (RGPD), una dada de caràcter personal és "qualsevol informació sobre una persona física identificada o identificable (l'interessat)".

Per **tractament** s'entén "qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció".

Objectiu del reglament i principis bàsics de l'RGPD

El parlament Europeu i el Consell de la Unió Europea, a partir del Tractat de funcionament de la Unió Europea, en concret de l'article 16, i d'una proposta de la Comissió Europea, van enviar una proposta del text legislatiu als parlaments nacionals, per posteriorment elaborar dos dictàmens. L'RGPD considera que la protecció del tractament de les dades personals és un dret fonamental, tal i com està a la Carta dels Drets Fonamentals de la Unió Europea a l'article 8, que estableix que qualsevol persona té dret a la protecció de les dades de caràcter personal que l'afecten. Pel que fa al tractament de les dades personals s'han de respectar les llibertats i els drets fonamentals, especialment el dret a la protecció de les dades de caràcter personal, sigui quina sigui la seva nacionalitat o residència.

L'**objectiu de l'RGPD** és, doncs, garantir i protegir la privacitat i la intimitat de les persones físiques. Tal i com queda clar a l'article 1 del RGPD on s'explica l'objecte d'aquest, engloba tres objectes:

1. Establir les normes relatives a la protecció de les persones físiques pel que fa al tractament de les dades personals i les normes relatives a la lliure circulació d'aquestes dades.

2. Protegir els drets i les llibertats fonamentals de les persones físiques i el seu dret a la protecció de les dades personals.

3. Evitar restriccions a la lliure circulació de les dades personals a la Unió Europea originades per les necessitats de protecció de dades.

L'RGPD canvia alguns articles de la LOPD i afegeix noves obligacions per a les empreses.

Els canvis més importants de l'RGPD respecte la LOPD són:

- El principi de **responsabilitat proactiva**. El nou Reglament indica que el responsable del tractament ha d'aplicar mesures apropiades per poder demostrar que el tractament és conforme al Reglament, tal i com aparèix a l'article 5. Les organitzacions han d'analitzar quines dades tracten i amb quines finalitats ho fan i han de mirar quins tipus d'operacions de tractament realitzen per tal d'aplicar les mesures que preveu l'RGPD. Aquestes mesures han de ser les adequades per complir amb el Reglament. També han de poder demostrar el compliment del Reglament davant de tercers. Aquest principi exigeix que el responsable del tractament ha de tenir una actitud proactiva, davant de tots els tractaments de dades que realitzi.

- El principi de l'**enfocament de risc**. El nou Reglament indica que s'ha de tenir en compte el risc per als drets i les llibertats de les persones. Així, algunes de les mesures només s'han d'aplicar quan hi hagi un alt risc per als drets i les llibertats. Les mesures previstes per l'RGPD s'han d'adaptar a les característiques de les organitzacions. El que pot ser bo per a una organització no necessàriament ho ha de ser per a una altra. No és el mateix una organització que utilitza dades de milions de persones, amb tractaments que contenen informació personal sensible o volums importants de dades sobre cada persona, que una petita empresa amb poques dades i que treballa amb dades no sensibles.

A més, manté (ampliats en alguns casos) els següents principis ja recollits a la LOPD:

- **Principi de qualitat de les dades**: les dades de caràcter personal només es poden recollir per al seu tractament i sotmetre's 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. L'RGPD exigeix reduir al mínim necessari tant el tractament de les dades com les persones autoritzades a accedir a aquestes dades.

- **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 s'han recollit. Es consideren compatibles, tanmateix, el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques.

- **Necessitat de consentiment de la persona afectada**: el tractament de les dades requereix el consentiment de la persona afectada.
- **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 se'n 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 voluntarietat 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 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.

A l'RGPD alguns d'aquests drets s'han ampliat:

- El dret de cancel·lació ha passat a denominar-se dret de supressió i té un aspecte molt comentat però adreçat essencialment als navegadors d'internet i xarxes socials: **el dret a l'oblit**.
- El dret al consentiment: L'RGPD requereix que l'interessat presti el consentiment mitjançant una declaració inequívoca o una acció afirmativa clara. Als efectes del nou Reglament, les caselles ja marcades, el consentiment tàcit o la inacció no constitueixen un consentiment vàlid. Igualment, perquè les dades estiguin especialment protegides, és necessari donar el consentiment exprés i per escrit.

També s'han incorporat dos nous drets: limitació del tractament i portabilitat.

- El dret a la limitació del tractament amplia el dret del consentiment; és el dret de l'usuari a posar limitacions als tractaments sobre les seves dades.
- El dret a la portabilitat de les dades inclou, per una banda, que la informació com a resposta al dret d'accés s'ha de proporcionar de manera completa i en format compatible d'ús corrent i, per una altra, que ha de poder-se transmetre a petició de l'interessat en aquest format directament a una altra organització (per exemple, si canviem de proveïdor).

Cancel·lació i bloqueig de dades

És el procediment en virtut del qual el responsable cessa en l'ús de les dades. La cancel·lació implicarà el bloqueig de les dades, que consisteix a identificar-les i reservar-les per impedir-ne el tractament, excepte per posar-les a disposició de les administracions públiques, jutges i tribunals per atendre 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.

És precís informar a les persones afectades per l'ús de les seves dades dels ítems que es llisten a continuació, per tal que puguin exercir pròpiament els drets anteriors:

- La base jurídica del tractament.
- Interessos legítims que es volen assolir.
- Necessitat de donar un consentiment. Aquest s'ha de donar amb un acte afirmatiu clar, específic, informat i inequívoc. Pot realitzar-se en paper o a través de mitjans electrònics.
- Termini de conservació de les dades. Quan aquest venci, el responsable del tractament n'ha de limitar el tractament a través de mitjans tècnics com impedir-hi l'acces als usuaris, trasllat temporal de les dades afectades a un altre sistema de tractament o retirada temporal d'un lloc d'Internet de les dades afectades.
- Dades de contacte amb el delegat de protecció de dades (si n'hi ha).
- Existència del dret a reclamar a una autoritat de control. Això és important, ja que també existeix, en cas de tractament inadequat o negligent, el dret a obtenir una reparació, i si escau una indemnització per part del perjudicat.
- Existència de decisions automatitzades o l'elaboració de perfils (si n'hi ha). L'interessat té dret a oposar-se a que les dades personals que l'afecten siguin objecte d'un tractament, inclosa l'elaboració de perfils. El responsable del tractament ha de deixar de tractar aquestes dades personals, tret que acrediti motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions. L'interessat també té dret a no ser objecte de decisions basades exclusivament en un tractament automatitzat.
- Dret a la informació de l'afectat davant canvis en les seves dades: Si hi ha un canvi de les dades s'ha d'informar del canvi a l'afectat, per tal de que les verifiqui i conegui el canvi.
- Si es transmetran les dades a tercers. Cal tenir present que només s'han de fer transferències de dades personals que es tracten o que es tractaran quan es transfereixin a un tercer país o a una organització internacional si, sens perjudici de la resta de disposicions del RGPD, el responsable i l'encarregat del tractament compleixen les condicions adecuades, incloses les relatives a les transferències posteriors de dades personals des del tercer país o organització internacional a un altre tercer país o una altra organització internacional.

La informació proporcionada en tot moment ha de ser clara i fàcilment intel·ligible: No s'ha de posar lletra petita, ni usar paraules ambígües ni frases complicades o difícils d'entendre.

La LOPDGD tracta, a més, dels drets que s'apliquen al cas de menors i de dades de persones difuntes.

2.2.2 Obligacions de les empreses i els implicats en els tractaments

La necessitat de proporcionar als usuaris els drets recollits per l'RGPD, deriva en una sèrie d'obligacions per a les empreses i persones responsables i encarregades d'efectuar els tractaments, com són:

- Proporcionar procediments senzills per exercitar els drets.
- Disposar de formularis conformes amb l'RGPD i la LOPDGD per informar als usuaris i perquè aquests exerceixin els seus drets.
- Pseudonimització de les dades i les bases de dades.
- Protecció de dades des del disseny i per defecte (article 25 RGPD); això implica tenir en compte les mesures de seguretat abans de l'inici del tractament i quan aquest s'està duent a terme).
- Tenir un registre de les activitats del tractament.
- Poder demostrar davant l'autoritat que es segueix la llei si s'és sol·licitat per aquesta.
- Notificar les violacions de seguretat.

D'altra banda, no és obligatori registrar a l'autoritat de control els fitxers amb dades personals que té l'organització, com passava amb l'anterior LOPD.

Altres obligacions recollides a l'RGPD són:

- En el Capítol 4 apareix l'obligació de xifrar les dades personals, a més de guardar-les amb pseudònims (pseudonimització) per tal de que sigui més difícil d'identificar de qui són les dades.
- En aquest mateix capítol, a l'article 42, s'assenyala que els organismes es podran certificar de forma voluntària.

2.2.3 Notificació de violacions de seguretat

L'article 33 de l'RGPD, *Notificació d'una violació de la seguretat de les dades personals a l'autoritat de control*, diu que el responsable ha de notificar a

l'autoritat de control la violació de seguretat, sense dilació indeguda i, si és possible, en un termini màxim de 72 hores i de conformitat amb l'article 55, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones.

Quan sigui probable que la violació comporti un alt risc per als drets de les persones interessades, el responsable l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill tal i com diu l'article 34, tret que:

- El responsable hagi adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades.
- El responsable hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc.
- Suposi un esforç desproporcionat. En aquest cas, cal optar per una comunicació pública o una mesura semblant.

La notificació de la fallada a les autoritats dins de les 72 hores següents a partir del moment al qual el responsable n'ha tingut constància pot ser objecte d'interpretacions variades. Normalment, es considera que se'n té constància quan hi ha certesa i coneixement suficient de les circumstàncies. La mera sospita no obliga a notificar ja que, en aquests casos, no és possible conèixer suficientment l'abast del succés.

Ara bé, si sospitem que el problema pot tenir un gran impacte, és recomanable contactar amb l'autoritat de supervisió.

En cas que no sigui possible realitzar la notificació dins el termini de 72 hores, pot fer-se més tard, però cal justificar-hi les causes del retard.

L'RGPD estableix el contingut mínim de la notificació. Aquests contenen elements com:

- La naturalesa de la violació.
- Les categories de dades i d'interessats afectats.
- Les mesures adoptades pel responsable per a solucionar la fallada i, si és el cas, les mesures aplicades per pal·liar els possibles efectes negatius sobre les persones interessades.

La informació també es pot proporcionar de forma escalonada, quan no es pugui fer completament al mateix moment de la notificació.

Finalment, el responsable del tractament ha de documentar qualsevol violació de la seguretat de les dades personals, inclosos els fets que hi estan relacionats, els seus efectes i les mesures correctores que s'han adoptat.

2.2.4 El responsable, l'encarregat del tractament i el delegat de protecció de dades (DPD)

L'RGPD introdueix les figures del responsable del tractament de dades, de l'encarregat del tractament i del delegat de protecció de dades.

El capítol IV de l'RGPD tracta del responsable, de l'encarregat del tractament i del delegat de protecció de dades.

Hi pot haver representants dels responsables i/o dels encarregats del tractament quan aquests no estan establerts a la Unió, però entra dins de l'àmbit del Reglament, segons recull l'article 3, apartat 2. En aquests casos, el responsable o l'encarregat del tractament ha de designar per escrit un representant a la Unió.

El responsable del tractament

El responsable del tractament o responsable és la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament. El responsable ho és i ha de poder demostrar (*accountability*) que les dades personals siguin:

- Adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten (minimització de dades).
- Conservades de manera que permetin identificar els interessats durant un període no superior al necessari per a les finalitats del tractament de dades personals.
- Exactes. Això implica que, quan sigui precís, s'hauran d'actualitzar. Cal adoptar les mesures raonables perquè es suprimeixin o es rectifiquin les dades personals que siguin inexactes amb les finalitats per a les quals es tracten ("exactitud");
- Tractades de manera lícita, lleial i transparent en relació amb l'interessat (licitud, lleialtat i transparència).
- Recollides amb finalitats determinades, explícites i legítimes; posteriorment no s'han de tractar de manera incompatible amb aquestes finalitats. D'acord amb l'article 89, el tractament posterior de les dades personals amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica i històrica o amb finalitats estadístiques no es considera incompatible amb les finalitats inicials (limitació de la finalitat).
- Tractades de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives adequades ("integritat i confidencialitat"), fent copies de seguretat...

Així, per exemple, el responsable del tractament serà qui haurà de decidir si les dades recollides inicialment amb el consentiment del client continuen essent vàlides per a una altra finalitat o no ho són i s'ha de tornar a demanar el consentiment al client. El responsable del tractament ha de prendre les mesures oportunes per facilitar a l'interessat tota la informació que indiquen els articles 13 (*Informació que cal facilitar quan les dades personals s'obtenen de l'interessat*) i 14 (*Informació que cal facilitar quan les dades personals no s'han obtingut de l'interessat*).

El responsable del tractament ha de facilitar a l'interessat l'exercici dels seus drets, en virtut dels articles 15 a 22.

L'encarregat del tractament

L'article 28 del RGPD tracta de l'**encarregat del tractament** o **encarregat**. L'encarregat és la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament. L'encarregat és únic i el nomena el responsable del tractament de les dades. L'encarregat del tractament pot, però, contractar a altres encarregats de tractament de dades amb el consentiment per escrit del responsable del tractament de dades. El tractament efectuat per l'encarregat s'ha de regir per un contracte o per un altre acte jurídic conforme al dret de la Unió o dels estats membres. Aquest contracte ha de vincular l'encarregat respecte del responsable i ha d'establir l'objecte, la durada, la naturalesa i la finalitat del tractament, així com el tipus de dades personals i categories d'interessats i les obligacions i els drets del responsable. Aquest contracte o acte jurídic ha d'estipular, en particular, que l'encarregat:

- Tracta les dades personals únicament seguint instruccions documentades del responsable.
- Garanteix que les persones autoritzades per tractar dades personals s'han compromès a respectar-ne la confidencialitat o estan subjectes a una obligació de confidencialitat de naturalesa estatutària.
- Respecta les condicions establertes als apartats 2 i 4, per recórrer a un altre encarregat del tractament.
- Pren totes les mesures necessàries, de conformitat amb l'article 32.
- Assisteix el responsable sempre que sigui possible, d'acord amb la naturalesa del tractament i mitjançant les mesures tècniques i organitzatives adequades perquè pugui complir amb l'obligació de respondre les sol·licituds que tinguin per exercici dels drets dels interessats.
- Ajuda el responsable a garantir el compliment de les obligacions.
- A elecció del responsable, ha de suprimir o retornar totes les dades personals, una vegada finalitzada la prestació dels serveis de tractament, i suprimir les còpies existents, tret que sigui necessari conservar les dades personals en virtut del dret de la Unió o dels estats membres.

- Ha de posar a disposició del responsable tota la informació necessària per demostrar que compleix les obligacions assenyalades en aquest article 28 de l'RGPD. Així mateix, ha de permetre i contribuir a la realització d'auditories, incloses inspeccions, per part del responsable o d'un altre auditor autoritzat pel responsable.

El delegat de protecció de dades (DPD)

El Reglament, a l'article 37, introdueix la figura del **Delegat de Protecció de Dades (DPD)** i especifica quan és necessari nomenar-lo.

El Delegat de Protecció de Dades pot formar part de la plantilla del responsable o l'encarregat o bé actuar en el marc d'un contracte de serveis.

El delegat de protecció de dades és nomenat pel responsable i l'encarregat del tractament i se l'ha de nomenar quan es alguna d'aquestes condicions:

- El tractament l'efectua una autoritat o un organisme públic, tret dels tribunals que actuen en l'exercici de la seva funció judicial.
- Les activitats principals del responsable o de l'encarregat consisteixen en operacions de tractament que requereixen una observació habitual i sistemàtica a gran escala.
- Les activitats principals del responsable o de l'encarregat consisteixen en el tractament a gran escala de categories especials de dades personals i de les dades relatives a condemnes i infraccions.

El delegat de protecció de dades s'ha de designar atenent a les seves qualitats professionals i als coneixements especialitzats del dret, a la pràctica en matèria de protecció de dades i a la capacitat per exercir les funcions esmentades a l'article 39, que principalment són:

- Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
- Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament.
- Cooperar amb l'autoritat de control.
- Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
- Supervisar que es compleix l'RGPD i la resta de legislació relativa a la protecció de dades.

Això no vol dir que el DPD hagi de tenir una titulació específica, però, tenint en compte que entre les funcions del DPD s'inclou l'assessorament al responsable o l'encarregat en tot el referent a la normativa sobre protecció de dades, els

coneixements jurídics en la matèria són sens dubte necessaris; també cal que compti amb coneixements aliens a l'àmbit estrictament jurídic, com per exemple en matèria de tecnologia aplicada al tractament de dades o en relació amb l'àmbit d'activitat de l'organització en la qual exerceix la seva tasca.

Altres coses a tenir en compte són:

- Un grup empresarial pot nomenar un únic delegat de protecció de dades, sempre que sigui fàcilment accessible des de cada establiment.
- Si el responsable o l'encarregat del tractament és una autoritat o un organisme públic, tret de jutjats i tribunals, es pot tenir un únic delegat de protecció de dades per diversos organismes.
- La posició del DPD a les organitzacions ha de complir els requisits que l'RGPD estableix expressament. Entre aquests requisits hi ha la total autonomia en l'exercici de les seves funcions, la necessitat que es relacioni amb el nivell superior de la direcció o l'obligació que el responsable o l'encarregat li facilitin tots els recursos necessaris per desenvolupar la seva activitat.

Els sistemes informàtics encarregats del tractament i del manteniment de dades gestionen sovint dades de caràcter personal. Quan ens trobem en aquesta situació, hem de complir l'RGPD i la resta de legislació de protecció de dades. Com que el tractament es fa en fitxers de l'empresa, la llei ens diu que hem d'adoptar les mesures necessàries per garantir la seguretat de les dades personals.

2.2.5 Dades personals

El concepte de *dada de caràcter personal* genera força confusions. Per determinar què és realment, ens hem de fixar en l'RGPD, que el defineix com "qualsevol informació sobre una persona física identificada o identificable, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona".

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 tinguin protecció les vinculades a la vida privada o íntima de la persona, sinó que són dades protegides 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..., 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...).
- Dades sanitàries (malalties, avortaments, cirurgia estètica...).
- Orientació sexual.
- Ideologia, creences religioses, afiliació sindical, estat civil...
- Dades econòmiques: bancàries, solvència, compres.
- Consums (aigua, gas, electricitat, telèfon...), subscripcions premsa...
- Dades judicials (antecedents penals).

Dades personals

Dades com el correu electrònic o dades biomètriques també són dades personals, ja que permeten identificar la persona. L'Agència de Protecció de Dades fins i tot considera la IP (Informe 327/2003) una dada personal.

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 i a la necessitat d'evitar que siguin usades per discriminar-nos. No es tracta de preservar la nostra intimitat, sinó d'evitar perjudicis per l'ús que es pugui fer d'aquestes dades.

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

Les dades sensibles reben una protecció més alta que la resta.

2.2.6 Infraccions i sancions de l'RGPD

L'incompliment d'una normativa legal pot comportar sancions. En el cas de l'RGPD, el règim de responsabilitat previst és de caràcter **administratiu** (menys greu que el penal i que no pot representar sancions privatives de llibertat). L'import de les sancions varia segons els drets personals afectats, volum de dades efectuats, els beneficis obtinguts, el grau d'intencionalitat i qualsevol altra circumstància que l'agència estimi oportuna.

Una diferència amb l'antiga LOPD és que no hi ha tipus de sancions (lleus, greus, molt greus). A l'article 83.2 especifica que les multes aniran en funció de la infracció. Les multes administratives poden arribar a ser d'entre 10 i 20 milions d'euros, o entre el 2 i el 4% del volum de negoci anual global. Per determinar la quantitat de les sancions es mirarà el cas particular tenint en compte:

- La naturalesa, gravetat i la durada de la infracció, estudiant la naturalesa, abast o propósit de la mateixa, així com el nombre d'interesats afectats i el nivell dels danys i perjudicis que hagin sofert.
- La intencionalidat o negligència en la infracció.

- Qualsevol mesura presa pel responsable o encarregat del tractament per solucionar i reduir els danys soferts pels interessats.
- El grau de responsabilitat de l'encarregat del tractament de les dades, segons les mesures aplicades per protegir la informació.
- Totes les infraccions anteriors dels responsables o encarregats del tractament.
- El grau de cooperació amb l'autoritat de control amb la finalitat de solucionar la infracció i mitigar els possibles efectes adversos de la infracció.
- Les categories de les dades de caràcter personal afectades per la infracció.
- La forma amb que l'autoritat de control va tenir coneixement de la infracció, en concret si el responsable o l'encarregat va notificar la infracció i en quina mesura.
- Que el responsable o l'encarregat ja hagin estat sancionats, amb advertència del compliment de les mesures.
- L'adhesió a codis de conducta o a mecanismes de certificació aprovats segons l'articulat del propi RGPD.
- Qualsevol altre factor agravant o atenuant aplicable a les circumstàncies del cas, com als beneficis financers obtinguts o a les pèrdues evitades, directa o indirectament, amb la infracció.

Exemple d'infracció i multa amb la nova llei

Donar les dades a una empresa de serveis, sense haver firmat el corresponent acord, amb les mesures de seguretat necessàries establertes per l'RGPD, que amb la LOPD era castigat fins a 300.000€, pasarà a ser multat fins a 10 milions d'euros o un 2% del volum de negoció total anual de l'any anterior.

2.3 Legislació sobre els serveis de societat de la informació i el comerç electrònic

Com a conseqüència de l'expansió de les xarxes d'ordinadors i especialment d'Internet, fenòmens que abans eren habituals dins del món analògic han acabat traspassant les fronteres per esdevenir freqüents en el món virtual (per exemple, el comerç electrònic). No podem esperar que el marc jurídic actual pugui donar resposta a tots els nous reptes provocats per l'ús de les tecnologies de la informació. Per donar resposta a aquests buits legals cal ampliar o redefinir conceptes jurídics. Aquesta regulació no solament ha d'evitar el mal ús de la tecnologia (per exemple, l'enviament de correu brossa o 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 és 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, l'objectiu de la **Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i del comerç electrònic** (LSSI) 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.

2.3.1 Concepte de serveis de la societat d'informació

Segons l'LSSI, el concepte de servei de la societat d'informació és molt ampli i comprèn els àmbits següents:

- Contractació de béns i serveis per via electrònica.
- Subministrament d'informació per via electrònica (per exemple, els diaris digitals).
- Activitats d'intermediació relatives a:
  - La provisió d'accés a la xarxa.
  - La transmissió de dades.
  - La realització de la còpia temporal de les pàgines d'Internet sol·licitades pels usuaris.
  - L'allotjament de dades en els servidors d'informació.
  - Els serveis o aplicacions facilitats per altres.
  - La provisió d'eines de cerca.
  - Els enllaços a altres llocs d'Internet.
- Qualsevol altre servei que es presti a petició individual dels usuaris (descàrrega de fitxers 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 cerca o qualsevol altre subjecte que disposi d'un lloc a Internet per mitjà del qual dugui 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 l'LSSI entén per proveïdors de serveis.

2.3.2 Obligacions i responsabilitat dels prestadors de serveis

No solament per desenvolupar l'esmentat marc de confiança, sinó també per poder perseguir les activitats il·lícites que es puguin desenvolupar a la xarxa, l'LSSI determina quines són les obligacions i responsabilitats dels prestadors de serveis. No oblideu, però, que l'LSSI se situa dins del marc jurídic extrapenal. Per això

les sancions que preveu aquesta llei no comporten penes privatives de llibertat. Per exemple, l'enviament de correu brossa o correu no consentit és una activitat sancionada per l'LSSI, però, en canvi, no apareix reflectida en el Codi Penal.

El correu brossa (*spam*) se sol prendre per un delicte informàtic, però no ho és.

Obligacions dels prestadors de serveis

Malgrat tot, les obligacions que tenen els prestadors de serveis, descrites en l'LSSI, possibiliten la persecució dels delictes relacionats amb 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.

Així, doncs, i sempre mitjançant una resolució judicial motivada, els prestadors de serveis han de col·laborar amb els jutges, i han 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 programes "pirates", els proveïdors de serveis hauran de lliurar al jutge encarregat de la investigació els fitxers de registre de l'activitat de l'usuari que ha allotjat el contingut il·lícit en el lloc.

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

Un altre aspecte destacable de 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).

Com podíem esperar, les dades que enregistra el proveïdor de serveis s'han d'emmagatzemar garantint els drets constitucionals i amb les mesures determinades per la llei de protecció de dades. Només pot retenir les dades imprescindibles per identificar l'**origen de la connexió** i el **moment en què s'inicià la prestació del servei**. La preservació de les dades no pot atemptar en cap cas 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 **responsabilitat civil, penal i administrativa**. Per determinar el tipus de responsabilitat que recau sobre ells caldrà diferenciar les situacions següents:

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.

Fòrum de discussió

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.

- 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. És el cas, per exemple, del gestor d'una llista de distribució de correu electrònic (*mailing list*) o del moderador d'un fòrum de discussió. En tots dos casos, el prestador pot tenir coneixement de la informació que s'introdueix a la Xarxa i en pot exercir-ne el control. Per tant, la seva responsabilitat és inqüestionable.

- Quan no hi ha participació activa del prestador amb relació als continguts

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 en són responsables, sempre que no es produeixin les situacions següents: que els prestadors no hagin originat la transmissió, que no hagin modificat ni seleccionat les dades o 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*). En aquest cas els proveïdors tampoc 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 (un lloc 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 o 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 coneixement efectiu quan:

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

En el cas del portal YouTube, els mateixos usuaris poden determinar i marcar els continguts que no consideren lícits.

- Finalment, quan el prestador facilita enllaços amb continguts o inclou eines de cerca, 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 o 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 usuaris potencials del comerç electrònic, convé que conegueu les obligacions d'informació que tenen totes les empreses que es dediquen a aquesta activitat. El portal web ha de mostrar, entre d'altres, les dades següents:

- La denominació social, NIF, domicili i adreça de correu electrònic o fax.
- Els codis de conducta als quals s'ha adherit.
- Preus dels productes o serveis que ofereix, 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 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.

2.3.3 Regulació de comunicacions publicitàries (correu brossa)

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

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

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

- L'RGPD determina la necessitat del consentiment de la persona interessada en el cas del tractament de dades amb finalitats de publicitat i de prospecció comercial.
- L'LSSI també prohibeix l'enviament de comunicacions publicitàries per correu electrònic (o mitjans electrònics equivalents) si no ha estat prèviament autoritzat de manera expressa pels destinataris.

L'incompliment d'aquesta prohibició pot constituir una **infracció lleu**, punible amb **una multa de fins a 30.000 euros**, o bé una **infracció greu**, que es pot castigar amb una **multa de 30.001 a 150.000 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 (si així ho fa saber).

Les infraccions de l'LSSI poden ser lleus, greus i molt greus.