Seguretat i alta disponibilitat

CFGS.ASX.M11/0.13

Administració de sistemes informàtics en xarxa

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
Alba Batlle Linares
Ivan Basart Carrillo
Carles Caño Valls
Jordi Cárdenas Guia
Miquel Colobran Huguet
Jordi Masfret Corrons
Josep Pons Carrió
Jordi Prats Català

Primera edició: febrer 2013

Dipòsit legal: B. 29402-2013

Introducció

Passades ja unes dècades d'evolució del món de la computació, la maduresa en el disseny dels sistemes informàtics ha fet obrir nous fronts importants pel que fa a la seguretat informàtica i a la disponibilitat de les dades. Aquesta és la justificació que aquest mòdul es trobi dins dels continguts del cicle de sistemes microinformàtics en xarxa, essent a més nou respecte al currículum de l'anterior legislació. El mòdul requereix el domini d'altres relacionats amb els sistemes informàtics i amb les xarxes d'ordinadors, i els seus continguts estan estructurats en quatre unitats.

La unitat formativa "Seguretat física, lògica i legislació" explica la seguretat informàtica a partir de la fiabilitat, un concepte utilitzat per mesurar la garantia de la qualitat de servei, en aquest cas la qualitat de servei d'un sistema informàtic. Posteriorment es defineixen les possibles vulnerabilitats d'un sistema com a mancances de seguretat en un determinat àmbit. En el sistema es podran detectar aquestes febleses i reaccionar per aplicar-hi contencions. Alhora, s'explica que cal tenir en compte que existeix una legislació, unes normatives i una protecció de dades i que cal vetllar pel seu compliment, coneixent també quan un incident de seguretat ha de ser comunicat per tal d'iniciar una investigació informàtica forense amb la finalitat de descobrir-ne l'autoria i poder iniciar els procediments legals corresponents.

La unitat formativa "Seguretat activa i accés remot" tracta la seguretat activa, tema cada cop més important des que els sistemes permeten accessos remots. La seguretat activa versa sobre les diferents opcions que té l'administrador per aplicar contramesures davant de possibles amenaces i atacs, per a la qual cosa disposa d'un gran ventall d'eines informàtiques. La manera correcta de procedir és incloure aquestes mesures i eines en el pla de seguretat del sistema o de l'empresa.

A la unitat formativa "Tallafocs i servidors intermediaris" es treballen dues eines importants en la gestió de la seguretat del trànsit de les dades: els tallafocs i els servidors intermediaris. Aquests elements són importants de configurar i gestionar per garantir la seguretat del servei i poder monitorar les possibles connexions de dades amb els servidors d'una organització, bé sigui dins la xarxa interna, bé en els nodes de connexió amb xarxes de gran abast, com ara Internet.

La darrera unitat formativa, "Alta disponibilitat", descriu les tecnologies potser més avançades de la informàtica de sistemes: l'alta disponibilitat i la virtualització. Aquests avenços en el disseny de sistemes han permès reduir les aturades de servei i han ajudat a millorar, en el cas de les configuracions en clúster, l'escalabilitat i el balanceig de càrrega del sistema, i en el cas de la virtualització, la facilitat de rèplica i de redimensionament de sistemes i de serveis.

Resultats d'aprenentatge

En finalitzar aquest mòdul, l'alumne/a:

Seguretat física, lògica i legislació

1. Reconeix les vulnerabilitats d'un sistema informàtic i adopta pautes i pràctiques de tractament segur de la informació.
2. Coneix la legislació i normativa sobre seguretat i protecció de dades i en valora la importància.

Seguretat activa i accés remot

1. Implanta mecanismes de seguretat activa, seleccionant i executant contramesures enfront d'amenaces o atacs al sistema.
2. Implanta tècniques segures d'accés remot a un sistema informàtic, interpretant i aplicant el pla de seguretat.

Tallafocs i servidors intermediaris

1. Implanta tallafocs per assegurar un sistema informàtic, analitzant-ne les prestacions i controlant-ne el trànsit cap a la xarxa interna.
2. Implanta servidors intermediaris aplicant-hi criteris de configuració que garanteixin el funcionament segur del servei.

Alta disponibilitat

1. Implanta solucions d'alta disponibilitat emprant tècniques de virtualització i configurant els entorns de prova.

Continguts

Seguretat física, lògica i legislació

Unitat 1

Seguretat física, lògica i legislació

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

Seguretat activa i accés remot

Unitat 2

Seguretat activa i accés remot

1. Mecanismes de seguretat activa
2. Implantació de tècniques d'accés remot

Tallafocs i servidors intermediaris

Unitat 3

Tallafocs i servidors intermediaris

1. Tallafocs
2. Servidors intermediaris

Alta disponibilitat

Unitat 4

Alta disponibilitat

1. Alta disponibilitat
2. Virtualització

Seguretat física, lògica i legislació

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

Índex

Introducció 5

Resultats d'aprenentatge 7

1 Seguretat informàtica 9
1.1 Conceptes de seguretat informàtica: fiabilitat, confidencialitat, integritat i disponibilitat 9
1.2 Elements vulnerables: maquinari, programari i dades 11
1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic 12
1.4 Seguretat física i ambiental 13
1.4.1 Ubicació física i condicions ambientals dels equips i servidors 14
1.4.2 Protecció física dels sistemes informàtics 16
1.5 Seguretat lògica 20
1.5.1 Criptografia i funcions hash 20
1.5.2 Criptosistemes de clau privada o simètrics 20
1.5.3 Criptosistemes de clau pública 21
1.5.4 Llistes de control d'accés 24
1.5.5 Polítiques d'emmagatzematge 26
1.5.6 Còpies de seguretat i imatges de suport 29
1.5.7 Mitjans d'emmagatzematge 33
1.6 Amenaces 36
1.6.1 Amenaces físiques 36
1.6.2 Amenaces lògiques 37
1.7 Anàlisi forense en sistemes informàtics 39
1.7.1 Assegurament de l'evidència digital 40
1.7.2 Identificació de l'evidència digital 40
1.7.3 Recollida de les evidències digitals 41
1.7.4 Obtenció i preservació d'evidències digitals 42
1.7.5 Anàlisi de les evidències digitals 44
1.7.6 Presentació i informe 45

2 Legislació sobre seguretat, protecció de dades i Codi Penal 47
2.1 Marc jurídic penal 47
2.1.1 El "delicte informàtic" 47
2.1.2 El Codi Penal i les conductes il·lícites relacionades amb la informàtica 48
2.1.3 Delictes contra la intimitat 49
2.1.4 Delicte de frau informàtic 51
2.1.5 Delicte de danys 52
2.1.6 Delictes contra la propietat intel·lectual 52
2.1.7 Delicte de revelació de secrets d'empresa 56
2.1.8 Altres delictes i la investigació dels delictes informàtics 57
2.2 Marc jurídic extrapenal 58
2.2.1 Legislació sobre protecció de dades 59
2.2.2 Obligacions de les empreses i els implicats en els tractaments 65

2.2.3 Notificació de violacions de seguretat 65
2.2.4 El responsable, l'encarregat del tractament i el delegat de protecció de dades (DPD) . 67
2.2.5 Dades personals 70
2.2.6 Infraccions i sancions de l'RGPD 71
2.3 Legislació sobre els serveis de societat de la informació i el comerç electrònic 72
2.3.1 Concepte de serveis de la societat d'informació 73
2.3.2 Obligacions i responsabilitat dels prestadors de serveis 73
2.3.3 Regulació de comunicacions publicitàries (correu brossa) 77

Introducció

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

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

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

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

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

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

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

Resultats d'aprenentatge

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

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

1. Seguretat informàtica

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

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

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

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

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

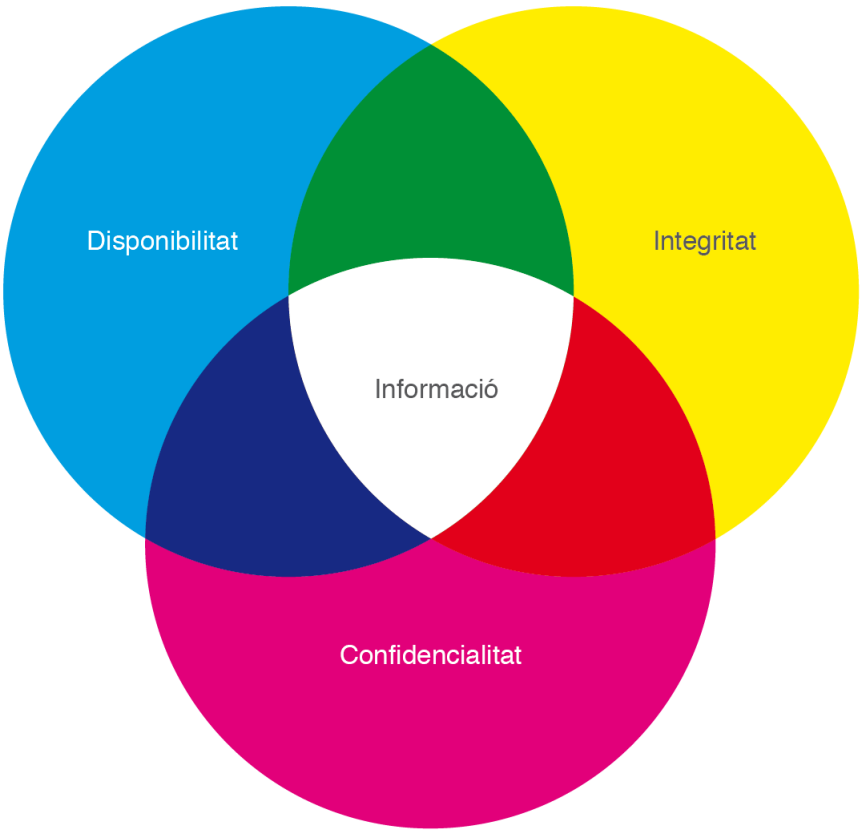
Com podem suposar, és difícil trobar un sistema informàtic que maximitzi les tres propietats. Normalment, i segons l'orientació del sistema, se'n prioritzarà alguna. Per exemple, en un sistema que emmagatzemi dades de caràcter policial, l'element que cal prioritzar és la confidencialitat de la informació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

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

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

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

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



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

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

1.2 Elements vulnerables: maquinari, programari i dades

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

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

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

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

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

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

1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic

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

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

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

Exemple de vulnerabilitat d'origen físic

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

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

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

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

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

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

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

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

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

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

Exemple d'enginyeria social

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

Mals hàbits

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

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

1.4 Seguretat física i ambiental

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

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

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

Cavalls de Troia

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

1.4.1 Ubicació física i condicions ambientals dels equips i servidors

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

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

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

Sistemes d'alimentació ininterrompuda

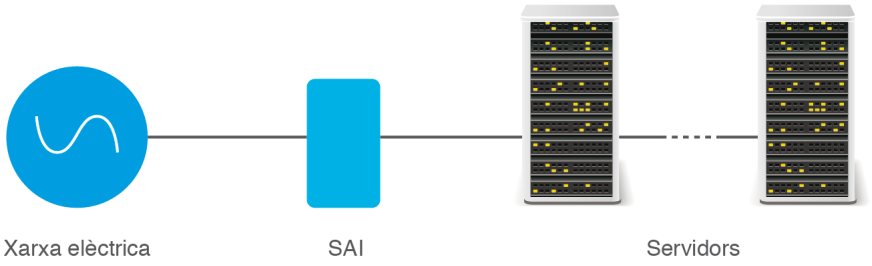
El **sistema d'alimentació ininterrompuda** (SAI) protegeix els servidors de talls de corrent i d'altres problemes relacionats amb la tensió.

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

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

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

Figura 1.2. Esquema de xarxa amb SAI



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

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

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

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

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

1.4.2 Protecció física dels sistemes informàtics

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

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

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic (útil en casos de robatori).
- Protegir i aïllar el cablatge de la xarxa (tant per a protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància (cal tenir present la normativa que en regula la instal·lació).
- Triar una topologia de xarxa adequada a les nostres necessitats.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Proveir mecanismes d'autenticació als usuaris que volen accedir al sistema.

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

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

Mecanismes d'autenticació d'usuaris

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

- Sistemes basats en elements coneguts per l'usuari.

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

1. Sistemes basats en elements coneguts per l'usuari

Els principals mecanismes dins d'aquest tipus d'autenticació són els sistemes basats en contrasenyes. És un dels mètodes que es fan servir més sovint per autenticar els usuaris que volen accedir a un sistema. Òbviament, és el mètode més barat, però també és el més vulnerable, ja que encara que la paraula de pas o contrasenya hauria de ser personal i intransferible, sovint acaba en poder de persones no autoritzades. D'altra banda, encara que les contrasenyes s'emmagatzemin xifrades en un fitxer, és possible desxifrar-les emprant múltiples tècniques.

Xifra

Una **xifra o criptosistema** és un mètode secret d'escriptura mitjançant el qual un text en clar es transforma en un text xifrat o criptograma, il·legible si no es disposa de la clau de xifratge.

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

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No usar la mateixa contrasenya en comptes diferents.
- No llençar documents amb contrasenyes a la paperera.
- Evitar utilitzar paraules de diccionari. Hi ha tècniques de descobriment de contrasenyes basades en la comparació amb diccionaris sencers de paraules, per idiomes, de temes concrets com esports... Aquestes tècniques reben el nom d'*atacs de diccionari*.
- Evitar utilitzar dades que puguin ésser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el mateix nom que l'identificador, el DNI, la data de naixement, el número de mòbil...).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament numèriques.
- Afavorir l'aparició de caràcters especials (!, *, ?...).
- No enviar contrasenyes per SMS o correu ni dir-les per telèfon.
- No utilitzar seqüències de teclat del tipus "qwerty" o "1234" (són seqüències que s'assagen en els atacs de diccionari).
- Fer servir sistemes mnemotècnics per recordar les contrasenyes (per exemple, "Cada dia al matí canta el gall quiquiriquic" donaria lloc a la contrasenya "CDAMCEGC").

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

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

2. Sistemes basats en elements que té l'usuari

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

PIN

El PIN (*Personal Identification Number*) és una contrasenya numèrica, sovint formada per quatre xifres, com, per exemple, el codi numèric que ens demana el caixer automàtic.

a) Sistemes basats en targetes intel·ligents i testimonis (*tokens*) de seguretat

Una targeta intel·ligent (*smartcard*) és similar a una targeta de crèdit, però a diferència d'aquesta, les targetes intel·ligents compten amb un microprocessador (i memòria) que les dota de les capacitats següents:

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

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

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

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

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

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

RFID

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

b) Sistemes biomètrics

Els sistemes biomètrics es basen en les característiques físiques de l'usuari que s'ha d'autenticar (o en patrons característics que puguin ser reconeguts, com per exemple, la signatura manual). Com a avantatge principal, l'usuari no ha de recordar cap contrasenya ni cal que porti cap testimoni o targeta al damunt. Solen ser més cars que els mètodes anteriors. Per això encara no es fan servir gaire, tot i que alguns d'aquests mètodes ofereixen un alt nivell de fiabilitat a un preu raonable

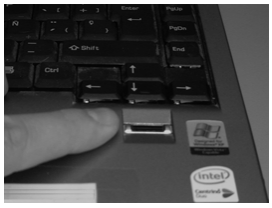
(per exemple, el reconeixement dactilar). Entre les característiques que es poden utilitzar per identificar un usuari mitjançant mesures biomètriques destaquem les següents:

Mesures biomètriques

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

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

Els sistemes biomètrics es componen de dos mòduls no interconnectats:



Lector d'empremtes dactilars incorporat en un ordinador portàtil.

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

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

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

1.5 Seguretat lògica

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

1.5.1 Criptografia i funcions hash

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

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

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

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

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

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

1.5.2 Criptosistemes de clau privada o simètrics

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

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

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

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

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

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

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

1.5.3 Criptosistemes de clau pública

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

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

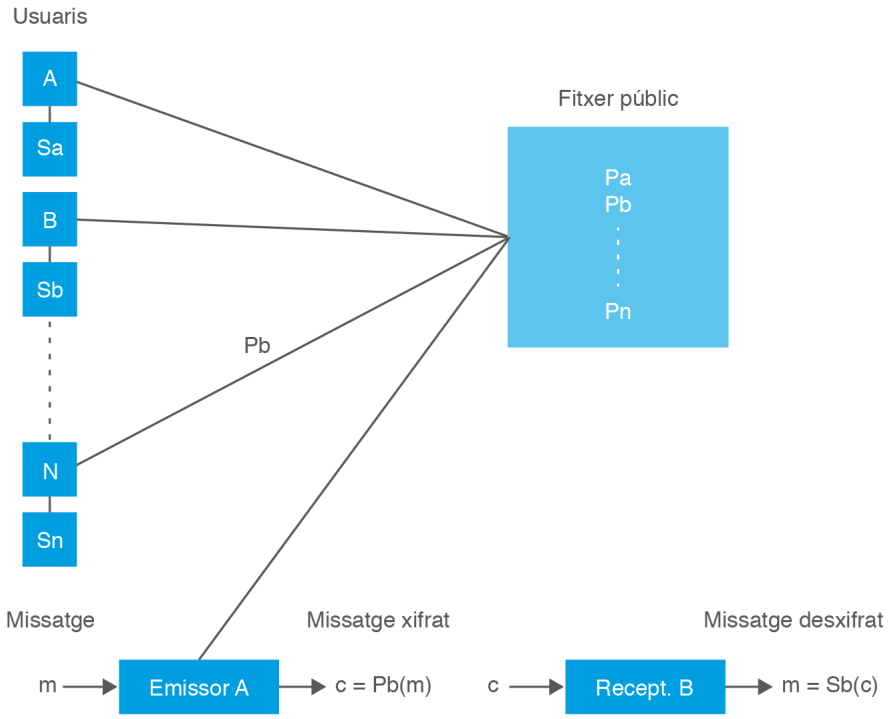
Criptosistemes de clau pública

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

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

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

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



A: usuari A

Sa: clau secreta de l'usuari A.

Sb: clau secreta de l'usuari B.

Pa: clau pública de l'usuari A.

Pb: clau pública de l'usuari B.

m: missatge a enviar

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

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

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

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

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

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

DSS

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

Certificat digital

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

Les funcions hash o funcions resum

Una **funció *hash*** o funció resum és una funció matemàtica que fa correspondre una representació de mida fixa a un missatge *m* de mida variable. Aquesta representació té de 128 a 512 bits (segons la funció que s'empri) i s'anomena *valor resum del missatge*.

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

Hola.txt 89736DF30DC47A7D5AC22662DC3B5E9C

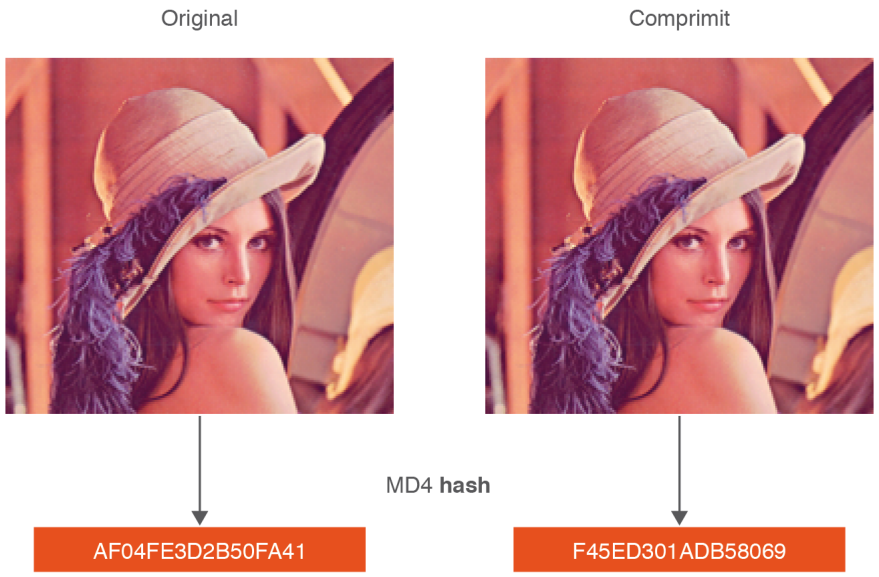
El valor *hash* identifica, pràcticament de manera unívoca, un fitxer qualsevol. Podríem dir, doncs, que exerceix de codi ADN de fitxers. No obstant això, cal fer una matisació important: existeix una probabilitat, encara que molt petita, que dos fitxers **diferents** tinguin el mateix valor *hash* (**col·lisió**).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

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

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

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

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



1.5.4 Llistes de control d'accés

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

Control d'accés

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

Principi de privilegi mínim

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

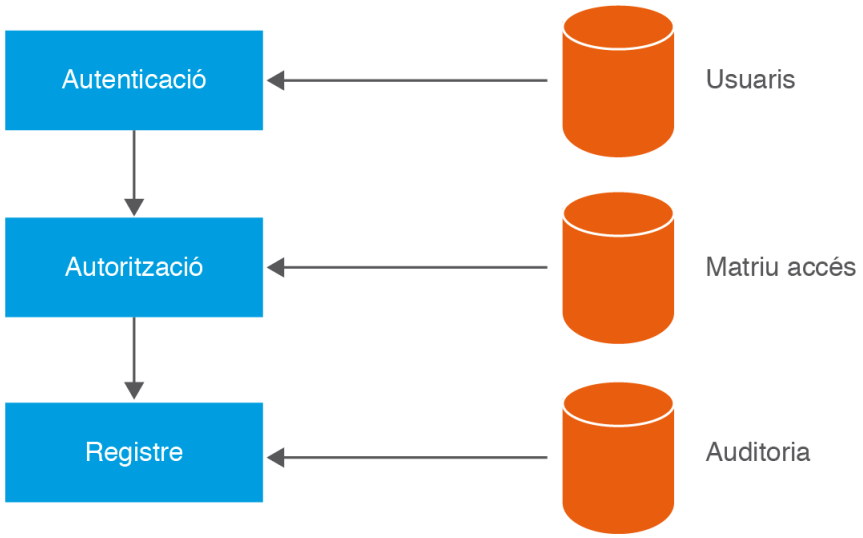
- **Autenticació**: mecanisme de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic. Habitualment es fa mitjançant nom de l'usuari i contrasenya o testimoni (*token*) del procés.
- **Autorització**: procés mitjançant el qual el sistema autoritza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

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

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

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

Figura 1.5. Procés de validació



Matriu de control d'accés

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

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

Taula 1.2. Matriu de control d'accés

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

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

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

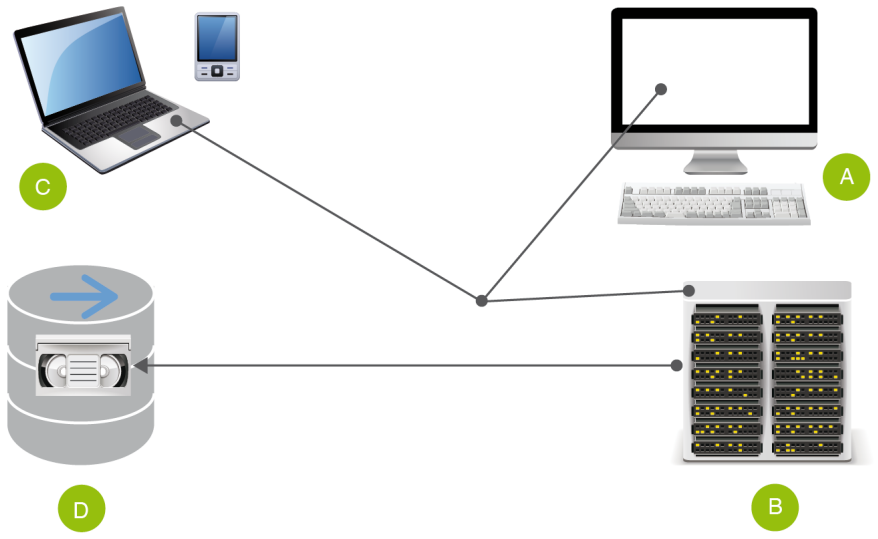
Llista de control d'accés (ACL)

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

1.5.5 Polítiques d'emmagatzematge

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

FIGURA 1.6. Ubicació de les dades en un sistema informàtic



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

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

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

(D) Política de còpies de seguretat.

Polítiques d'emmagatzematge local en els equips de treball

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

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

Política d'emmagatzematge a la xarxa corporativa

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

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

Política sobre l'ús de dispositius externs

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

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

Política de còpies de seguretat

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

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

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

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

1.5.6 Còpies de seguretat i imatges de suport

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

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

Tipus de còpies de seguretat

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

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

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

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

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

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

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

Figura 1.7. Copia de seguretat incremental

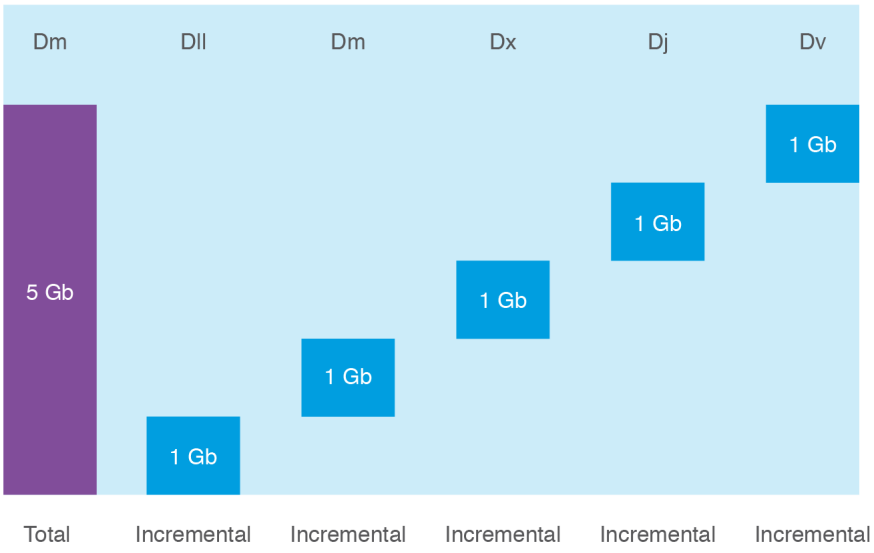
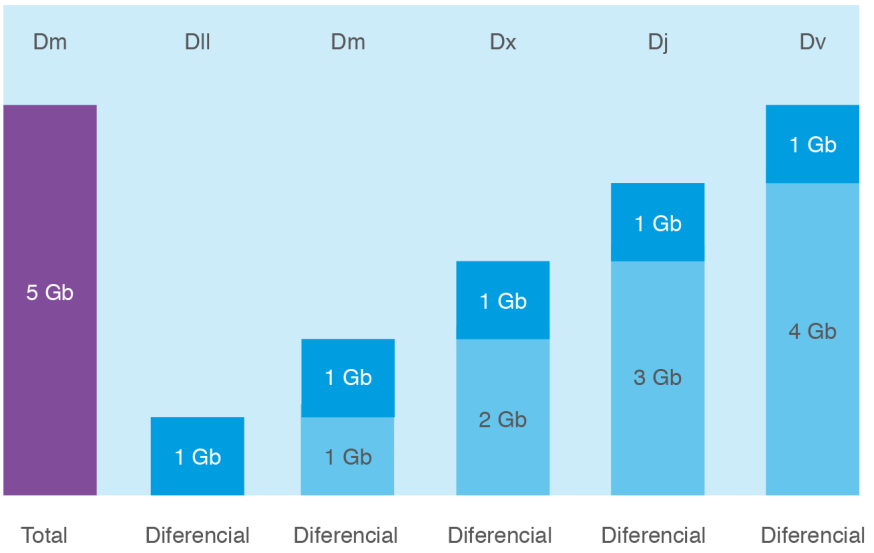


Figura 1.8. Copia de seguretat diferencial



Polítiques de còpies de seguretat

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

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

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

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

- Informació que varia diàriament
- Informació no variable

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

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

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

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

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

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

1.5.7 Mitjans d'emmagatzematge

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

Targetes perforades al tèxtil

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

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

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

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

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

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

Tendències

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

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

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

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

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

Còpia disc a disc

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

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

Llibreries de còpia comercials

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

1.6 Amenaces

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

1.6.1 Amenaces físiques

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

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

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

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

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

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

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

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

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

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

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

Solid State Drive

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

1.6.2 Amenaces lògiques

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.7 Anàlisi forense en sistemes informàtics

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

Definició d'evidència

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

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

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

Fragilitat de l'evidència digital

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

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

Preguntes clau:

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

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

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

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

1.7.1 Assegurament de l'evidència digital

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

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

1.7.2 Identificació de l'evidència digital

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

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

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

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

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

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

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

1.7.3 Recollida de les evidències digitals

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

Recollida d'ordinadors en funcionament

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

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

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

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

Recollida d'ordinadors apagats

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

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

1.7.4 Obtenció i preservació d'evidències digitals

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

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

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

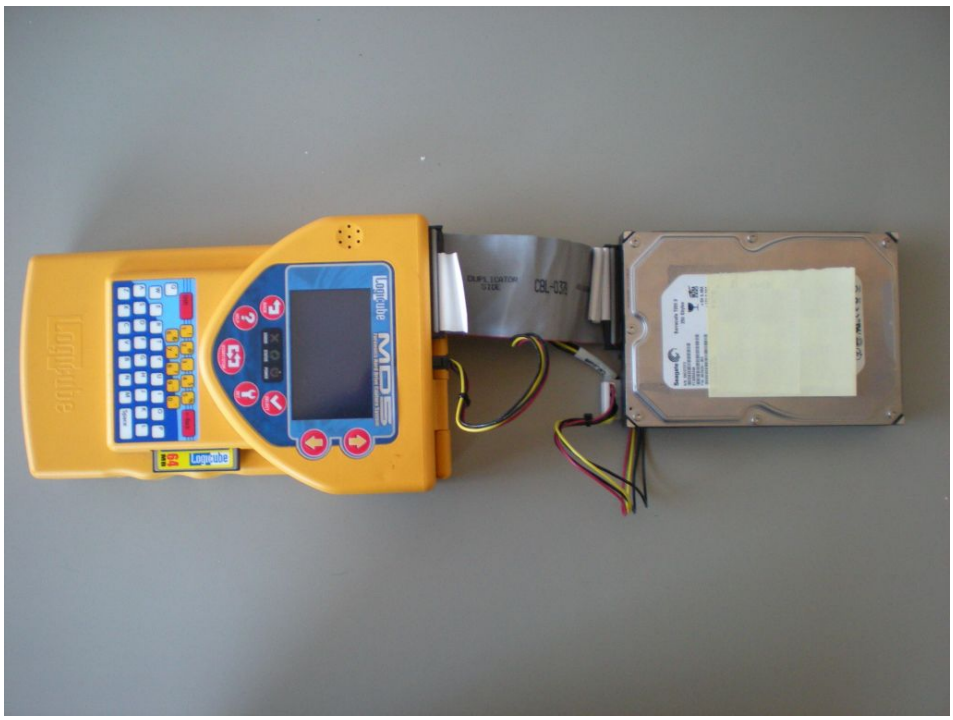
La còpia o clon s'efectuarà, normalment, en dispositius (DVD, discs durs...) aportats per l'analista. L'elecció d'un o altre mitjà (normalment es fa sobre discs durs) dependrà de la quantitat d'informació continguda en els suports originals. Finalment, el programari o maquinari emprat per a l'obtenció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

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

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

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

Figura 1.9. Dispositiu de clonació



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

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

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

1.7.5 Anàlisi de les evidències digitals

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

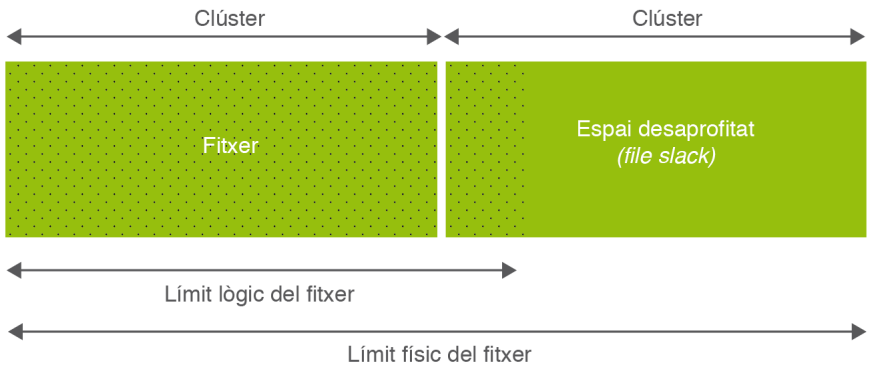
Un exemple de metadada podria ser, per exemple, el camp "Autor" d'un fitxer DOC.

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

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

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

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



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

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

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

1.7.6 Presentació i informe

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

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

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

2.1 Marc jurídic penal

D'una manera intuïtiva, tots coneixem l'existència d'un conjunt de normes jurídiques que regulen les conductes constitutives de delicte, i també les sancions previstes en aquestes situacions (algunes poden ser fins i tot privatives de llibertat). El recull legislatiu aplicable en aquest tipus de matèria s'anomena Codi Penal. Cada país disposa de les seves pròpies normes i, per tant, és possible que variïn d'un país a un altre. És molt important conèixer l'essència de la normativa que afecta l'ús de les tecnologies, ja que, amb independència de la nostra voluntat, condiciona l'ús de les tecnologies, tant des del punt de vista del treballador tècnic, com del de l'usuari d'un ordinador d'una llar qualsevol.

Definició de delicte

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

2.1.1 El "delicte informàtic"

El delicte informàtic no apareix explícitament definit en l'actual Codi Penal (1995), ni en les reformes posteriors (Llei 15/2003 i Llei 5/2010) que se n'han fet i, per tant, no es pot parlar de delicte informàtic pròpiament dit, sinó de delictes fets amb l'ajut de les noves tecnologies, en els quals l'ordinador s'usa com a mitjà d'execució del delicte (per exemple, l'enviament d'un correu electrònic amb amenaces) o com a objectiu d'aquesta activitat (per exemple, una intrusió en un sistema informàtic).

Límits tècnics i legals

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

Una **intrusió** és un accés no autoritzat a un sistema informàtic.

La legislació del nostre país encara presenta buits pel que fa als mal anomenats *delictes informàtics*, de manera que tan sols oferirem un seguit de directrius bàsiques, més relacionades amb el sentit comú que amb la normativa complexa que es va generant entorn de l'aplicació de les noves tecnologies.

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

- Si el meu cap em demana que li mostri el contingut de la bústia de correu personal d'un treballador, tinc l'obligació de fer-ho?
- Puc entrar a la bústia de correu electrònic d'un amic?
- Uns intrusos han modificat el lloc web de l'empresa en què treballo. Aquest fet és denunciable? A qui ho he de denunciar?
- El sistema informàtic de la feina emmagatzema dades de caràcter personal (com, per exemple, el nom, els cognoms, l'adreça i el DNI dels treballadors). Cal protegir aquestes dades d'alguna manera?
- Puc penjar a Internet un lloc web amb les fotografies i logotips del meu grup de música preferit?
- Puc descarregar lliurement qualsevol fitxer de música de la xarxa?

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

2.1.2 El Codi Penal i les conductes il·lícites relacionades amb la informàtica

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

La constitució és la norma fonamental de l'Estat, superior a la resta de lleis i a qualsevol tipus de norma.

Un dels articles de la Constitució espanyola (1978) relacionats amb la pràctica informàtica (tant des del punt de vista tècnic com del simple usuari) és l'article 18, que reconeix el dret a la intimitat. Han de ser objecte de protecció no sols l'àmbit íntim de l'individu, sinó també l'esfera familiar i domiciliària.

Article 18 de la Constitució

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

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

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

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

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

2.1.3 Delictes contra la intimitat

Una part molt important dels delictes relacionats amb la informàtica entra dins de la tipificació de **delictes contra la intimitat**. Sovint, els autors d'aquestes conductes no són conscients de la importància dels béns protegits per la llei i no s'adonen de les conseqüències de les seves accions fins que ja és massa tard.

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

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

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

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

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

Activitats personals

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

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

Usurpació i cessió de dades reservades de caràcter personal

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

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

El Codi Penal considera un agreujant que l'objecte del delicte siguin dades de caràcter personal que revelin ideologia, religió, creences, salut, origen racial o vida sexual. Altres circumstàncies agreujants són que la víctima sigui un menor d'edat o incapacitat o que la persona que comet el delicte sigui responsable dels fitxers que hi estan involucrats. Mereix una consideració especial l'article 199.2, en el qual es castiga la conducta del professional que, incomplint l'obligació de reserva, **divulga els secrets** d'una altra persona.

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

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

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

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

Delicte d'intrusió

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

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

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

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

2.1.4 Delicte de frau informàtic

En l'article 248.2 del Codi Penal es castiga la conducta de qui, emprant qualsevol mètode informàtic, aconsegueixi la transferència no consentida de qualsevol bé, amb ànim de lucre i perjudici sobre tercer. També apareixen en el Codi Penal les conductes preparatòries per a la comissió de delictes de frau informàtic, les quals poden ser, a tall d'exemple, la fabricació, la facilitació o simplement la mera possessió de programes específics destinats a la comissió del delicte de frau informàtic.

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

Definició d'enginyeria social

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

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

2.1.5 Delicte de danys

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

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

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

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

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

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

2.1.6 Delictes contra la propietat intel·lectual

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

Xarxes d'igual a igual

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

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

Llei de propietat intel·lectual

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

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

Permís dels titulars

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

Exemples de delictes contra la propietat intel·lectual

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

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

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

Llicència de programari

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

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

Pel que fa a la **creació de programari**, també cal fer algunes consideracions. Segons el tipus de contracte al qual es trobi subjecte el treballador, el programari que desenvolupi per a una organització determinada pertany a l'empresa i, en conseqüència, si el treballador abandona l'organització, no es pot emportar el programari que ha creat en el seu antic lloc de treball. Com en el cas de la utilització del correu electrònic, seria recomanable que el contracte de treball especifiqués aquesta qüestió.

La còpia privada

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

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

Tipus de llicències

L'ús d'una llicència no adequada (per exemple, una llicència personal en lloc d'una llicència de xarxa) pot comportar problemes diversos i no s'hi val a argumentar el desconeixement com a eximent.

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

- **OEM (**Original Equipment Manufacturer**).** Tipus de llicència, normalment referida a sistemes operatius (encara que també es pot aplicar al maquinari), que supedita la venda del programa com a part integrant d'un equip informàtic nou (programari preinstal·lat). Així, doncs, aquest programari no es pot vendre aïlladament, sinó juntament amb el maquinari que l'incorpora. Solen no disposar de l'embalatge de la versió normalitzada del producte. No es poden vendre ni cedir a tercers separats del maquinari.
- ***Retail***. Consisteix en les versions de venda normalitzades d'un programari, amb els embalatges que se solen veure a les botigues d'informàtica. A diferència de les versions OEM, es poden vendre independentment del maquinari on s'integren i poden tenir algun extra que no apareix en les versions OEM.
- **Llicències per volum.** Llicències destinades a empreses i institucions (com instituts i universitats). Són similars a les llicències OEM, però no estan

vinculades a equips nous. Poden servir, per exemple, per instal·lar un programari d'ús comú en una xarxa d'ordinadors d'un institut.

Llicències de programari lliure

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

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

Free Software Foundation

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

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

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

Programari descatalogat (abandonware)

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

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

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

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

Projecte GNU (GNU is Not Unix)

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

L'any 1991 Linus Torvalds va començar a escriure el nucli del sistema operatiu Linux, que va distribuir amb llicència GPL. Gràcies a les aportacions de molts altres programadors, el nucli de Linux es va acabar combinant amb el sistema GNU, i va formar l'anomenat GNU/Linux o distribució Linux, paradigma dels sistemes operatius lliures.

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

- **Llicències MPL** (Mozilla Public License) i derivades. Aquest tipus de llicència rep el nom del projecte de programari lliure Mozilla, a bastament conegut per tota la comunitat d'internautes. En aquest cas, i a diferència de les llicències GPL, no cal que el producte final també sigui llicenciat en MPL (encara que el codi font modificat o copiat amb MPL ha de mantenir aquest tipus de llicència). D'aquesta manera, es promou efectivament la col·laboració entre autors i la generació de programari lliure, ja que les llicències GPL presentaven el problema d'afavorir una certa expansió endogàmica a causa de l'obligació que el producte final fos també llicenciat en GPL. Aquestes llicències són més restrictives que les BSD i, en definitiva, es poden considerar a mig camí entre aquestes i les GPL.

- **Llicències *copyleft***. En aquest cas, el propietari de la llicència gaudeix del dret de còpia, modificació i redistribució. A més, també pot desenvolupar una versió d'aquest programari (amb llicència subjecte a *copyright*) i vendre'l o cedir-lo amb qualsevol de les llicències estudiades, sense que això afecti les llicències *copyleft* ja atorgades. L'autor també pot retirar una llicència *copyleft*, però sense efectes retroactius, ja que l'autor no té dret a retirar el permís d'una llicència que encara es troba vigent. Es pot aplicar no només a programes, sinó a tota mena de creacions artístiques (música, vídeo...).

2.1.7 Delicte de revelació de secrets d'empresa

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

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

2.1.8 Altres delictes i la investigació dels delictes informàtics

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

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

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

- **Els fitxers o registres locals**. Els sistemes operatius i els programaris que s'executen en els ordinadors enregistren algunes de les activitats que fan en els anomenats *fitxers de registre*. Per exemple, la intrusió d'un pirata en un sistema informàtic deixa, si l'atacant no és gaire hàbil, empremtes en diversos fitxers del sistema. La informació que contenen aquests fitxers (per exemple, l'adreça IP de l'atacant) és la primera baula que els investigadors analitzen per arribar a establir l'origen de l'atac.
- **Els registres dels proveïdors de servei d'Internet (PSI)**. La persona que ha comès el delicte (o qualsevol altre fet susceptible de ser investigat) haurà utilitzat la connexió oferta per un cert proveïdor de serveis d'Internet. Les dades associades a aquesta connexió són emmagatzemades pels PSI segons la **Llei de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions** (com a màxim 12 mesos, a partir de la data de comunicació de reserva, encara que es pot ampliar o reduir), les quals només poden ser cedides als investigadors per ordre judicial. Així, doncs, un cop que els investigadors han establert la informació bàsica del succés (IP d'origen, franja horària i la data en què s'ha produït l'esdeveniment), caldrà que sol·licitin al jutge una ordre perquè el proveïdor de serveis els lliuri la informació requerida (associada a la IP i a la resta de dades determinades en les etapes inicials de la investigació) per continuar el procés i identificar l'usuari que ha emprat la connexió sospitosa.

Proveïdor de serveis (PSI)

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

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

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

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

1. Adjuntar els fitxers de registre (registres locals del sistema) relacionats amb el delicte comès. Aquests fitxers han de reflectir, en cas que hagin quedat registrats, la IP de l'atacant i les accions produïdes en el sistema investigat.
2. En cas que s'hagi produït un delicte de danys, cal adjuntar una valoració dels danys ocasionats.
3. Actuar amb rapidesa (els proveïdors no emmagatzemen indefinidament els fitxers de registre dels seus servidors).
4. En cas que aquesta acció delictiva s' hagi produït per correu electrònic, cal adjuntar les capçaleres completes del correu rebut.
5. En cas que sigui necessari, cal considerar la possibilitat de duplicar (o clonar) el disc dur del servidor per preservar les proves del delicte i, a continuació, reinstal·lar el sistema per evitar que el delicte es continuï produint. No obstant això, cal anar amb compte amb aquesta consideració. Suposem, per exemple, que l'administrador d'un sistema descobreix que el servidor del qual és responsable allotja pornografia infantil. La duplicació del disc dur (a l'efecte de salvaguardar les proves) i la reinstal·lació posterior de tot el sistema permetrien evitar que el delicte (la difusió de pornografia infantil) es continués produint, però al mateix temps en podria dificultar la investigació.

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

2.2 Marc jurídic extrapenal

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

Marc extrapenal

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

La legislació té molta cura de la protecció de les dades perquè contenen informació personal que ha d'ésser protegida adequadament. Això afecta de manera negativa els sistemes informàtics, la gestió de les organitzacions, i fins i tot el dia a dia de les

persones. El conjunt de normes intenta trobar un equilibri entre aquests elements, aparentment oposats: un nivell de seguretat de les dades adequat, juntament amb una protecció suficient de la intimitat, i permetre a les empreses operar amb la informació de manera eficient.

2.2.1 Legislació sobre protecció de dades

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

La situació actual és producte, d'una banda, de la normativa en matèria de protecció de dades i, de l'altra, de l'activitat creixent de l'**Agència Espanyola de Protecció de Dades**, organisme autònom encarregat d'assegurar el compliment de la legislació vigent (i fruit de la mateixa legislació).

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

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

Agències autonòmiques

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

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

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

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

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

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

A continuació teniu un llistat d'aquestes lleis :

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

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

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

El Reglament General de Protecció de dades (RGPD)

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

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

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

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

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

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

Què és una dada de caràcter personal?

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

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

Objectiu del reglament i principis bàsics de l'RGPD

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

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

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

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

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

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

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

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

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

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

- **Principi de qualitat de les dades**: les dades de caràcter personal només es poden recollir per al seu tractament i sotmetre's a aquest tractament quan siguin adequades, pertinents i no excessives amb relació a l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'hagin obtingut. L'RGPD exigeix reduir al mínim necessari tant el tractament de les dades com les persones autoritzades a accedir a aquestes dades.

- **Finalitat expressa**: les dades de caràcter personal objecte de tractament no poden ser usades per a finalitats que no siguin compatibles amb aquelles per

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

- **Necessitat de consentiment de la persona afectada**: el tractament de les dades requereix el consentiment de la persona afectada.
- **Actualitat de les dades**: les dades personals que s'incorporin en un fitxer han de respondre a una situació actual.
- **Principi d'exactitud**: les dades personals han de ser susceptibles de modificació i de rectificació des del moment en què se'n coneix la modificació.
- **Deure d'informació a la persona afectada**: les persones interessades a les quals se sol·licitin dades de caràcter personal hauran de ser advertides prèviament de manera expressa, precisa i inequívoca:
  - Que les seves dades seran incloses en un fitxer, de la finalitat de la recollida i dels destinataris de la informació.
  - De l'obligatorietat o voluntarietat de donar aquestes dades.
  - De les conseqüències que porten aparellades l'obtenció de les dades o de la negativa a subministrar-les.
  - De la possibilitat d'exercir els **drets d'accés, rectificació, cancel·lació i oposició** (drets ARCO).
  - De la identificació i de l'adreça de la persona encarregada de dur a terme el tractament del fitxer o, si escau, del seu representant, perquè els afectats puguin exercir els seus drets.

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

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

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

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

Cancel·lació i bloqueig de dades

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

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

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

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

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

2.2.2 Obligacions de les empreses i els implicats en els tractaments

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

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

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

Altres obligacions recollides a l'RGPD són:

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

2.2.3 Notificació de violacions de seguretat

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

El responsable del tractament

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

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

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

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

L'encarregat del tractament

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

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

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

El delegat de protecció de dades (DPD)

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

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

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

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

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

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

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

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

Altres coses a tenir en compte són:

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

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

2.2.5 Dades personals

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

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

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

Tenen la consideració de dades personals:

- Nom i cognoms, data de naixement.

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

Dades personals

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

Dades personals sensibles

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

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

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

2.2.6 Infraccions i sancions de l'RGPD

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

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

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

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

Exemple d'infracció i multa amb la nova llei

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

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

Com a conseqüència de l'expansió de les xarxes d'ordinadors i especialment d'Internet, fenòmens que abans eren habituals dins del món analògic han acabat traspassant les fronteres per esdevenir freqüents en el món virtual (per exemple, el comerç electrònic). No podem esperar que el marc jurídic actual pugui donar resposta a tots els nous reptes provocats per l'ús de les tecnologies de la informació. Per donar resposta a aquests buits legals cal ampliar o redefinir conceptes jurídics. Aquesta regulació no solament ha d'evitar el mal ús de la tecnologia (per exemple, l'enviament de correu brossa o no consentit), sinó que ha de generar un entorn de confiança en el qual es delimitin clarament les responsabilitats i els deures de cadascú, sense el qual no és possible l'establiment de transaccions, com ara el comerç electrònic.

El **comerç electrònic** o *e-commerce* consisteix en la compra i venda de productes o serveis mitjançant xarxes d'ordinadors (com, per exemple, Internet).

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

2.3.1 Concepte de serveis de la societat d'informació

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

- Contractació de béns i serveis per via electrònica.
- Subministrament d'informació per via electrònica (per exemple, els diaris digitals).
- Activitats d'intermediació relatives a:
  - La provisió d'accés a la xarxa.
  - La transmissió de dades.
  - La realització de la còpia temporal de les pàgines d'Internet sol·licitades pels usuaris.
  - L'allotjament de dades en els servidors d'informació.
  - Els serveis o aplicacions facilitats per altres.
  - La provisió d'eines de cerca.
  - Els enllaços a altres llocs d'Internet.
- Qualsevol altre servei que es presti a petició individual dels usuaris (descàrrega de fitxers de vídeo o àudio...), sempre que representi una activitat econòmica per al prestador.

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

Proveïdors de serveis

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

2.3.2 Obligacions i responsabilitat dels prestadors de serveis

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

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

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

Obligacions dels prestadors de serveis

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

La llei imposa el **deure de col·laboració dels prestadors de serveis d'intermediació** per impedir que determinats serveis o continguts il·lícits es continuïn divulgant.

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

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

Un altre aspecte destacable de la preservació dels registres és la consideració de la IP com una dada personal (tot i que no identifica directament una persona, sí esdevé un mitjà per identificar-la).

Com podíem esperar, les dades que enregistra el proveïdor de serveis s'han d'emmagatzemar garantint els drets constitucionals i amb les mesures determinades per la llei de protecció de dades. Només pot retenir les dades imprescindibles per identificar l'**origen de la connexió** i el **moment en què s'inicià la prestació del servei**. La preservació de les dades no pot atemptar en cap cas contra el secret de les comunicacions.

Règim de responsabilitats dels prestadors de serveis

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

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

Fòrum de discussió

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

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

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

allotjats, la determinació de la responsabilitat ja no és tan evident i consta de les exempcions següents:

- Si el servei consisteix en la mera transmissió de les dades proveïdes pel destinatari del servei, o en proporcionar l'accés a la xarxa, s'entén que els proveïdors desconeixen els continguts transmesos i no en són responsables, sempre que no es produeixin les situacions següents: que els prestadors no hagin originat la transmissió, que no hagin modificat ni seleccionat les dades o que no hagin seleccionat el destinatari.
- Els prestadors solen emmagatzemar en els servidors còpies automàtiques i temporals de les dades facilitades pel destinatari del servei (*caching*). En aquest cas els proveïdors tampoc no són responsables del contingut d'aquestes dades, sempre que no hagin modificat la informació.

Caching

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

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

Coneixement efectiu

Els prestadors de serveis tenen coneixement efectiu quan:

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

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

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

- Finalment, quan el prestador facilita enllaços amb continguts o inclou eines de cerca, no és responsable de la informació redirigida pels enllaços, sempre que es produeixin els requisits d'exempció, ja esmentats en l'apartat d'allotjament: quan els prestadors no tinguin coneixement efectiu que l'activitat o la informació és il·lícita o que pot lesionar béns o drets d'un

tercer susceptible d'indemnització o en cas que en tinguin coneixement, no tenen cap responsabilitat si retiren amb prestesa les dades o hi impossibiliten l'accés.

Obligacions de les empreses que fan comerç electrònic

Com a usuaris potencials del comerç electrònic, convé que conegueu les obligacions d'informació que tenen totes les empreses que es dediquen a aquesta activitat. El portal web ha de mostrar, entre d'altres, les dades següents:

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

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

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

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

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

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

2.3.3 Regulació de comunicacions publicitàries (correu brossa)

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

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

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

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

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

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

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

Seguretat activa i accés remot

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

Seguretat i alta disponibilitat

Índex

Introducció **5**

Resultats d'aprenentatge **7**

1 Mecanismes de seguretat activa **9**
1.1 Sistemes personals. Atacs i contramesures . . . 9
1.1.1 Classificació dels atacs . . . 9
1.1.2 Anatomia dels atacs . . . 15
1.1.3 Anàlisi de programari maliciós . . . 19
1.2 Eines preventives . . . 22
1.2.1 Instal·lació i configuració . . . 22
1.3 Eines pal·liatives . . . 27
1.3.1 Instal·lació i configuració . . . 27
1.4 Actualització de sistemes i aplicacions . . . 30
1.4.1 Per què cal actualitzar el sistema operatiu i les aplicacions? . . . 31
1.4.2 Com actualitzar? . . . 31
1.5 Seguretat en la xarxa corporativa . . . 32
1.5.1 Monitoratge del trànsit de xarxes . . . 32
1.5.2 Seguretat en els protocols per a comunicacions sense fil . . . 36
1.5.3 Riscos potencials dels serveis de xarxa . . . 38
1.5.4 Intents de penetració. Detecció d'intrusions . . . 44
1.6 Les xarxes públiques. Seguretat en la connexió . . . 47
1.6.1 Pautes i pràctiques segures . . . 47

2 Implantació de tècniques d'accés remot **51**
2.1 Seguretat perimètrica . . . 51
2.1.1 Elements bàsics de la seguretat perimètrica . . . 52
2.1.2 Perímetres de xarxa. Zones desmilitaritzades . . . 54
2.1.3 Arquitectura feble de subxarxa protegida . . . 57
2.1.4 Arquitectura forta de subxarxa protegida . . . 58
2.2 Xarxes privades virtuals. VPN . . . 59
2.2.1 Beneficis i inconvenients de les VPN envers les línies dedicades . . . 60
2.2.2 Nivell de xarxa a VPN: SSL, TLS i IPSec . . . 61
2.2.3 Nivell d'aplicació a VPN. L'SSH . . . 62
2.3 Servidors d'accés remot . . . 63
2.3.1 Protocols d'autenticació . . . 64
2.3.2 Configuració de paràmetres d'accés . . . 66
2.3.3 Servidors d'autenticació . . . 67

Introducció

Les tecnologies de la informació, i en especial Internet, han convertit la comunicació en un element clau i a la vegada vulnerable per part de tercers. Així, doncs, la facilitat per realitzar tasques de manera remota i per comunicar-nos s'han d'equilibrar amb la seguretat en aquestes comunicacions. Una gestió incorrecta del trànsit i accés d'aquesta informació pot ocasionar l'exposició, la còpia o l'esborrat de dades sensibles i pot provocar la pèrdua del sistema d'informació i, en conseqüència, la paralització de l'activitat de l'organització i grans pèrdues econòmiques.

Al llarg d'aquest mòdul heu treballat diversos conceptes tècnics i legals relacionats amb la seguretat informàtica. En aquesta unitat, però, veureu com es poden classificar els atacs a sistemes informàtics i quines mesures, ja siguin mitjançant programari o maquinari, es poden adoptar per minimitzar-ne els efectes. Aprendreu que un sistema d'informació pot ser "proactiu" i que amb un conjunt de mesures de seguretat adient es pot pal·liar una de les problemàtiques actuals; l'accés a la informació a través de xarxes insegures o públiques, com és el cas d'Internet.

En l'apartat "Mecanismes de seguretat activa" es descriuen els elements que permeten identificar els atacs, així com les eines per prevenir-los. Conèixer els tipus d'atac us permetrà prevenir-los, detectar-los i evitar-los.

En l'apartat "Implantació de tècniques d'accés remot" s'expliquen el conjunt de configuracions de seguretat, ja siguin de programari, de maquinari o mixtes, que permeten l'accés segur a la xarxa d'informació des de l'exterior.

Al llarg de la unitat veureu que la seguretat està orientada a evitar incidents i a minimitzar-ne els efectes si succeeixen. Us adonareu que aquests incidents tant poden provenir de l'exterior de la xarxa com de l'interior i que, per tant, cal preveure tots els escenaris possibles.

La unitat descriu, des d'un vessant pràctic i teòric, aspectes essencials de la seguretat informàtica. Aquesta es pot entendre com un fenomen "en capes": la de l'ordinador de sobretaula, la dels servidors, la de la xarxa LAN, la dels punts de connexió amb xarxes insegures i la de la interconnexió de xarxes, coneguda com a Internet. Per treballar els continguts d'aquesta unitat didàctica és convenient anar fent les activitats i els exercicis d'autoavaluació, així com llegir els annexos.

Resultats d'aprenentatge

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

1. Implanta mecanismes de seguretat activa, seleccionant i executant contramesures enfront d'amenaces o atacs al sistema.
    - Classifica els principals tipus d'amenaces lògiques contra un sistema informàtic.
    - Verifica l'origen i l'autenticitat de les aplicacions instal·lades en un equip, així com l'estat d'actualització del sistema operatiu.
    - Identifica l'anatomia dels atacs més habituals, així com les mesures preventives i pal·liatives disponibles.
    - Analitza diversos tipus d'amenaces, atacs i programari maliciós, en entorns d'execució controlats.
    - Implanta aplicacions específiques per a la detecció d'amenaces i l'eliminació de programari maliciós.
    - Utilitza tècniques de xifrat, signatures i certificats digitals en un entorn de treball basat en l'ús de xarxes públiques.
    - Avalua les mesures de seguretat dels protocols usats en xarxes sense fil.
    - Reconeix la necessitat d'inventariar i controlar els serveis de xarxa que s'executen en un sistema.
    - Descriu els tipus i característiques dels sistemes de detecció d'intrusions.
2. Implanta tècniques segures d'accés remot a un sistema informàtic, interpretant i aplicant el pla de seguretat.
    - Descriu escenaris típics de sistemes amb connexió a xarxes públiques en els quals es precisa fortificar la xarxa interna.
    - Classifica les zones de risc d'un sistema, segons criteris de seguretat perimètrica.
    - Identifica els protocols segurs de comunicació i els seus àmbits d'utilització.
    - Configura xarxes privades virtuals mitjançant protocols segurs a diferents nivells.
    - Implanta un servidor com a passarel·la d'accés a la xarxa interna des d'ubicacions remotes.
    - Identifica i configura els possibles mètodes d'autenticació en l'accés d'usuaris remots a través de la passarel·la.
    - Instal·la, configura i integra en la passarel·la un servidor remot d'autenticació.

1. Mecanismes de seguretat activa

La protecció de la informació és la conseqüència de l'aplicació d'un conjunt de mecanismes o estratègies de seguretat. A grans trets, aquestes estratègies han de considerar els principis següents:

- La seguretat ha de ser un objectiu global.
- La seguretat s'ha de dissenyar com quelcom que és part de l'organització, tenint en compte tots aquells aspectes que la puguin conformar.
- El marc legal s'ha de considerar, des de l'inici, com una part més del disseny de les polítiques de seguretat.

La gestió i planificació de tota la seguretat és clau. En cas contrari, res del que es faci tindrà un objectiu final, i per tant, només millorarà parcialment la seguretat. A més, la gestió no només és necessària en la implantació de la seguretat, sinó també en el seu control i manteniment.

Tallafoc

Un tallafoc és un exemple de **seguretat activa**. Filtra l'accés a certs serveis en determinades connexions per bloquejar un intent d'atac. Un altre exemple de seguretat activa pot ser l'ús de contrasenyes.

Entenem per **seguretat activa** tots aquells mecanismes i mesures (físics i lògics) que permeten prevenir i detectar possibles intents de comprometre els components d'un sistema informàtic.

Per **seguretat passiva** entenem el conjunt de mesures implementades en els sistemes per minimitzar els efectes d'un incident i mantenir informats els administradors sobre les incidències que puguin comprometre la seguretat.

Són exemples de **seguretat passiva** un sistema de detecció d'intrusos o la realització de còpies de seguretat.

1.1 Sistemes personals. Atacs i contramesures

Amb la revolució tecnològica dels darrers anys els sistemes personals han esdevingut part de la nostra vida. Les tauletes tàctils, els mòbils, les PDA, els ordinadors portàtils i, fins i tot, els equips personals de sobretaula estan, d'una o altra manera, connectats a xarxes de transmissió d'informació i són, per tant, susceptibles de patir atacs per part de tercers.

1.1.1 Classificació dels atacs

La protecció d'un sistema informàtic no només s'ha d'adreçar al maquinari i al programari, sinó també a les dades, tant si es troben circulant per una xarxa com si estan emmagatzemades en un disc dur o en altres suports. Pensem que si bé

gairebé sempre és possible substituir el maquinari o el programari, les dades, objectiu primordial de tot sistema informàtic, no tenen substitut en cas que es perdin definitivament.

Els atacs que es poden produir en un sistema informàtic es poden classificar segons l'objectiu de l'atac, segons la forma de l'atac i segons el tipus d'atacant, entre d'altres formes.

Classificació segons l'objectiu de l'atac

Els atacs que pot patir el maquinari, el programari i les dades es poden classificar en quatre grans grups:

- **Interrupció**: atac contra la disponibilitat en el qual es destrueix, o queda no disponible, un recurs del sistema (per exemple, tallar una línia de comunicació o deshabilitar el sistema de fitxers del servidor).

- **Intercepció**: atac contra la confidencialitat en el qual un element no autoritzat aconsegueix l'accés a un recurs. Aquest tipus d'atac no es limita a possibles usuaris que actuïn com a espies en la comunicació entre emissor i receptor. Per exemple, un procés que s'executa subreptíciament en un ordinador i que emmagatzema en un fitxer les tecles que prem l'usuari que utilitza el terminal (*keylogger*), també constituiria un atac d'intercepció.

Atac de denegació de servei

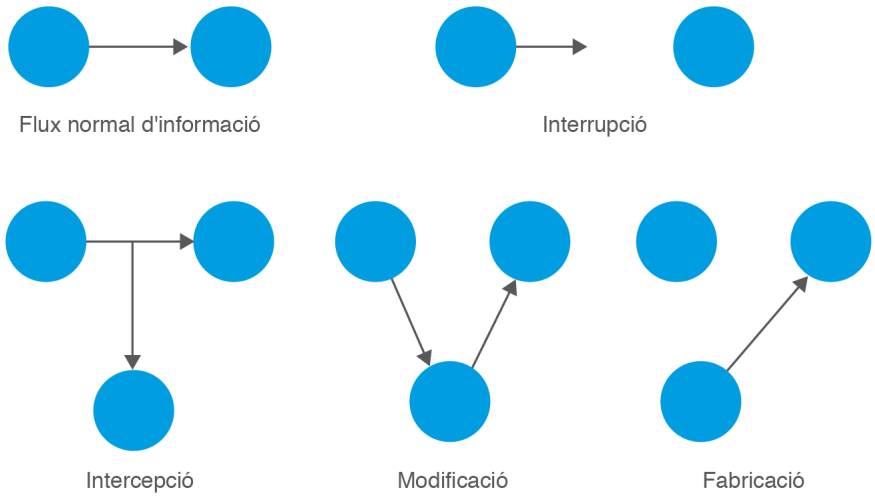
Un exemple característic d'atac d'interrupció és l'atac de denegació de servei, en el qual s'inutilitza el maquinari o programari de manera que no siguin accessibles des de la xarxa.

- **Modificació**: atac contra la integritat en el qual, a més d'aconseguir l'accés no autoritzat a un recurs, també s'aconsegueix modificar-lo, esborrar-lo o alterar-lo de qualsevol manera. Els atacs fets pels intrusos (esborrament de bases de dades, alteració de pàgines web...) són exemples d'aquesta modalitat d'atac.

- **Fabricació**: atac contra la integritat en el qual un element aconsegueix crear o inserir objectes falsificats en el sistema (per exemple, afegir de manera no autoritzada un nou usuari i la contrasenya corresponent al fitxer d'usuaris).

A la figura 1.1 es pot observar una representació gràfica d'aquesta classificació.

Figura 1.1. Tipus d'atacs que pot patir la comunicació entre emissor i receptor



Classificació segons la forma de l'atac

Els atacs provinents de persones es poden classificar en dos grans grups:

- Atacs passius
- Atacs actius

Atacs passius
L'atacant no modifica ni destrueix cap recurs del sistema informàtic, simplement l'observa, normalment amb la finalitat d'obtenir alguna informació confidencial.

Sovint, aquest atac es produeix sobre la informació que circula per una xarxa. L'atacant no altera la comunicació, sinó que senzillament l'escolta i obté la informació que es transmet entre l'emissor i el receptor. Com que la informació que es transmet no resulta alterada, la detecció d'aquest tipus d'atac no és fàcil. Una manera molt eficaç de resoldre aquest problema és usar tècniques criptogràfiques per fer que la informació no es transmeti en text clar i no sigui comprensible per als espies.

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

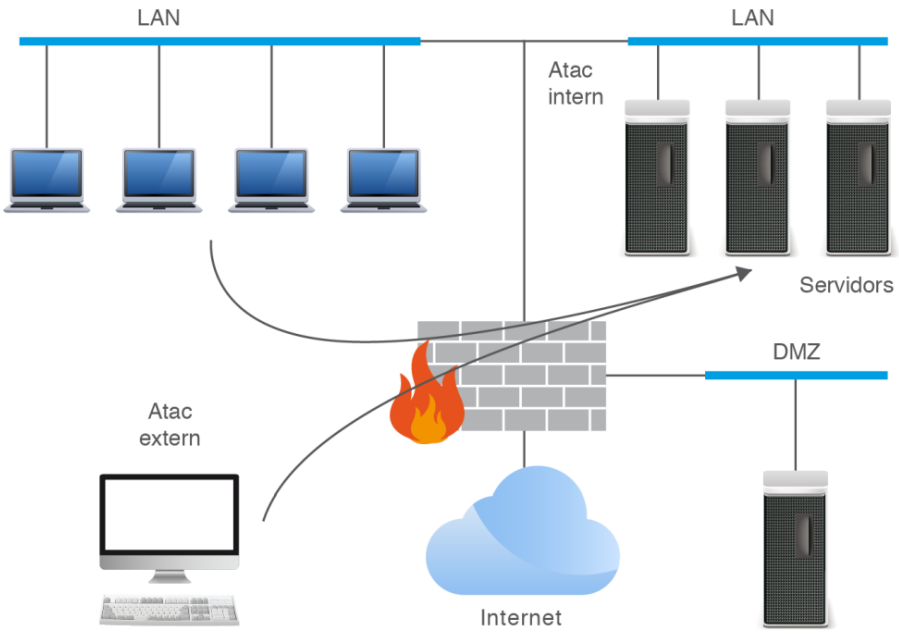
Atacs actius
En una acció d'aquest tipus, l'atacant altera o destrueix algun recurs del sistema.

Un espia que monitora una xarxa podria causar problemes molt seriosos, com els que exposem a continuació:
Suplantació d'identitat: l'espia pot suplantar la identitat d'una persona i enviar missatges en nom seu.
Reactuació: un o diversos missatges legítims són interceptats i reenviats diverses vegades per produir un efecte no desitjat (per exemple, intentar repetir diverses vegades un ingrés en un compte bancari).
Degradació fraudulenta del servei: l'espia evita el funcionament normal dels recursos del sistema informàtic. Per exemple, podria interceptar i eliminar tots els missatges que s'adrecen a un usuari determinat.
Modificació de missatges: es modifica una part del missatge interceptat i es reenvia a la persona a qui anava adreçat originalment.

Classificació segons el tipus d'atacant

La major part dels atacs que pot patir un sistema informàtic es produeixen en mans de persones que, amb diversos objectius, intenten accedir a informació confidencial, destruir-la o aconseguir el control absolut del sistema atacat. Cal tenir present que un atac pot provenir tant de l'interior de la xarxa (*insiders*) com de l'exterior (*outsiders*). Es pot veure esquemàticament a la figura 1.2.

Figura 1.2. Representació esquemàtica de com es realitzen els atacs per part d'insiders i outsiders



Acostumem a pensar que la gran majoria dels atacs provenen de l'exterior de l'organització i que són escassos, però les estadístiques demostren tot el contrari. La realitat és que:

- Els atacs externs són més nombrosos que els interns.
- El percentatge d'èxit en els atacs interns és més elevat.
- El dany causat per atacs interns és molt més gran que el provocat per atacs externs.

Conèixer els objectius dels atacants i les seves motivacions és essencial per prevenir-ne i detectar-ne les accions. Els principals possibles atacants d'un sistema informàtic són:

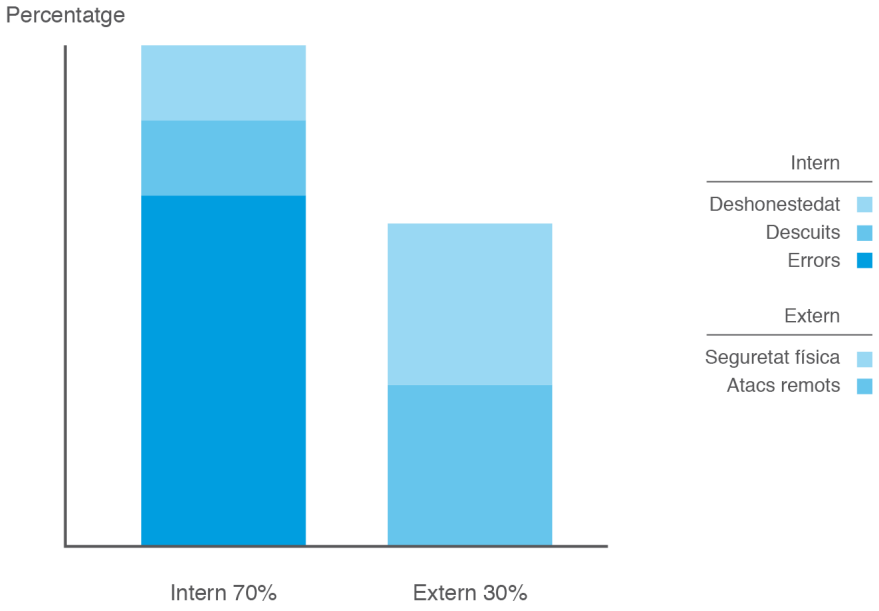
- Personal de la mateixa organització
- Antics treballadors
- Intrusos informàtics (*hackers*)
- Intrusos remunerats

Personal de la mateixa organització
Tot i que normalment el personal intern gaudeix de la confiança de l'organització, cal tenir en compte que alguns atacs es poden produir des de dins mateix de la institució. Sovint no cal que aquests atacs siguin intencionats (tot i que, quan ho són, són els més devastadors que es poden produir); poden ser accidents provocats pel desconeixement del personal (per exemple, el formatat accidental d'un disc dur).

Les tècniques bàsiques o contramesures per minimitzar els riscos d'atacs d'aquest tipus són:

- Assegurar-se que els usuaris amb permisos administratius són persones de confiança.
- Limitar la quantitat de permisos que una única persona posseeix.
- Limitar al màxim el nombre de persones amb permisos de confiança.
- Cercar escletxes de seguretat en els permisos.
- Definir una bona política de formació (pel que fa a la seguretat) per a tot el personal de l'organització.
- Impossibilitar que els usuaris sense privilegis puguin instal·lar programes (la majoria d'usuaris d'una organització no necessiten instal·lar programes, ja que per a la seva feina només necessiten els recursos o programes que els proporciona l'organització).
- Deshabilitar el ports USB per evitar la fuita d'informació (o proveir mecanismes criptogràfics que evitin l'extracció en text clar de la informació del sistema).

FIGURA 1.3. Percentatge i tipus d'atacs en una organització (www.cybsec.com)



.

Antics treballadors

Una part molt important dels atacs a sistemes informàtics són els fets per antics treballadors que, abans de marxar acomiadats o descontents per les condicions laborals, instal·len programes maliciosos com, per exemple, virus o bombes lògiques que s'activen en la seva absència (per exemple, quan arriba una data determinada). La presència d'aquest tipus de programa no sempre és fàcil de detectar, però almenys sí que es poden evitar els atacs que l'antic treballador pugui dur a terme des de fora amb el nom d'usuari i la contrasenya de què disposava quan encara treballava a l'organització (aquesta situació és més freqüent del que ens pensem). Per tant, una bona contramesura per a aquest problema és donar de baixa tots els comptes de l'extreballador i canviar les contrasenyes d'accés el sistema al més aviat possible. Així mateix, es poden proveir mecanismes d'autenticació més forts que no pas l'ús de només un nom d'usuari i contrasenya, per exemple, mitjançant un testimoni de seguretat.

Testimonis de seguretat

Els testimonis de seguretat o *security tokens* són 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 inici de sessió o cada cert temps).

Intrusos informàtics (hackers)

Els intrusos informàtics normalment duen a terme atacs passius destinats a obtenir informació confidencial (per exemple, un examen d'un curs) o amb la finalitat de posar-se a prova per obtenir el control del sistema atacat. Si l'atacant és prou hàbil, fins i tot pot esborrar les empremtes de les seves accions en els fitxers que les enregistren. Com que aquest tipus d'accions no produeixen cap efecte visible, no són fàcilment detectables.

Hackers i crackers

Quan la finalitat de la intrusió és destructiva, la persona que fa l'acció rep el nom de *cracker* (pirata). La nostra intenció no és diferenciar entre *hackers* i *crackers*, de manera que s'utilitzarà el terme intrús en relació amb qualsevol tipus d'intrusió, sigui o no destructiva. La mera intrusió en un sistema informàtic pot ésser considerada un delicte, amb independència que es produeixin o no danys en el sistema.

Els intrusos solen aprofitar les vulnerabilitats conegudes de sistemes operatius i programaris per aconseguir el control de tot el sistema informàtic. Per dur a terme aquest tipus d'accions n'hi ha prou d'executar diversos programes que es poden

obtenir a Internet i que automatitzen els atacs als sistemes informàtics sense que l'intrús necessiti disposar de gaires coneixements tècnics.

A vegades, l'únic interès de l'intrús és deixar una empremta de la seva "habilitat" per introduir-se en els sistemes sense autorització. Així, és relativament freqüent que modifiqui, per exemple, un lloc web (*defacement*) i hi deixi el seu pseudònim. No oblidem, però, que aquesta activitat és un delicte de danys recollit en el Codi Penal.

A més d'eines de caràcter tècnic, els intrusos disposen d'altres estratègies més senzilles (almenys des del punt de vista informàtic), però igual d'efectives. Per exemple, poden fer una senzilla recerca de contrasenyes escrites en papers entre la brossa continguda en una paperera (*trashing*) o en les notes adhesives que hom sol enganxar al monitor d'un terminal de treball, o emprar qualsevol tècnica d'enginyeria social.

Enginyeria social

L'enginyeria social és la pràctica d'obtenir informació confidencial mitjançant la manipulació i engany dels posseïdors legítims d'aquesta informació.

Intrusos remunerats

Tot i no ser gaire freqüent, també val la pena tenir en compte l'atac d'intrusos remunerats. En aquest cas, els intrusos estan perfectament organitzats (poden estar en diferents localitzacions geogràfiques fins i tot) i ataquen de manera coordinada una entitat determinada. Disposen de molts mitjans tècnics i reben remuneracions molt elevades de l'organisme rival que dirigeix l'atac, sovint amb l'ànim d'accedir a informació confidencial (un nou disseny, un nou programari...) o bé de provocar un dany important en la imatge de l'entitat atacada.

Atacs distribuïts

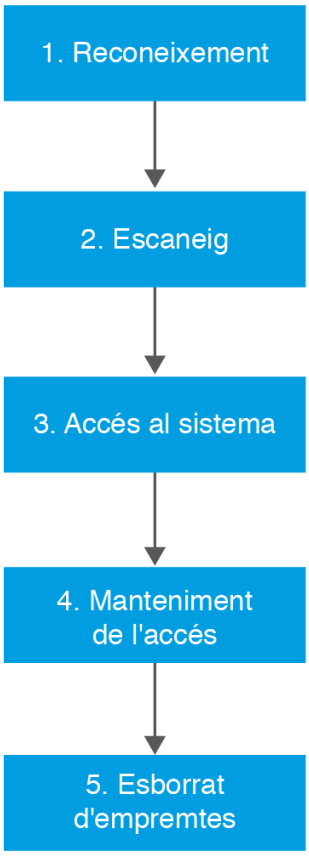
La preparació i realització d'un atac informàtic consta de diverses fases, algunes d'elles molt tècniques. Per aquest motiu, alguns atacs es realitzen de forma distribuïda, de manera que cada membre de la coalició efectua unes determinades fases o accions de l'atac.

1.1.2 Anatomia dels atacs

Els atacs informàtics solen constar d'un cicle de cinc fases (figura 1.4):

1. Reconeixement
2. Escaneig
3. Accés al sistema
4. Manteniment accés
5. Esborrat empremtes

Figura 1.4. Fases d'un atac informàtic



Cal diferenciar entre l'**atac informàtic** i el **delicte informàtic**. No obstant això, les conseqüències dels atacs informàtics poden estar recollides en el Codi Penal.

El coneixement del funcionament intern d'un atac informàtic ens ajuda a avançar-nos als esdeveniments i preveure activitats que podrien comprometre el nostre sistema informàtic.

Fase 1: reconeixement

Aquesta primera fase té caràcter preparatori i consisteix en la recopilació, per part de l'atacant, de tota la informació possible del sistema que pretén comprometre. No oblidem que l'atacant pot tenir tot el temps del món per preparar la seva estratègia, mentre que nosaltres només ens podem preparar de forma general per evitar i minimitzar les conseqüències d'un atac.

L'atacant pot utilitzar diverses tècniques a l'hora de reconèixer un sistema. Per exemple, pot emprar enginyeria social o *trashing*, amb la finalitat d'aconseguir informació valuosa per accedir al sistema. Fixem-nos que, en cas d'emprar tècniques d'enginyeria social, l'atacant ni tan sols hauria hagut d'emprar cap mètode informàtic per obtenir la informació que desitja.

Sniffing

El monitoratge d'una xarxa (*sniffing*) no és, en si mateix, una conducta delictiva. No oblidem que aquests tipus d'eines són emprades lícitament pels administradors de sistemes informàtics.

Altres tècniques pròpies d'aquesta fase són:

- Fer recerques a Internet (notem que, normalment, la informació corporativa de la nostra organització, ha de ser visible a la xarxa per motius comercials

i, per tant, es pot localitzar fàcilment). En tot cas, cal ser curós amb la informació que es mostra a la xarxa i deixar, en la mesura del possible, només aquella que sigui necessària pel funcionament de l'organització i que no pugui comprometre la seguretat del sistema.

- Capturar el trànsit de xarxa (*sniffing*).
- Utilitzar l'ordre whois per esbrinar dades relatives al sistema que volem investigar (per exemple, l'empresa que va enregistrat un domini determinat, o la seva adreça). Les bases de dades consultades per whois (la consulta també es pot fer mitjançant diversos webs) són públiques i, tot i que aquesta informació es podria emprar de forma maliciosa, pot ser molt útil, per exemple, per saber si un domini determinat està disponible.

Fase 2: escaneig

En aquesta fase, l'atacant utilitzarà tota la informació obtinguda en l'apartat anterior per sondejar el sistema que pretén atacar i detectar una vulnerabilitat (o vulnerabilitats) específica, que pugui aprofitar per accedir al sistema (per exemple, una vulnerabilitat del sistema operatiu que usa el sistema objectiu, una vulnerabilitat d'una aplicació...).

En definitiva, l'atacant intentarà, principalment, obtenir informació dels comptes d'usuari, de les versions del sistema operatiu i de les aplicacions, així com els ports oberts. Moltes eines d'administració de sistemes es poden emprar en aquesta fase amb finalitats il·lícites, com per exemple els escàners de xarxa o de ports (***nmap*** executat a la figura 1.5).

Figura 1.5. Exemple d'ús de l'ordre nmap

```
root@ubuntu:/home/user# nmap localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2012-05-06 18:33 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1711 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.565 seconds
```

L'eina *nmap* no serveix únicament per conèixer els ports que té oberts una màquina, sinó que també es pot emprar per identificar la seva adreça MAC o el sistema operatiu que utilitza, entre altres utilitats.

Hi ha moltes més eines que es poden emprar en aquesta fase. D'entre elles, podríem destacar, per exemple, les ordres ***tracert*** en entorns Windows o ***traceroute*** en entorns Linux/Unix. Aquesta ordre es pot emprar per esbrinar els canvis de xarxa que realitzen els paquets per la xarxa fins arribar a la seva destinació.

Cal tenir en compte que aquestes eines, vistes aquí amb finalitats malicioses, tenen moltíssima utilitat per l'administrador del sistema i que, per tant, el seu ús principal és lícit.

Vulnerabilitat

S'entén per *vulnerabilitat* qualsevol punt feble que pugui posar en perill la seguretat d'un sistema informàtic. Aquesta feblesa s'ha d'entendre com una qüestió interna (latent) del sistema. Pot ser aprofitada per un atacant per violar la seguretat del sistema informàtic o simplement pot provocar danys de manera no intencionada (per exemple, un error de programació pot fer que un programari tingui comportaments irregulars i insospitats).

Exploits

Els exploits són programes maliciosos (entren dins de la categoria de les anomenades amenaces lògiques) que aprofiten una vulnerabilitat (coneguda o no) d'un programari informàtic, conseqüència d'un error de programació. No existeix un exploit general, sinó que cada programa, a causa dels gairebé inevitables errors de programació, té les seves peculiars vulnerabilitats, que poden ser hàbilment explotades pels programadors experimentats (si bé a Internet es poden trobar exploits per violar la seguretat de tota mena d'aplicacions i sistemes operatius sense necessitat de tenir coneixements de programació).

Port

Un port és un punt pel qual entra o surt la informació d'un ordinador. Els protocols relatius a Internet (FTP, Telnet...) utilitzen emissor i receptor, un port de sortida i recepció comú en ambdós extrems de la comunicació.

Nessus

Nessus és un conegut programa d'escaneig de vulnerabilitats. Escaneja els ports i prova exploits per atacar el sistema que s'està escanejant.

Fase 3: obtenció de l'accés

Aquesta és la fase en la qual es duu a terme l'atac de manera efectiva, aprofitant les vulnerabilitats localitzades a la fase anterior.

Sovint, aquesta fase es desenvolupa atacant, des de la xarxa, l'equip objectiu, però poden haver-hi parts de l'atac que s'efectuïn localment, en el sistema de l'atacant (per exemple, el trencament d'un fitxer de contrasenyes).

La realització d'un atac no sempre requereix coneixements elevats: Internet proveeix molta informació i *exploits*, que es poden, malauradament, emprar sense necessitat de saber programar o de tenir grans coneixements informàtics. Òbviament, les mesures de seguretat de què disposi l'equip objectiu són essencials per evitar l'èxit dels atacants. Si hom té un sistema molt assegurat i actualitzat, la informació d'ús comú a la xarxa serà clarament insuficient per perpetrar una intrusió amb èxit.

Fase 4: manteniment de l'accés

Una vegada l'intrús ha obtingut l'accés al sistema, intentarà preservar la possibilitat d'efectuar nous accessos en el futur. En aquesta tasca l'ajudaran diversos programes de codi maliciós, com els cavalls de Troia i els *rootkits*. No és només la possibilitat de causar danys evidents al sistema (esborrat de fitxers, per exemple) el que ens ha d'inquietar; l'atac també pot servir per instal·lar *malware* que monitori les accions que estem fent (*keylogger*), per capturar tot el trànsit de la xarxa (*sniffing*), instal·lar un FTP de contingut il·lícit o utilitzar el sistema atacat com a plataforma per atacar altres sistemes informàtics.

Una xarxa de zombis

Una xarxa de zombis o botnet està formada per un grup d'ordinadors (fins i tot milers) connectats a la xarxa, infectats per codi maliciós que permet el seu control remot per part d'un atacant o grup d'atacants. Les botnets poden ésser emprades per realitzar accions sense l'autorització dels propietaris de les màquines infectades, com ara atacs massius sobre altres sistemes informàtics (atacs de denegació de servei distribuït o DDoS).

Rootkits

Els *rootkits* (terme que prové d'unir la paraula anglesa root, que és el nom assignat a Unix al compte de màxims privilegis i kit que significa conjunt d'eines o programes) són eines informàtiques emprades normalment amb finalitats malicioses (com l'obtenció d'informació) que permeten l'accés il·lícit al sistema per part d'un atacant remot. Fan servir tècniques per ocultar la seva presència i la d'altres processos que puguin estar realitzant accions malicioses sobre el sistema. Els *rootkits* són molt perillosos, perquè cedeixen el control del sistema a l'atacant remot.

Fase 5: esborrat de les empremtes

És vital per a l'intrús esborrar les empremtes del que ha fet en el sistema. Moltes de les accions que ha dut a terme segurament hauran quedat, amb independència del sistema operatiu emprat, enregistrades en fitxers de registre (*log*). Alguns d'ells són fàcilment editables, però d'altres no ho són tant, ja que no són fitxers de text. En definitiva, el que intentarà l'intrús és eliminar totes aquestes entrades del fitxers de *log* i registres d'alarmes de les eines de detecció d'intrusos (IDS) amb la finalitat que els administradors del sistema no puguin descobrir que algú s'hi ha introduït de manera no autoritzada.

Els **detectors d'intrusos** o IDS s'expliquen amb més detall en l'apartat "Intents de penetració. Detecció d'intrusos" d'aquesta mateixa unitat formativa.

1.1.3 Anàlisi de programari maliciós

Per *programari maliciós* s'entén qualsevol programa que pugui tenir efectes perniciosos en el sistema informàtic que l'allotja. El seu nom anglès, *malware*, prové de la contracció de *malicious software*. Els virus, cucs i cavalls de Troia són exemples típics de programari maliciós.

Sovint, el codi maliciós s'insereix dins d'un programa "autoritzat" i executa una sèrie d'accions desconegudes per l'usuari, les quals actuen normalment en detriment seu. El codi maliciós pot estar ocult i provocar tota mena de danys com, per exemple, l'esborrament de dades o l'enviament d'informació confidencial de l'usuari per correu electrònic. En altres ocasions, el codi maliciós no s'insereix dins d'un programa autoritzat, sinó que es presenta com un nou programa que desenvolupa alguna funció útil. L'usuari l'executa, esperant que implementi aquesta funció, però el programa, en canvi, duu a terme accions desconegudes i normalment pernicioses per a l'usuari.

Amenaces lògiques

El codi maliciós, en totes les seves múltiples variants, es pot enquadrar dins el que s'anomenen amenaces lògiques.

Si bé s'ha de retrocedir fins a l'any 1972 per trobar el que s'ha considerat el primer virus de la història (anomenat Creeper, infectava màquines de l'Arpanet, xarxa antecedent de l'actual Internet), no va ser fins a la dècada dels anys vuitanta que es van començar a desenvolupar i a convertir en un greu problema de seguretat.

Fins a l'any 2005, el codi maliciós es va estendre per la xarxa sobretot en forma de virus, cucs i cavalls de Troia. El seu objectiu era, simplement, causar danys o aportar als seus creadors un cert reconeixement públic. No obstant això, a partir d'aquell moment, apareix un nou objectiu: guanyar diners. Així, els cavalls de Troia sovint persegueixen la captura de les dades bancàries de les operacions efectuades en els ordinadors personals infectats. A més de conceptes nous, com els programes de publicitat (*adware*) i els programes espia (*spyware*), apareix un nou tipus d'engany, la pesca electrònica (*phishing*), també centrada en l'obtenció de diners, però basada en l'enginyeria social.

Programari de publicitat

Es defineix com programari de publicitat o *adware* el programari que mostra publicitat. Per exemple, les versions de demostració d'alguns programaris poden ensenyar publicitat diversa (d'aquí ve que siguin gratuïtes o de demostració). Encara que normalment s'instal·len sense el consentiment de l'usuari, no són maliciosos.

Programa espia

Es defineix com programa espia o *spyware* el programa que recull informació sobre els hàbits dels usuaris sense el seu consentiment. Aquesta recaptació es pot dur a terme amb finalitat publicitària o bé per capturar informació personal.

Els cavalls de Troia bancaris es propaguen normalment, fins i tot en l'actualitat, per mitjà del correu electrònic (encara que es poden difondre d'altres formes, com per exemple a través de dispositius USB) i es basen en l'enginyeria social per persuadir l'usuari que executi el fitxer maliciós. Les dades capturades pel codi maliciós s'envien per correu electrònic a l'atacant, que intentarà fer-ne ús en benefici propi. Per obtenir un guany econòmic significatiu, cal que l'atacant o grup d'atacants infecti el major nombre possible de màquines, de forma completament indiscriminada. Altres codis maliciosos, però, tenen un objectiu molt més concret i específic (una determinada organització, per exemple). En aquests casos es poden arribar a dissenyar de manera específica. Això suposa un elevat cost de desenvolupament, si bé el benefici econòmic esperat pot arribar a ser molt elevat.

Pesca electrònica

La pesca electrònica o *phishing* és una estratègia d'enginyeria social, en la qual s'usa la suplantació de correus electrònics o llocs web per intentar obtenir informació confidencial de l'usuari.

El sistema operatiu que més ha patit l'atac del codi maliciós és Windows, si bé també se n'ha desenvolupat per a la resta de sistemes, no tan majoritaris com aquesta plataforma. Darrerament s'observa una clara tendència al desplaçament d'aquest problema de seguretat als terminals de telefonia mòbil, cada vegada més sofisticats i vulnerables a l'acció del codi maliciós.

Detecció del codi maliciós

A continuació estudiarem algunes de les tècniques que es poden fer servir per detectar i prevenir la presència de codi maliciós en el nostre sistema informàtic. Segons la configuració del sistema, la detecció del codi (normalment fitxers compilats) serà més o menys complicat. Per exemple, si es coneix la darrera data d'actualització del sistema i es localitza algun fitxer de sistema posterior a aquesta data, es pot pensar en la presència de codi maliciós. En aquest sentit, pot ser de molta ajuda l'observació dels paràmetres següents:

- Darrera data de modificació dels fitxers.
- Data de creació dels fitxers.
- Mida dels fitxers.

Malauradament, les dates i mides dels fitxers es poden alterar amb facilitat i, per tant, no són una font d'informació segura. Les funcions *hash* ens poden ser de molta utilitat per garantir la integritat del sistema.

Les **funcions resum o *hash*** permeten obtenir el que podríem anomenar una *empremta* única d'un fitxer o conjunt de fitxers (com un ADN del fitxer). Podeu trobar més informació a l'apartat de criptografia de la unitat "Seguretat física, lògica i legislació"

Així, l'administrador pot generar en qualsevol moment una instantània o empremta *única* del sistema informàtic fent servir funcions *hash*. Qualsevol alteració d'un fitxer, per mínima que sigui, provocarà que quan l'administrador torni a calcular la funció *hash*, obtingui un resultat diferent. L'eina més coneguda per dur a terme aquesta funció rep el nom de **Tripwire** (és una eina de font pública basada en Linux/Unix). El seu funcionament és el següent: una vegada s'ha instal·lat el sistema operatiu, s'obté un valor *hash* per a cadascun dels fitxers rellevants i s'emmagatzema en una base de dades, l'accés a la qual està protegit per contrasenya.

Quan l'administrador vol comprovar la integritat del sistema, executa Tripwire i si s'ha produït algun canvi en algun fitxer, es generarà el senyal d'avís corresponent en el fitxer de sortida de l'aplicació. El funcionament correcte d'aquest procediment només es pot garantir si la base de dades on es guarden les sortides resum no és modificable per cap usuari. Això es pot aconseguir fent que la base de dades tingui atribut de només lectura, o emmagatzemant-la en un suport que no admeti reescriptures com, per exemple, un DVD.

Amb eines com Tripwire es poden detectar els fitxers de sistema als quals s'ha inserit codi maliciós, és a dir que es pot garantir la integritat dels fitxers del sistema, però no ens permet analitzar en línia la presència de programari maliciós, ni ens permet fer una anàlisi, per exemple, dels programes que ens descarreguem d'Internet. Per a aquest tipus d'anàlisis caldrà recórrer als antivirus.

Els **antivirus** són objecte d'estudi a l'apartat "Eines pal·liatives" d'aquesta mateixa unitat.

Anàlisi del codi maliciós

Un dels problemes més greus que podem trobar a l'hora d'analitzar un determinat *malware* és la possibilitat que la mateixa anàlisi impliqui la infecció d'altres equips a través de la xarxa. A grans trets, es realitza preparant l'entorn, recollint la informació i finalment analitzant i documentant el que s'ha recollit.

Preparació d'un medi d'anàlisi controlat

Així, doncs, abans d'iniciar l'anàlisi és important disposar dels mitjans que ens permetin veure quines accions realitza el codi maliciós sense possibilitat d'afectar cap altre equip. Per aquest motiu, procurarem que la màquina amb la qual hem de provar el presumpte codi maliciós estigui desconnectada de la nostra xarxa de treball habitual. No cal disposar d'ordinadors específics i construir una xarxa dedicada a l'anàlisi, ja que, sortosament, els programes de virtualització ens permeten crear un laboratori de màquines i xarxes virtuals sense gaire dificultat i amb un alt grau de control. No obstant això, si disposem dels recursos suficients, sempre podem definir una xarxa específica i aïllada de la resta d'ordinadors.

Cal, doncs, definir dues o més màquines virtuals, en xarxa, amb una instal·lació bàsica de sistema operatiu, una de les quals, la que actua de màquina atacada, allotja el presumpte codi maliciós. A més, han de tenir instal·lades diverses eines que ens permetran analitzar què està passant quan s'activi el codi maliciós. Per exemple, un programa de monitoratge de trànsit de xarxa, com ara **Wireshark**, pot ser de molta utilitat.

Els dos programes de virtualització d'ús més freqüent són VMWare i VirtualBox.

Abans d'iniciar l'anàlisi, també és interessant recollir certes dades del sistema, prèvies a la infecció, com ara quins són els ports oberts, els processos en execució, usuaris i grups definits, quins són els recursos compartits...

Eines com Sysinternals o ***nmap*** ens poden ajudar en aquesta tasca.

Recollida d'informació

Una vegada s'ha executat el *malware*, s'efectua una nova recollida d'informació, adreçada a l'estudi del codi maliciós i als efectes que provoca.

- **Recollida estàtica**. Relacionada directament amb el codi malicós objecte d'estudi: nom del fitxer, versió, com és la interfície gràfica (si és que en té)...

- **Recollida dinàmica**. Es basa en els efectes que produeix el codi maliciós: anàlisi del trànsit de xarxa, processos en execució, canvis en el sistema de fitxers...

Anàlisi i documentació de la informació

Totes les proves efectuades s'han d'analitzar (tinguem present que hi pot haver un volum d'informació molt gran) i documentar amb la finalitat que els resultats obtinguts serveixen per prevenir atacs de *malware* com l'estudiat o semblant.

Aquesta metodologia, centrada en l'estudi en un medi controlat, no és el que habitualment ens trobarem. L'escenari habitual és un sistema informàtic que, de vegades, ni tan sols sabrem si es troba o no infectat, tot i que una sèrie d'indicis ens ho fan pensar. No obstant això, la metodologia explicada també resulta de molta utilitat en aquests casos.

1.2 Eines preventives

Per *eines preventives* entenem totes aquelles eines i mecanismes que ens ajudin a reforçar la seguretat i a detectar febleses en el nostre sistema.

1.2.1 Instal·lació i configuració

Els danys que es poden produir en el cas d'un atac poden ser desastrosos. Així doncs, és necessari instal·lar eines i configurar mecanismes amb l'objectiu de minimitzar els atacs reeixits. Aquests mecanismes i eines poden anar orientats a l'usuari, a l'equip o al sistema informàtic.

Polítiques de seguretat de contrasenyes

Quan hem de triar una contrasenya per a un compte d'usuari, sovint la definim de la forma més òbvia i senzilla de recordar per nosaltres. Hem de tenir en compte, però, que en fer-ho així, podem comprometre la seguretat del sistema informàtic. Per definir correctament una contrasenya, hauríem de prendre les precaucions 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, per idiomes, de temes concrets com esports... Aquestes tècniques reben el nom d'**atacs de diccionari**.
- Evitar utilitzar dades que puguin ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el mateix nom que l'identificador, el DNI, la data de naixement, el número de mòbil...).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament numèriques.
- Afavorir l'aparició de caràcters especials (!, *, ?, ...).
- No enviar contrasenyes per SMS o correu, ni dir-les per telèfon.

- No utilitzar seqüències de teclat del tipus “qwerty” o “1234” (són seqüències que s’assagen en els atacs de diccionari).
- Fer servir regles mnemotècniques per recordar les contrasenyes (per exemple, “Cada dia al matí canta el gall quiquiriquic” donaria lloc a la contrasenya “CDAMCEGK”).

A més d’aquestes recomanacions sobre la tria de les contrasenyes, també és important disposar d’eines que en permetin el control.

Per exemple, mitjançant **eines de comprovació proactiva** es pot evitar que una mala contrasenya entri a formar part de la base de dades de contrasenyes del sistema. Així, si un usuari tria una contrasenya que apareix en el filtre de l’eina (és a dir que es tracta d’una mala contrasenya) serà rebutjada automàticament.

Un exemple d’eina de comprovació proactiva és `npasswd`, substitut de l’ordre `passwd` en entorns Linux/Unix.

En general, aquestes eines poden permetre, per exemple:

- Registrar totes les sessions i els errors que s’han produït (normalment existeix un límit al nombre d’intents que es poden fer).
- Especificar regles diverses: les contrasenyes han de tenir un nombre mínim de caràcters, no poden consistir en la mateixa contrasenya però a l’inrevés, no poden ser exclusivament numèriques...
- Enviar un missatge a l’usuari que intenti crear una contrasenya feble, segons les regles que s’han definit.

Contrasenya del BIOS i diferents nivells de contrasenyes

Les contrasenyes no apareixen només en els inicis de sessió; les podem trobar en diferents nivells del sistema informàtic, començant per el BIOS.

BIOS

El sistema bàsic d’entrada/sortida o BIOS (*Basic Input-Output System*) és un programa emmagatzemat en un xip ROM que s’ocupa, en el moment en què l’ordinador s’inicia, de carregar el sistema operatiu en la memòria de l’ordinador i de comprovar els dispositius que té connectats.

La utilització de contrasenyes del BIOS en els ordinadors és un aspecte que sovint es descuida, tot i que, si no la posem, l’intrús podria modificar la configuració d’arrencada, de manera que l’ordinador s’iniciés des d’un dispositiu USB, un CD o un DVD. D’aquesta manera, l’intrús podria robar informació, eliminar-la o introduir qualsevol codi maliciós al sistema.

Els nivells en els quals situar un mecanisme d’autenticació en una estació de treball són: BIOS, sector d’arrencada de l’equip, sistema operatiu o, fins i tot, sol·licitat per un programa.

A més del BIOS, també és necessari afegir contrasenyes als gestors d’arrencada, com per exemple GRUB. Així podem evitar que els intrusos puguin modificar les opcions d’inici dels diferents sistemes operatius que controla el gestor.

Debilitats en BIOS

Notem que el BIOS es pot reconfigurar mitjançant els ponts (*jumpers*) allotjats a la placa base, o desconnectant la bateria CMOS (petita memòria que conté la informació de la configuració del sistema i que necessita una bateria per conservar-la). Per tant, si no protegim l’apertura de la carcassa de l’ordinador, un intrús, si té accés físic a l’ordinador, pot saltar-se fàcilment la contrasenya del BIOS.

A la figura **??** i la figura 1.7 s’observa com editant el fitxer menu.lst podem introduir una contrasenya en el GRUB (per a més seguretat, cal xifrar aquesta contrasenya). A més, és possible definir una contrasenya per cadascun dels sistemes operatius que controli el gestor.

Figura 1.6. Edició del fitxer menu.lst

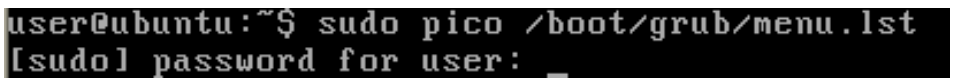
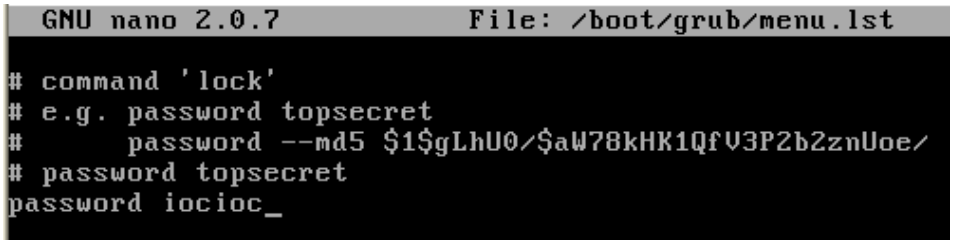


FIGURA 1.7. Definició de la contrasenya "iocioc" dins del fitxer menu.lst



GNU GRUB

El GNU GRUB (*Grand Unifier Bootloader*) és un gestor d'arrencada per a entorns Linux que s'usa per iniciar un o més sistemes operatius instal·lats en el mateix equip (per exemple, Linux i Windows).

Definició de polítiques d'usuaris i grups

La definició dels permisos dels usuaris (és a dir, la determinació de les tasques i accions que poden dur a terme en un sistema informàtic) és una excel·lent mesura preventiva que evita que els usuaris no puguin fer més que allò que necessiten per a la seva feina.

En termes generals, l'administrador desenvolupa aquesta tasca de definició en quatre nivells:

1. En primer lloc, crea i gestiona i els comptes de usuari (individuals).

2. A continuació defineix els grups d'usuaris segons les similituds de les tasques que han de dur a terme i en funció de les seves necessitats d'accés. Un usuari pot pertànyer a més d'un grup.

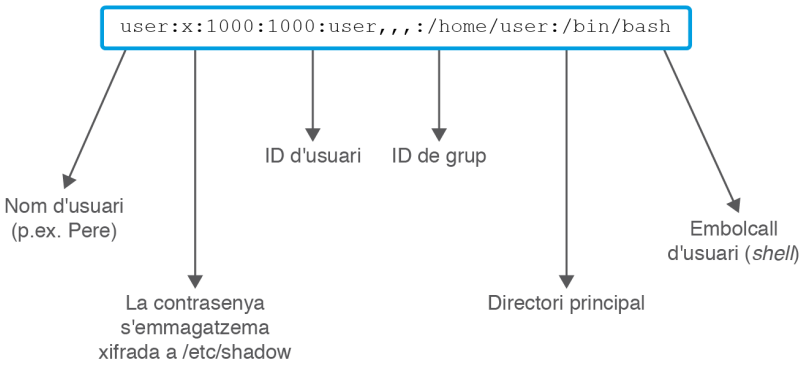
3. Una vegada definits els grups, l'administrador assigna els drets sobre fitxers i directoris (per exemple, podem fer que tots els membres d'un grup anomenat Professors, tinguin permís de lectura i escriptura sobre un directori anomenat Examen).

4. Finalment, es poden acabar de perfilar els drets individuals de cadascun dels usuaris, ja que dins d'un mateix grup, poden haver-hi necessitats diferents.

Tot seguit, i a tall d'exemple, veurem molt breument com dur a terme aquestes operacions en el sistema operatiu Linux/Unix.

- **Definició d'usuaris**. Cada entrada del fitxer /etc/passwd (figura 1.8) conté informació del compte d'un usuari. Entre altres dades, conté el nom d'usuari, el grup primari al qual pertany i el seu directori principal. Les contrasenyes, normalment, no s'emmagatzemen en aquest fitxer, sinó que es troben xifrades en un altre fitxer anomenat /etc/shadow. Per afegir nous usuaris es pot emprar, com a usuari administrador, l'ordre `useradd nom_usuari` (o ***adduser***).

FIGURA 1.8. Descripció dels camps d'una entrada del fitxer /etc/passwd



- **Definició de grups**. La gestió dels grups es realitza de manera similar a la dels usuaris. Les dades dels grups s'emmagatzemen en el fitxer /etc/group, l'estructura del qual és similar a la d'/etc/passwd. Cada línia o entrada del fitxer conté, entre altra informació, el nom del grup, l'identificador del grup (*group ID*) i la llista d'usuaris que en són membres. Per afegir un nou membre, n'hi ha prou d'editar el fitxer /etc/group/ i afegir el nou membre al final de la llista. En cas que hi hagi ocultació de dades, hi haurà un equivalent al fitxer /etc/shadow anomenat /etc/gshadow. De forma similar a la creació de nous usuaris, l'ordre `groupadd nom_usuari` (o addgroup) permet la definició d'un nou grup.

Els fitxers /etc/shadow i /etc/gshadow només són accessibles per l'usuari arrel.

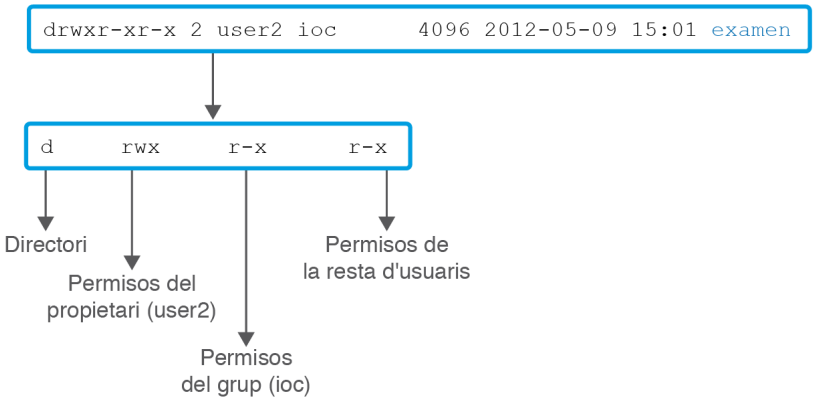
- Ens queda però, veure com ho podem fer perquè un fitxer o un directori **canviï de propietari**. Perquè canviï d'usuari es pot emprar l'ordre `chown nom_usuari nom_fitxer`. De manera similar, amb l'ordre `chgrp nom_usuari nom_fitxer` podem definir que un grup sigui propietari d'un fitxer o directori. A la figura 1.9 podem comprovar que el grup propietari del directori *Examen* després d'executar `chgrp` passa a ser ioc.

FIGURA 1.9. Execució de la instrucció chgrp ioc examen

```
root@ubuntu:/home/user# ls -l
total 22848
drwxr-xr-x 2 user2 root     4096 2012-05-09 15:01 examen
-rw-r--r-- 1 root  root   420935 2011-04-15 04:02 hash_www
-rw-r--r-- 1 root  root   420994 2011-04-15 04:04 hash_www2
-rw-r--r-- 1 user  user  4763163 2009-07-01 00:14 Joomla_1.5.12-Stable-Full_Pack
age.tar.gz
-rw-r--r-- 1 root  root  5051955 2012-04-24 17:19 mac_fls.txt
-rw-r--r-- 1 root  root 12673318 2012-04-24 17:20 timeline.csv
root@ubuntu:/home/user# chgrp ioc examen
root@ubuntu:/home/user# ls -l
total 22848
drwxr-xr-x 2 user2 ioc      4096 2012-05-09 15:01 examen
-rw-r--r-- 1 root  root   420935 2011-04-15 04:02 hash_www
-rw-r--r-- 1 root  root   420994 2011-04-15 04:04 hash_www2
-rw-r--r-- 1 user  user  4763163 2009-07-01 00:14 Joomla_1.5.12-Stable-Full_Pack
age.tar.gz
-rw-r--r-- 1 root  root  5051955 2012-04-24 17:19 mac_fls.txt
-rw-r--r-- 1 root  root 12673318 2012-04-24 17:20 timeline.csv
root@ubuntu:/home/user# _
```

- A Linux/Unix, l'accés del usuaris i grups als fitxers i directoris es determina mitjançant permisos. Hi ha tres tipus de permisos: accés de lectura (r), accés d'escriptura (w) i accés d'execució (x). Així, si observem els atributs del directori *Examen* a la figura 1.9 veurem el que es mostra a la figura 1.10.

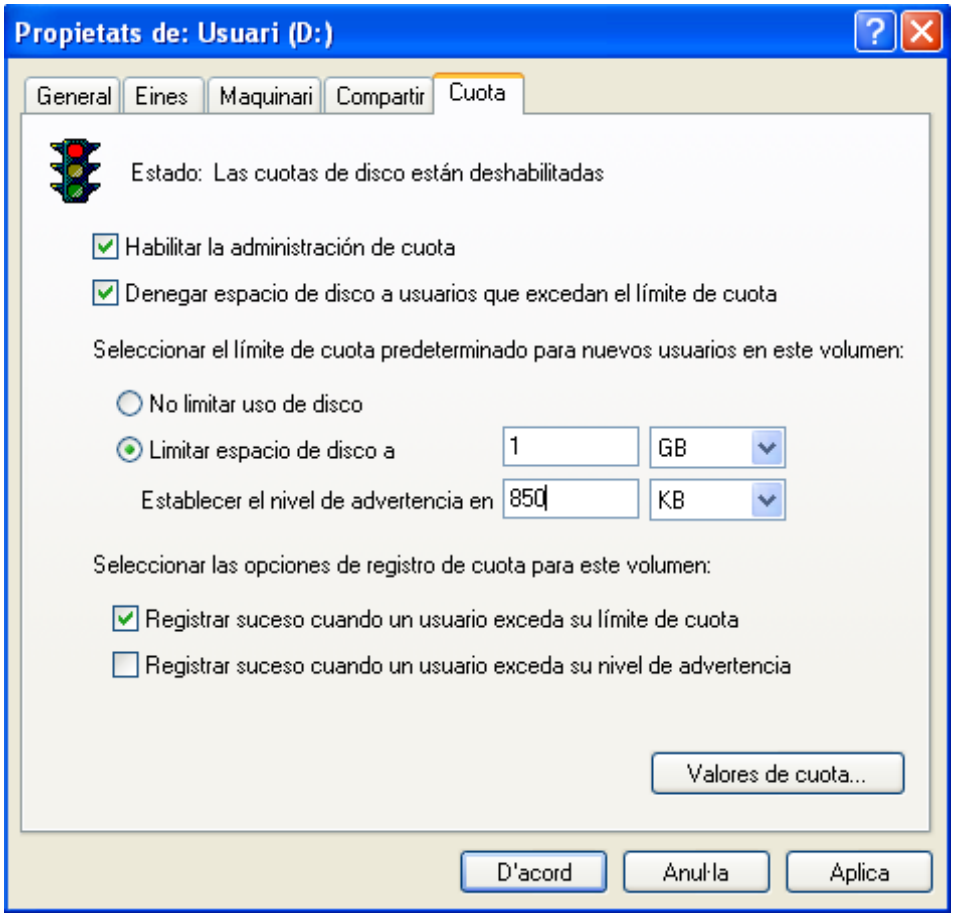
FIGURA 1.10. Permisos del directori Examen



Per executar segons quines ordres ens cal disposar de permisos d'usuari supervisor.

A més, per millorar la seguretat dels fitxers i directoris, es poden emprar les anomenades **llistes de control d'accés** (ACL), amb les quals es poden individualitzar els privilegis que té un usuari sobre un determinat fitxer, sense tenir en compte el grup al qual pertany.

FIGURA 1.11. Assignació d'espai de quota sobre una partició anomenada Usuari



Encara que la captura de pantalla correspon a un Windows XP amb el pedaç de català instal·lat, observem que hi ha parts de la interfície que no estan en català, com la corresponent a la imatge.

Finalment, també és habitual assignar una **quota de disc dur** als usuaris, de manera que no puguin ocupar indiscriminadament tot l'espai de disc dur. Per

exemple, en el sistema operatiu Windows XP podem activar la quota de disc des de les propietats de la partició (ha d'estar en format NTFS) sobre la qual volem definir les quotes d'usuari. En la figura 1.11 podem veure les opcions que tenim per gestionar la quota i denegar l'espai de disc als usuaris que hagin excedit la seva quota. En aquest cas establiríem una quota idèntica per a tots els usuaris, però emprant l'opció *Valors de quota* podríem personalitzar el límit de cadascun dels usuaris. Com podem veure a la imatge, també existeix l'opció d'enregistrar els esdeveniments que excedeixin la capacitat de quota. Després es podran consultar amb el visor d'esdeveniments. En el cas de *windows* és el gestor de consola eventvwr.msc.

En els sistemes Linux es poden establir quotes d'usuari amb l'eina de configuració de sistema **Webmin**.

Ús de tècniques criptogràfiques

La utilització de la criptografia, tant pel que fa a la informació emmagatzemada (per exemple, creant una partició xifrada) com a la informació circulant (per exemple, usant SSH o Telnet segur), permet mantenir la confidencialitat de les dades i impedeix que puguin ser interceptades per intrusos.

A l'annex d'aquesta unitat trobareu un tutorial del programa de criptografia TrueCrypt.

1.3 Eines pal·liatives

Per *eines pal·liatives* entenem aquelles eines i mecanismes que bloquegen els intents de trencar la seguretat de l'equip i eviten els danys provocats pel codi maliciós.

Hi ha moltes eines i mecanismes que pertanyen alhora a la categoria d'eines preventives i a la d'eines pal·liatives.

1.3.1 Instal·lació i configuració

Tal com passa amb els eines preventives, les eines i mecanismes pal·liatius poden anar orientats a l'usuari, a l'equip o al sistema informàtic.

Antivirus

Arran de la proliferació experimentada pels virus informàtics durant la dècada dels vuitanta, van aparèixer els anomenats *antivirus*, és a dir, programes que tenen com a objectiu detectar i eliminar els virus.

Antivirus i codi maliciós

El codi maliciós, en totes les seves variants, es pot enquadrar dins del que s'anomenen amenaces lògiques, els elements més representatius de les quals són els virus, els cucs i els cavalls de Troia.

En l'actualitat, els programes antivirus poden detectar, blocar i eliminar els virus informàtics que trobin, però, a més poden reconèixer altres codis maliciosos.

Els antivirus tenen una part resident en la memòria de l'equip que els permet comprovar en temps real els fitxers que s'executen, creen o modifiquen. També poden revisar, per exemple, els elements adjunts als correus electrònics, així com els scripts o guions que s'executen des dels navegadors web. Per aquest

motiu, els antivirus alenteixen l'arrencada i el funcionament normal del sistema, ja que consumeixen molts recursos per realitzar aquestes comprovacions i mantenir actualitzada la **base de dades de firmes** (patrons binaris que s'utilitzen per identificar possibles virus). No obstant això, òbviament, és molt recomanable, sinó imprescindible, tenir un antivirus instal·lat en el nostre sistema informàtic.

Les tècniques que utilitzen els antivirus per reconèixer nous virus que no apareixen a la seva base de dades s'anomenen **heurístiques**.

Sovint, els creadors dels virus realitzen modificacions dels virus originals per tal de dificultar-ne la detecció. Malgrat això, els antivirus són capaços de reconèixer la firma genèrica que identifica tota la família, sense necessitat d'actualitzar la base de dades de firmes (pensem que si s'haguessin d'identificar tots els virus de forma individual, la mida de la base de dades podria ser enorme).

L'ús d'aquestes tècniques d'identificació pot comportar que es produeixin **falsos positius**, és a dir, fitxers que s'identifiquen falsament com a codi maliciós. De tota manera, el més preocupant, pel que fa a la seguretat del sistema, és que es produeixin **falsos negatius**, és a dir, fitxers que no s'han identificat com a maliciosos, però que ho són.

De vegades, l'antivirus no està instal·lat al sistema, sinó que hi accedeix mitjançant un navegador d'Internet (**antivirus en línia**). En aquest cas, ja que hi accedeix directament al fabricant, la base de dades de firmes sempre està actualitzada. D'altra banda, el fet de treballar via web, fa que no calgui instal·lar el programa i que puguem provar fàcilment antivirus de diferents fabricants. No obstant això, cal tenir en compte que no ofereixen una protecció permanent, a diferència dels **antivirus fora de línia**, els instal·lats en l'equip informàtic. Els antivirus en línia es poden considerar un complement dels fora de línia, si bé no són tan fiables com aquests.

A més de la solució en línia hi ha altres formes d'usar un antivirus sense necessitat d'instal·lar-lo en el sistema. Hi ha antivirus portables (als quals podem accedir, per exemple, des d'un dispositiu USB), i fins i tot **CD autònoms** o *live CD* (és a dir, un CD des de qual podem iniciar el sistema) amb antivirus inclosos, opció molt interessant, ja que evita iniciar el sistema operatiu de la màquina i eludeix, per tant, les tècniques d'ocultació que utilitzen alguns codis maliciosos.

Programes antiespia

A més dels antivirus, existeixen solucions específiques per a la detecció i desinfecció de programes espia i codi maliciós en general, que es poden combinar amb l'antivirus i el tallafoc que fem servir habitualment.

L'objectiu dels programes espia és capturar informació del sistema infectat, bé per conèixer els hàbits de navegació de l'usuari o bé per apropiar-se de la seva informació personal (dades bancàries, per exemple). En qualsevol cas, la instal·lació d'aquest tipus de codi maliciós sempre es fa sense el consentiment de l'usuari afectat. Precisament a causa del seu objectiu de captació, aquest tipus de codi maliciós es troba contínuament en funcionament i pot arribar a alentir considerablement el funcionament del sistema informàtic.

La difusió de l'*spyware* es pot realitzar de moltes maneres. Tenim tendència a pensar que, si no executem cap programari "estrany" no podem ser víctimes de cap codi maliciós. En l'actualitat però, alguns tipus de programa espia no requereixen pràcticament cap acció per part de l'usuari (per exemple, la infecció es pot produir visitant un lloc web) o bé es poden trobar ocults en programes suposadament segurs (com, per exemple, en un controlador de dispositiu).

El comportament de l'*spyware* difereix molt del dels virus i, per aquest motiu, als ulls dels antivirus, pot semblar innocu. Així, és habitual combinar solucions d'antivirus amb programes antiespia, perquè, de fet, no ataquen el mateix problema.

Per evitar l'acció dels enregistradors de teclat que solen incloure els programes espia, s'han desenvolupat teclats virtuals (per exemple, solen aparèixer als web de les entitats bancàries) que eviten que l'usuari hagi d'usar el teclat a l'hora d'introduir dades. Com podem veure a la figura 1.12, els teclats virtuals són teclats gràfics en els quals els usuaris poden seleccionar les lletres amb un clic del ratolí en lloc de prémer una tecla. No obstant això, alguns *keyloggers* poden capturar la pantalla a cada clic, per la qual cosa els teclats virtuals tampoc es poden considerar completament segurs. Per evitar aquest problema, alguns teclats virtuals introdueixen el caràcter quan el ratolí es mou, durant uns segons, sobre la lletra en qüestió, en lloc d'introduir-la amb un clic.

Figura 1.12. Aparença d'un teclat virtual

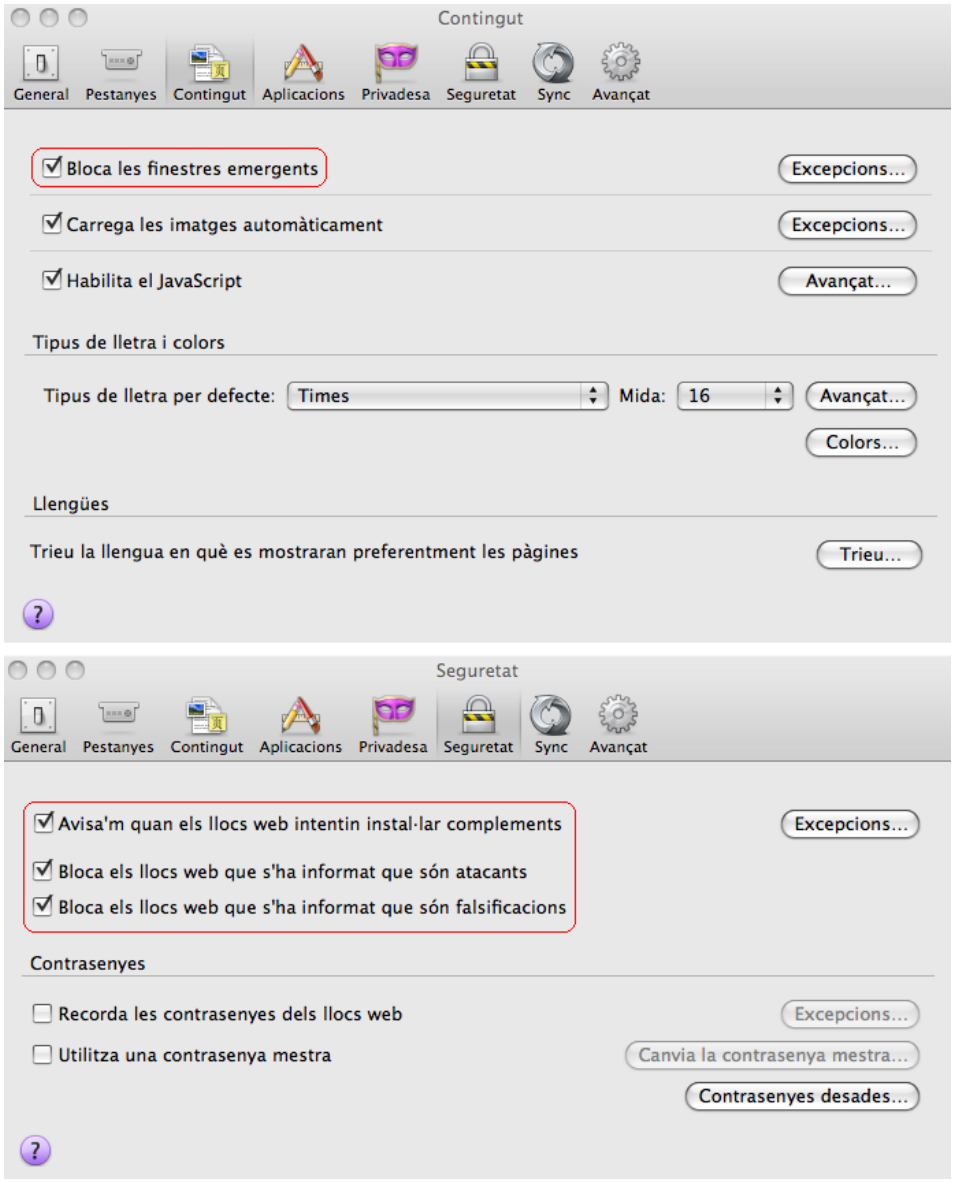
Finalment, com es pot imaginar, no hi ha cap eina que pugui garantir que un sistema informàtic estigui completament lliure de codi maliciós, de manera que el fet que no s'hagi pogut detectar no vol dir que no hi sigui. En tot cas, és essencial que totes les eines pal·liatives tinguin les seves bases de dades actualitzades i que el sistema operatiu i els programaris estiguin actualitzats amb els darrers pedaços publicats.

Eines de bloqueig web

Com s'acaba de veure, la simple navegació web pot comprometre la seguretat d'un sistema informàtic. Per aquest motiu és important que puguem bloquejar els llocs webs que puguin suposar una amenaça per a la seguretat.

De fet, molts navegadors d'Internet es poden configurar perquè bloquin les finestres emergents (filtres *pop-up*) o evitin els adreçaments a llocs de *phishing* (filtres *antiphishing*). Per exemple, a la figura 1.13 podem veure les pestanyes de configuració del navegador Firefox, on podem definir aquests bloquejos (entre d'altres opcions).

FIGURA 1.13. Pestanyes de configuració del navegador Firefox



A més dels navegadors, els antivirus també tenen opcions de bloqueig dels llocs d'Internet que consideren perillosos.

1.4 Actualització de sistemes i aplicacions

L'actualització de sistemes i aplicacions és una faceta sovint poc atesa. Com qualsevol programa d'ordinador, el sistema operatiu i les aplicacions tenen errors

o omissions que poden plantejar problemes de seguretat. En el cas del sistema operatiu és especialment important, ja que és la base a partir de la qual permet el funcionament de la resta de programes instal·lats a l'equip.

1.4.1 Per què cal actualitzar el sistema operatiu i les aplicacions?

Les actualitzacions de sistemes operatius i aplicacions tenen les motivacions següents:

- Corregir les vulnerabilitats detectades. Els intrusos solen aprofitar les vulnerabilitats (tant dels sistemes operatius, com de les aplicacions) per accedir sense autorització al sistema. Per tant, és essencial que les actualitzacions s'instal·lin el més aviat possible per intentar tancar les escletxes de seguretat provocades per aquestes vulnerabilitats. De vegades, encara que no hi hagi ningú dirigint un atac, l'usuari pot executar un programa maliciós que, aprofitant una vulnerabilitat, causi algun dany al sistema. Per tant, com en el cas de l'atac premeditat, convé tenir el sistema operatiu i les aplicacions sempre al dia, amb les darreres actualitzacions publicades.

Un ***exploit 0-day*** implica l'existència d'una vulnerabilitat d'un programa, generalment desconeguda per la comunitat i per la qual encara no s'ha desenvolupat cap actualització. Normalment aquesta vulnerabilitat és desconeguda pel desenvolupador del programari, tot i que de vegades es coneix però no es considera perillosa, i per aquest motiu no es desenvolupa l'actualització que solucionaria el problema. Aquesta manca de resposta fa que els *exploits 0-day* es propaguin amb molta facilitat per tota la xarxa i constitueixen un greu problema de seguretat.

- Permetre la gestió del nou maquinari que, de forma periòdica, va apareixent al mercat.
- Afegir noves funcionalitats i millores a les versions anteriors. Si bé la motivació anterior és més important que aquesta, cal tenir present que les actualitzacions sovint comporten l'afegit de noves funcions i millores en relació a les antigues versions.

1.4.2 Com actualitzar?

Hem vist la importància de mantenir el sistema operatiu i les aplicacions completament actualitzades. Ara bé, com es duu a terme aquesta actualització?

Pel que fa a les aplicacions, moltes es poden configurar perquè, quan detectin l'existència d'una nova actualització a través d'Internet, preguntin a l'usuari si vol baixar-la i, en cas afirmatiu, la descarreguin automàticament.

Pel que fa a les actualitzacions del sistema operatiu, Windows té activada per defecte una opció (Windows Update) que permet descarregar de forma automàtica

les actualitzacions del sistema operatiu. L'usuari pot desactivar aquesta opció i també pot triar si les actualitzacions descarregades s'instal·len automàticament, o si vol veure primer quines són i decidir per si mateix quines vol instal·lar (en general és recomanable veure la descripció de l'actualització i no instal·lar-la per defecte).

A més d'aquesta opció d'actualització individual (per a cada equip), els administradors poden gestionar de forma centralitzada la distribució de les actualitzacions a tota la xarxa mitjançant l'anomenat Windows Server Update Services (WSUS). Amb aquest servei s'aconsegueix que les descàrregues es realitzin des del servidor central i evitar així que cada equip s'hagi de connectar individualment al web de Microsoft.

El sistema operatiu Linux (per exemple, en la distribució Ubuntu) té un gestor d'actualitzacions que funciona de manera similar al de Windows. Com en aquest sistema, permet veure la descripció de les actualitzacions i decidir quines volem instal·lar. També podem comprovar en qualsevol moment si hi ha cap actualització pendent.

També es pot comprovar l'existència d'actualitzacions i ordenar-ne la instal·lació des de la línia d'ordre:

```
1 sudo apt-get update && sudo apt-get upgrade
```

Així mateix, amb l'ordre ***apt-get*** (o ***aptitude***), executada com a usuari arrel, podem instal·lar nous paquets. Per exemple, amb l'ordre següent instal·laríem el conjunt d'eines The Sleuth Kit, molt emprat en informàtica forense:

```
1 apt-get install sleuthkit
```

Continuant amb l'exemple d'Ubuntu, també podem afegir o eliminar aplicacions mitjançant un entorn gràfic, en lloc de fer-ho des de línia d'ordres, emprant el gestor de paquets Synaptic.

1.5 Seguretat en la xarxa corporativa

La seguretat de la xarxa inclou totes les eines i polítiques adoptades per l'administrador del sistema per prevenir i controlar l'accés no autoritzat, mal ús, modificació o inhabilitació d'una xarxa informàtica i els seus recursos.

1.5.1 Monitoratge del trànsit de xarxes

El monitoratge de la xarxa consisteix a supervisar i analitzar el trànsit que hi circula per tal de detectar els incidents de seguretat que s'hi puguin produir, així com per mantenir la qualitat del servei dins dels llindars previstos.

El monitoratge es pot dur a terme amb dues aproximacions diferents, complementàries i no excloents:

- **Monitoratge passiu:** es basa en l'escolta i anàlisi del trànsit real de la xarxa. A diferència de l'aproximació activa, en aquesta no s'injecta trànsit a la xarxa, només es recull la informació i s'analitza. En aquesta aproximació s'usen els anomenats *detectors* o *sniffers*, que es poden trobar en diverses ubicacions com ara encaminadors, commutadors. Amb aquestes tècniques es pot caracteritzar el trànsit de xarxa i veure quin ús se'n fa.
- **Monitoratge actiu:** l'aproximació activa consisteix a injectar paquets de prova a la xarxa, o enviar-ne als servidors i aplicacions, i a mesurar el temps de resposta obtingut. Es pot emprar per supervisar el rendiment de la xarxa, encara que, mitjançant eines actives com els escàners també es poden detectar vulnerabilitats. A diferència de l'aproximació passiva, en el monitoratge actiu s'afegeix trànsit a la xarxa.

Eines passives

Abans de poder emprar cap eina d'anàlisi passiva, cal instal·lar un detector per poder monitorar el trànsit de xarxa.

S'anomenen **detectors (*sniffers*)** els programes que permeten la captura i l'enregistrament de la informació que circula per una xarxa.

El seu funcionament es basa en l'activació del mode promiscu de les interfícies de xarxa (la interfície escolta tot el tràfic de la xarxa enlloc d'estar atenta només a les dades que li envien) de les estacions de treball. Amb l'activació d'aquest mode, l'estació de treball podrà monitorar, a més dels paquets d'informació que s'hi adrecen d'una manera explícita, el trànsit sencer de la xarxa. Això inclou, per exemple, la captura de noms d'usuari i contrasenyes (en cas que circulin en text clar, sense xifrar), o fins i tot la intercepció de correus electrònics o de qualsevol altre document confidencial.

L'ús dels detectors com a eines de supervisió de la xarxa és perfectament lícit, però la captura d'informació personal és una activitat clarament il·lícita.

Si bé els detectors es poden emprar com a eines de supervisió (comptabilització del trànsit, identificació d'aplicacions...) per l'administrador de la xarxa, també poden ser emprats maliciosament amb altres finalitats. L'activitat dels detectors és difícilment detectable perquè no deixen empremtes. No podem tenir constància de la informació que pot haver estat interceptada pels detectors (si no és de manera indirecta, per mitjà dels atacs que pot patir el sistema informàtic). Això sí, com que no hi ha cap raó, normalment, perquè una targeta estigui treballant en mode promiscu, una manera d'esbrinar si hi ha detectors és cercar la presència de targetes en mode promiscu. Això es pot fer amb diverses eines: ***ifconfig***, ***ifstatus*** o Network Promiscous Ethernet Detector (NEPED)...

El detector més conegut és **Wireshark**, conegut antigament com Ethereal.

A més de les mesures de detecció de possibles *sniffers* es poden fer servir mesures de protecció d'abast més general. Per exemple, si es xifren els documents que s'envien per la xarxa amb PGP, encara que puguin ser interceptats, molt difícilment podran ser desxifrats per l'espia. Malauradament, les eines criptogràfiques

protegeixen la informació que circula, però no permeten establir connexions segures. Per això és de vital importància la instal·lació d'altres eines com, per exemple, un servidor de *Secure Shell* (SSH) i les respectives utilitats dels clients. *Secure Shell* permet l'establiment d'inicis de sessió segurs i es pot fer servir com a substitut de l'ordre `telnet`.

Pretty Good Privacy (PGP) és un conegut programa de criptografia que empra tècniques de criptografia de clau pública i privada.

Eines actives

Les eines actives són aquelles que utilitzen la xarxa per descobrir informació a través d'enviar peticions als dispositius de xarxa com ara estacions de treball, servidors o encaminadors.

Escàners

Els escàners de **xarxa** analitzen els serveis i ports disponibles d'ordinadors remots a la recerca de debilitats conegudes que puguin aprofitar els atacants (en certa manera, doncs, automatitzen les tasques que duria a terme un intrús remot).

> Els **escàners** són eines de seguretat que serveixen per detectar les vulnerabilitats d'un sistema informàtic.

TCP i UPD

TCP és la sigla de Transmission Control Protocol, i UPD, la de User Datagram Protocol. Són els protocols que comparteixen tots els ordinadors connectats a Internet per poder-se connectar entre ells.

L'anomenat **escaneig de ports** consisteix a esbrinar els ports TCP/UDP que estan oberts en una màquina remota pertanyent a una xarxa determinada. Els ports oberts constitueixen una informació molt interessant per als possibles intrusos, ja que les vulnerabilitats dels processos que estan en funcionament poden permetre l'accés no autoritzat al sistema.

L'assignació dels ports no és arbitrària, sinó que és determinada per la Internet Assigned Numbers Authority (IANA). Aquests són alguns exemples d'assignació de ports a serveis d'Internet:

- Port TCP/UDP 20: FTP (dades)
- Port TCP/UDP 21: FTP (control)
- Port TCP/UDP 23: Telnet
- Port TCP/UDP 25: SMTP
- Port TCP/UDP 53: DNS
- Port TCP/UDP 80: HTTP
- Port TCP/UDP 110: POP3
- Port TCP/UDP 194: IRC

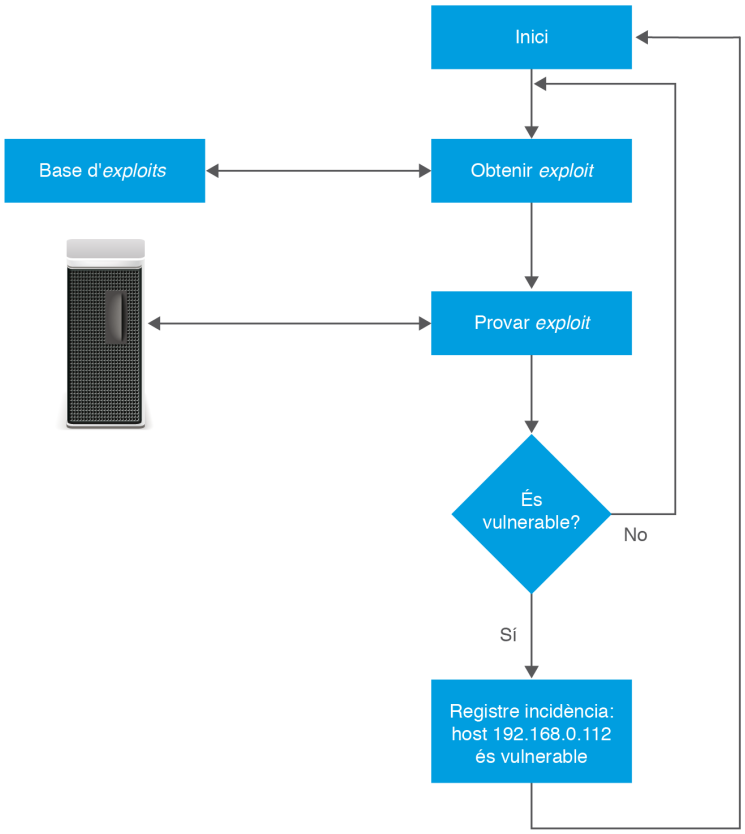
Port

Un **port** és un punt pel qual entra o surt la informació d'un ordinador. Els protocols relatius a Internet (FTP, Telnet…) utilitzen ports emissors i receptors, un port de sortida i recepció comú en els dos extrems de la comunicació.

Els ports 1024 a 65535 s'anomenen *ports registrats*, no estan sota el control de la IANA i poden ser utilitzats per determinades aplicacions. Per exemple, una aplicació client d'una eina de control remot maliciosa podria utilitzar un port d'aquest rang per realitzar les seves tasques i passar desapercebuda per l'usuari local o l'administrador del sistema.

Tots els escàners comparteixen, en trets generals, un esquema de funcionament similar, que podem veure representat en la figura 1.14.

Figura 1.14. Diagrama de flux d'un escàner de xarxa



Tot i que els escàners són eines de molta utilitat per als administradors dels sistemes informàtics, també els intrusos en poden fer un ús maliciós. Els escàners permeten l'automatització de centenars de proves per localitzar les vulnerabilitats d'un sistema. D'altra banda, no cal que l'intrús conegui amb precisió les vulnerabilitats del sistema; pot utilitzar simplement la informació que li proporciona l'escàner, sense necessitat de ser un expert informàtic.

Ordres de sistema

Per a una diagnosi ràpida de possibles errors en la comunicació, és recomanable utilitzar les ordres `ping` i `traceroute`. Amb `ping` es pot determinar si una màquina està connectada o no a la xarxa. Amb `traceroute` es pot obtenir una descripció del camí que es va seguint per arribar a una determinada màquina, de manera que en cas que una estació no respongui es pot determinar el lloc on es produeix el problema.

Al mercat hi ha moltes eines que faciliten el monitoratge de la xarxa, com per exemple MRTG (Multi Router Traffic Grapher) o el conegut Nagios.

1.5.2 Seguretat en els protocols per a comunicacions sense fil

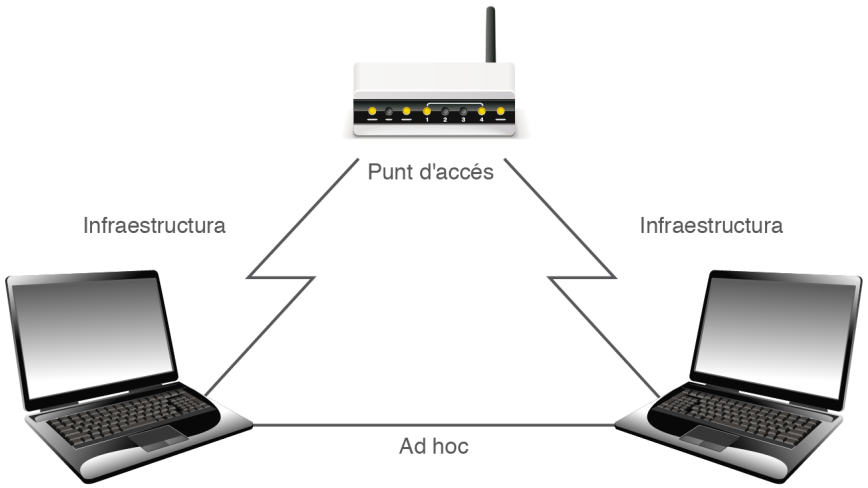
Les comunicacions sense fil, basades en ones de ràdio o infraroges, permeten connectar-se a la xarxa des de qualsevol lloc de l'organització i en qualsevol moment sense necessitat d'estendre cap cablejat, la qual cosa permet la possibilitat d'ampliar les dimensions de la xarxa amb molta facilitat.

Wi-Fi significa *wireless fidelity* (fidelitat sense fil). Les xarxes locals sense fils s'anomenen **WLAN** (*Wireless Local Area Network*).

Les xarxes locals sense fil poden operar en **mode *ad hoc*** o en **mode infraestructura**:

- **Mode ad hoc** (client a client). Totes les màquines que es troben dins de la mateixa àrea es poden comunicar entre si directament. No és habitual, encara que és pràctic, per exemple, per enviar informació entre dos ordinadors.
- **Mode infraestructura** (client a punt d'accés). Les estacions es comuniquen amb els anomenats **punts d'accés**, que actuen de repetidors i difonen la informació a la resta de la xarxa.

FIGURA 1.15. Mode d'operació de les xarxes sense fil



Com que la informació no necessita cap mitjà determinat per circular, aquestes xarxes presenten problemes de seguretat importants. Per exemple, en una configuració normal de xarxa, el tallafoc sol ser un element crític de la seguretat i reuneix una part important de les mesures de protecció als atacs exteriors. En una xarxa sense fil però, els atacants ja no necessiten passar pel tallafoc i poden atacar directament altres dispositius de xarxa. Per aquest motiu, inicialment es va preveure la utilització d'un protocol de xifratge anomenat WEP (*Wired Equivalent Protocol*), que forma part de l'especificació de la norma IEEE 802.11. Amb aquest protocol, una clau WEP predeterminada se situava en cada punt d'accés i en cada client, de manera que només als clients amb la mateixa clau se'ls permetia l'accés. No obstant això, aquest mecanisme no és segur i en l'actualitat es pot desxifrar sense massa problemes. El protocol WEP es basa en un algorisme de xifrat,

anomenat RC4, que és molt feble. Es pot desxifrar interceptant un determinat volum de paquets en circulació (per exemple, amb l'eina Aircrack).

IEEE

L'Institute of Electrical and Electronic Engineers (IEEE) és un organisme que data de l'any 1980 i que va elaborar les normes IEEE 802.X, que defineixen els estàndards de funcionament de les xarxes d'àrea local.

Arran dels problemes de seguretat provocats pel protocol WEP, es va desenvolupar un altre sistema, anomenat WPA (*Wi-Fi Protected Access*), que forma part de l'especificació IEEE 802.11 i, millora l'anterior i proveeix mecanismes d'autenticació. El WPA també utilitza l'algorisme de xifratge RC4, però presenta certes diferències en relació a WEP pel que fa a la gestió de claus.

L'especificació IEEE 802.11 i es va continuar desenvolupant fins a produir el sistema WPA2, que utilitza l'algorisme criptogràfic estàndard de clau privada AES (*Advanced Encryption Standard*) en lloc de l'RC4.

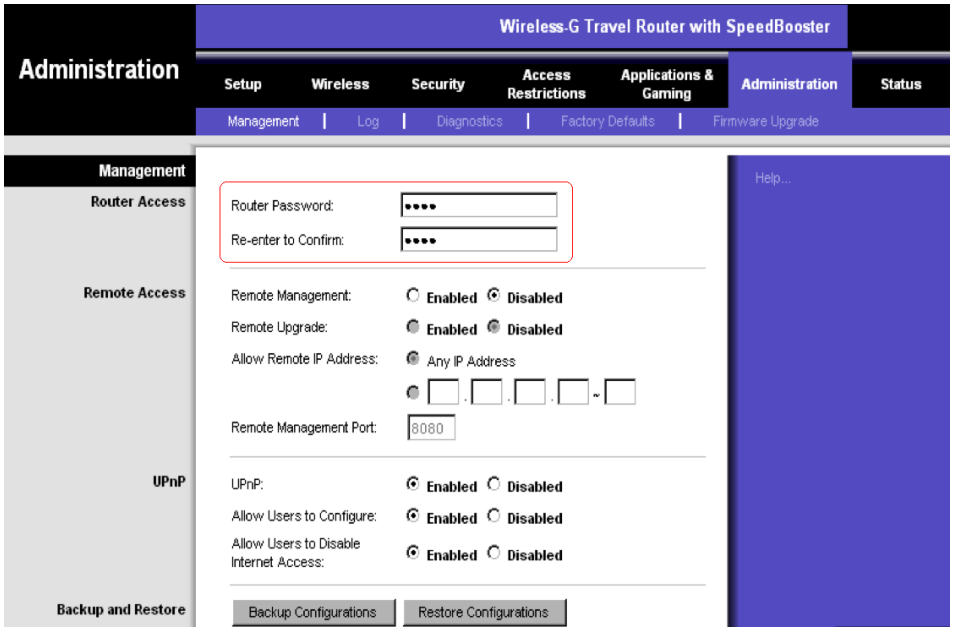
Tant el WPA com el WPA2 presenten vulnerabilitats i es poden atacar. Això és conseqüència del fet que, malgrat les millores criptogràfiques, el mecanisme d'associació d'un client a la xarxa sense fil és molt semblant, amb independència del sistema de seguretat que es triï (WEP, WPA o WPA2).

> Cal tenir present que les xarxes locals sense fil requereixen, a causa de la seva natura intrínseca, unes mesures de seguretat més grans que les que s'adoptarien en una xarxa cablejada.

Vist a grans trets el funcionament de les xarxes sense fil, passem a fer algunes recomanacions per millorar la seguretat de les WLAN:

- Canviar la contrasenya per defecte (pensem que els fabricants solen emprar la mateixa contrasenya per a tots els seus equips).

FIGURA 1.16. Tauler d'administració d'un punt d'accés



- Activar el filtrat d'adreces MAC de manera que només es puguin connectar els dispositius especificats (totes les recomanacions que estem veient es

duen a terme des de menús similars a la figura 1.16). Aquest mecanisme no autentica l'usuari, sinó la interfície del terminal que s'hi connecta. No obstant això, cal tenir present que les adreces MAC poden ésser falsificades fàcilment.

- Activar el xifratge WEP/WPA.
- Desactivar, si no hi ha cap raó tècnica per mantenir-la, l'assignació d'IP per DHCP (d'aquesta manera caldrà assignar la IP de forma manual).

DHCP és l'acrònim de *Dynamic Host Configuration Protocol*.

- Els punts d'accés fan per defecte la difusió (*broadcast*) del SSID, és a dir, del nom lògic associat a la xarxa. Per evitar els accessos no desitjats es pot eliminar aquesta difusió.

SSID

El SSID (*Service Set Identifier*) és un codi format com a màxim per 32 caràcters que han de compartir tots els dispositius que es connecten entre si en una xarxa sense fils. També es coneix com a nom de la xarxa.

Broadcast és la difusió d'informació d'un node emissor a una multitud de nodes receptors de forma simultània.

1.5.3 Riscos potencials dels serveis de xarxa

Una xarxa és un conglomerat de molts elements heterogenis. Per tant, la seva seguretat, així com els riscos a què pot estar exposada, s'ha de cercar en primer lloc en els dispositius individuals que la conformen, i després en les interrelacions existents entre tots aquests dispositius i en la globalitat de la xarxa. Els servidors i les estacions de treball són elements essencials de la xarxa, no obstant això, en aquest apartat ens centrarem en l'estudi de la seguretat dels elements de la xarxa.

Seguretat dels elements de xarxa

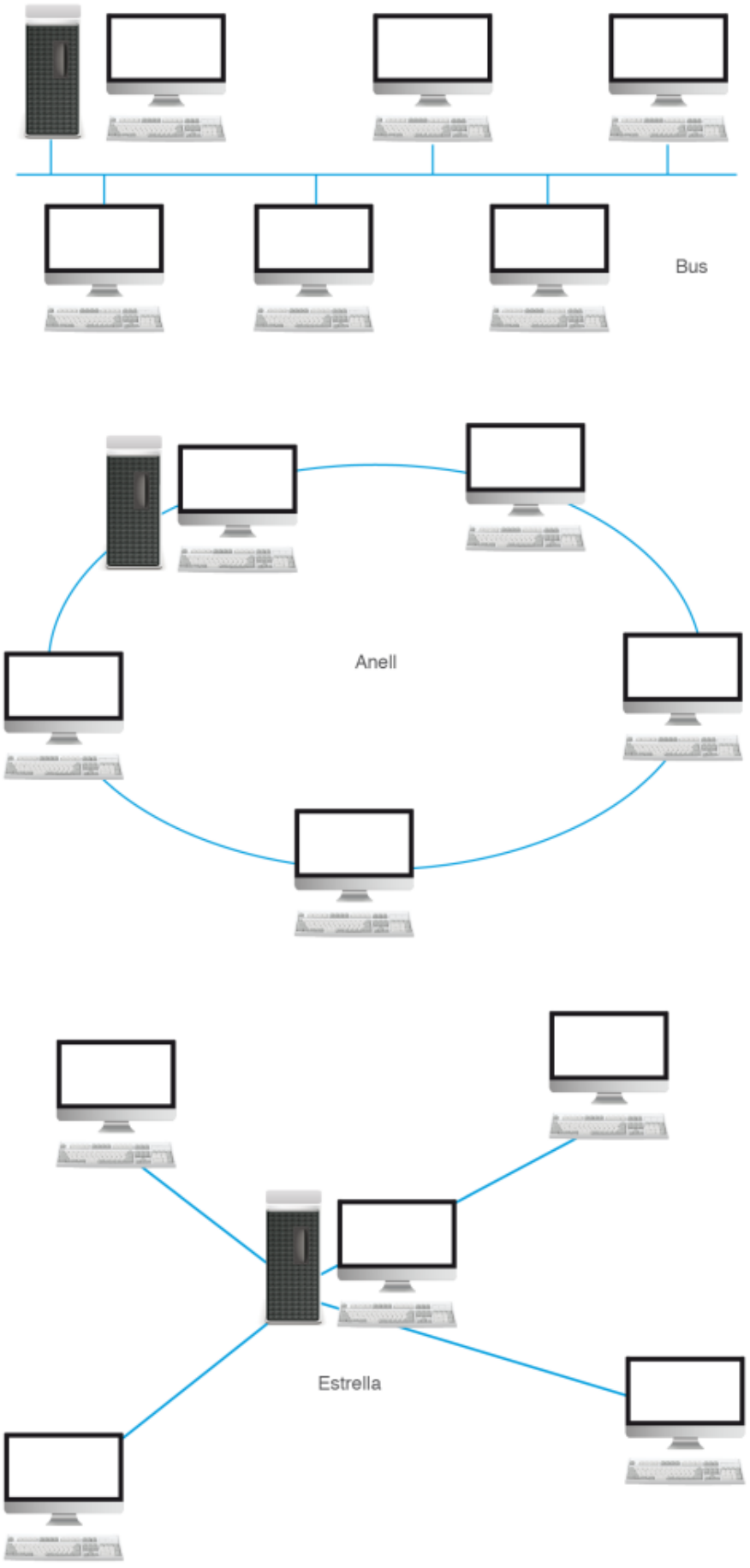
Quan parlem de seguretat dels elements de xarxa hem de tenir en compte les possibles vulnerabilitats de tots els elements que la constitueixen: la topologia, la seguretat del maquinari o els sistemes d'autenticació.

Seguretat de les topologies i els tipus de xarxa

Per *topologia* s'entén la forma o estructura de la xarxa des del punt de vista lògic, que pot diferir del seu disseny físic. Vegem a la figura 1.17 alguns exemples de topologia de xarxa. Notem que, segons la topologia, els riscos que assumeix la xarxa poden ser diferents.

Per exemple, una topologia d'estrella és especialment resistent a la caiguda de les estacions de treball (a diferència de les altres dues), però en canvi té un punt crític, l'element central, que si és atacat o cau per qualsevol motiu pot provocar la caiguda de tota la xarxa.

Figura 1.17. Tipus de topologies de xarxes



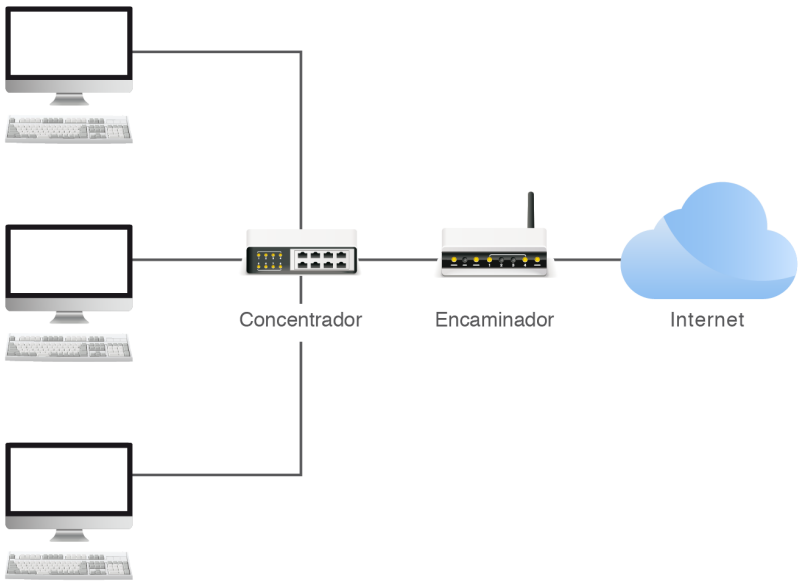
Seguretat del maquinari de xarxa

Pel que fa a la seguretat dels commutadors, concentradors i encaminadors, cal prendre les precaucions següents:

- Activació del xifratge (en cas que els dispositius ho admetin).
- En cas que no sigui necessari, cal desactivar el control remot d'administració.
- Canviar les contrasenyes d'administració predeterminades d'aquests dispositius.
- Usar llistes d'accés que permetin només els protocols, ports i adreces IP que la xarxa i els usuaris necessitin. Denegar la resta.

Com podem veure en la figura 1.18, l'encaminador pot esdevenir el punt més crític d'una xarxa des del punt de vista de possibles atacs externs. Al ser l'encaminador el dispositiu que permet el tràfic entre dues xarxes (molt sovint Internet és una d'elles), aquest element és visible per tothom. Representa, per tant, el punt d'entrada per atacants externs i el primer dispositiu a comprometre ja que és públic.

FIGURA 1.18. L'encaminador com a element de risc de la xarxa



Control d'accés a la xarxa basat en autenticació

IEEE 802.1X

L'IEEE 802.1X és un protocol creat per l'IEEE per al control d'accés a la xarxa basat en ports. Utilitza l'EAPOL (EAP sobre la xarxa d'àrea local) i és utilitzat per transportar les credencials del client a l'autenticador.

A més de les polítiques de contrasenyes d'usuari i tècniques de xifratge de la informació, també cal considerar els mètodes de control d'accés dels dispositius que es volen connectar a la xarxa. Aquest mètode requereix tres components i es basa en l'adreça MAC del dispositiu:

- **Client**: dispositiu (per exemple un portàtil) que desitja connectar-se a la LAN mitjançant una xarxa de telecomunicacions.

- **Autenticador**: és l'element que controla l'accés físic al medi, basant-se en l'estat d'autenticació del client. L'estat inicial dels ports de l'autenticador és "no controlat". Si el procés d'autenticació finalitza afirmativament, el port canvia el seu estat a "controlat" i el dispositiu és autoritzat a accedir al medi.

- **Servidor d'autenticació**: és el dispositiu de "confiança" que s'encarrega d'efectuar la validació de la identitat del client. Notifica el resultat a l'autenticador.

Atacs als serveis de xarxa

Els serveis de xarxa poden ser víctimes de diversos tipus d'atacs, entre els quals podem destacar:

1. Atacs de denegació de servei

2. Atacs de falsejament d'identitat (*spoofing*)

a) Atacs de denegació de servei

S'anomena *atac de denegació de servei (denial of service)* tota acció iniciada per una persona o entitat que inutilitza el maquinari o programari de manera que els recursos del sistema no siguin accessibles des de la xarxa. Els atacs de denegació de servei (DoS) poden atacar el maquinari de la xarxa, el sistema operatiu fins i tot les aplicacions del sistema. Els atacs DoS poden implicar altres ordinadors intermediaris (fins i tot milers), amb la qual cosa s'aconsegueix un dany encara més gran. A més, l'atacant pot ocultar la seva adreça IP gràcies als ordinadors pont (anomenats *zombis*). Aquest tipus d'atac s'anomena atac *DoS distribuït* (DDoS o *distributed denial of service*).

Els atacs de denegació de servei són atacs **contra la disponibilitat** dels recursos d'un sistema informàtic.

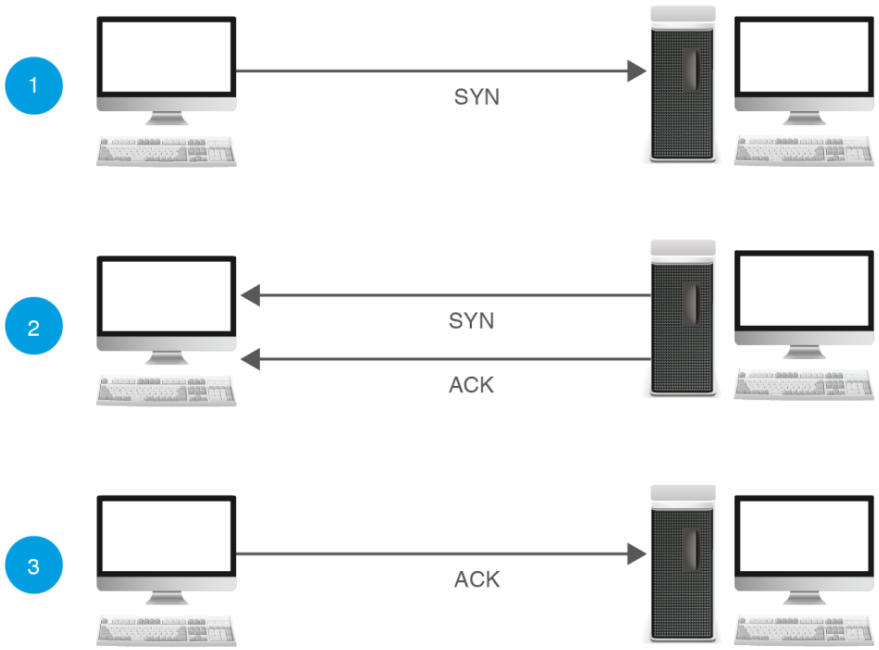
Vegem un exemple d'atac de denegació de servei: l'atac SYN. Aquest atac consisteix en l'enviament d'un gran nombre de sol·licituds de connexió per segon. El sistema atacat respon correctament les sol·licituds de connexió, però en no obtenir resposta del sistema atacant, es col·lapsa i no pot atendre les sol·licituds de connexió legítimes. Aquest atac es basa en el *modus operandi* del protocol d'establiment de sessió entre client i servidor:

1. L'ordinador client envia una sol·licitud de sincronització (SYN) al servidor.

2. El servidor respon amb un missatge ACK (*acknowledgement*) i un missatge de sincronització al client.

3. En resposta a la sol·licitud de sincronització, l'ordinador client envia una resposta ACK al servidor.

FIGURA 1.19. Protocol d'establiment de sessió en tres passos



El servidor manté en cua d'espera tots els paquets SYN que va rebent, fins que són cancel·lats per l'enviament del corresponent ACK per part del client (o bé expira el temps d'espera establert per un temporitzador). L'atac SYN es produeix quan els paquets enviats per l'emissor contenen adreces IP falses i, en conseqüència, el servidor no podrà rebre mai el paquet ACK que alliberaria la cua de recepció. Així, quan aquesta s'omple, les noves (i legítimes) sol·licituds de connexió no es poden servir i es produeix la denegació de servei.

b) Atacs de falsejament d'identitat (*spoofing*)

Observem que amb tècniques de falsejament d'identitat es poden aconseguir atacs de denegació de servei.

En els atacs d'*spoofing* l'intrús fa servir tècniques de suplantació d'identitat. Les formes més conegudes d'aquests atacs són el **falsejament d'IP**, el **falsejament d'ARP** i el **falsejament de DNS**.

En el cas del falsejament d'IP, l'atacant obté accés no autoritzat a una xarxa suplantant la seva adreça IP per la d'un equip en el qual es confia dins de la xarxa. Un dels camps de la capçalera IP conté l'adreça d'origen. Aquest tipus d'atac substitueix l'adreça i fa veure que s'ha enviat des d'una màquina diferent. Com a anècdota, aquest tipus d'atac va convertir a Kevin Mitnick en el *hacker* més conegut del món. Mesos més tard, va ser arrestat per l'FBI per robatori de fitxers.

Les tècniques de falsejament d'ARP es poden fer servir per realitzar els anomenats *atacs man-in-the-middle*.

L'atac *man-in-the-middle* (MITM) és un atac contra la confidencialitat i la integritat.

En aquest tipus d'atac, l'atacant vol conèixer tot el trànsit de xarxa entre l'usuari A i B i viceversa, però, com es pot veure en la figura 1.20, no és possible perquè es troben connectats mitjançant un commutador (element de xarxa que controla el tràfic de xarxa en base a la informació de l'adreça de cada paquet). De manera molt resumida, l'atacant aconsegueix que tant l'usuari A com el B usin la seva adreça MAC (conservant les adreces IP respectives), per la qual cosa pot espiar el trànsit de xarxa entre els dos.

FIGURA 1.20. Atac man-in-the-middle

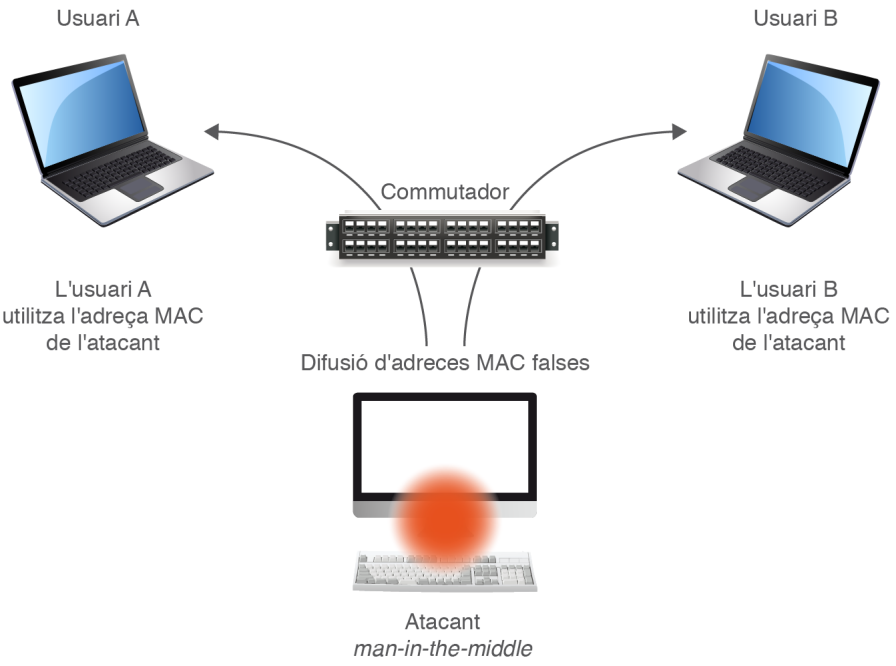
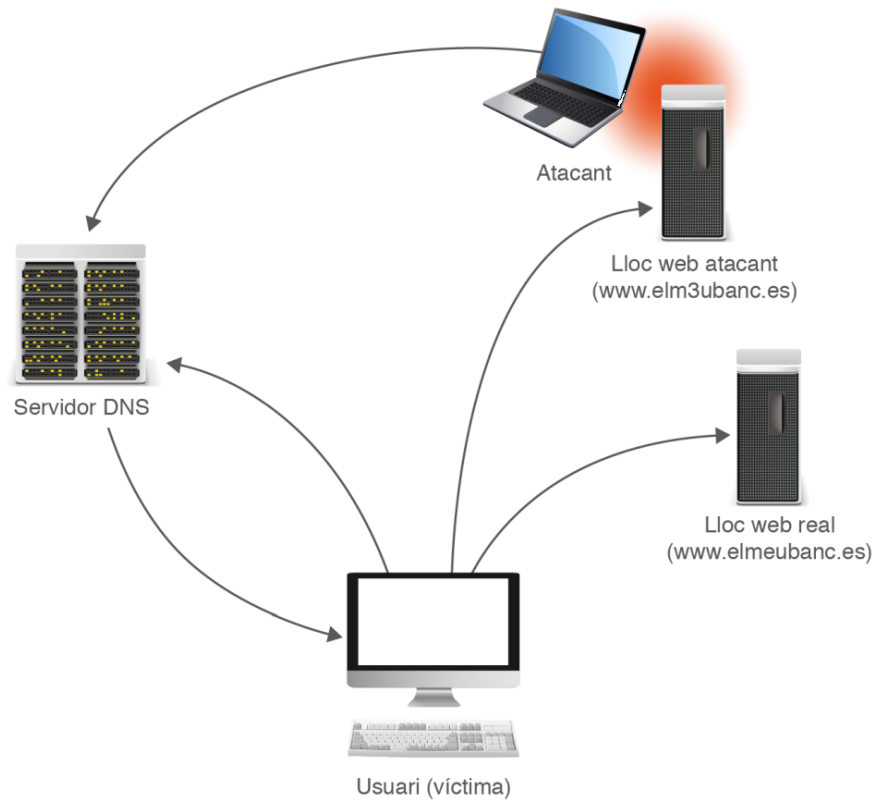


FIGURA 1.21. Esquema d'un atac de desencaminament



Amb la tècnica del **falsejament de DNS** es pot realitzar un tipus d'atac anomenat *desencaminament (pharming)*, en el qual la màquina atacada, quan sol·licita una adreça IP determinada al seu servidor DNS (per exemple, www.el_meu_banc.es),

rep una adreça falsa. Així, continuant amb l'exemple, la víctima suposarà que està accedint al seu banc, mentre que en realitat ho fa al lloc web proporcionat per l'atacant, on es capturaran les claus d'accés de l'usuari a la seva entitat financera (figura 1.21).

Pharming i phishing

No s'ha de confondre el desencaminament (*pharming*) amb la pesca (*phishing*). El desencaminament és un atac molt tècnic, mentre que la pesca és una estratègia d'enginyeria social dissenyada perquè les víctimes accedeixen a llocs web falsos, on capturaran les seves claus personals. Si són reeixits, tots dos atacs acaben, però, amb el mateix resultat.

1.5.4 Intents de penetració. Detecció d'intrusions

Actualment les xarxes informàtiques tenen algun punt que les connecta amb altres xarxes (típicament Internet). Així doncs, la xarxa d'una organització rebrà informació externa com per exemple correus electrònics, peticions de pàgines web al seu servidor, o actualitzacions de programari de les aplicacions i sistemes operatius instal·lats. En aquest escenari, és inevitable qüestionar-se si tota la informació externa que viatja per la xarxa de l'organització és maliciosa. Si n'hi ha que no ho és, com es pot esbrinar?

Sistemes de detecció d'intrusos

Els sistemes de detecció d'intrusos (IDS) monitoren els continguts del flux d'informació de la xarxa a la recerca i rebuig de possibles atacs. Poden combinar maquinari i programari, i normalment s'instal·len en els dispositius més externs de la xarxa, com ara tallafocs. Admeten diferents tipus de classificacions:

- Segons la font de la informació
- Segons el tipus d'anàlisi que realitzen
- Segons el tipus de resposta de l'IDS

Segons la font de la informació

Un *Network IDS* de font oberta molt conegut és l'anomenat **Snort**, usat tant en plataformes Windows com a Linux.

- **Basats en xarxa** (*Network IDS*). Monitoren una xarxa a la recerca d'elements que puguin indicar un atac contra algun dels seus components. Són elements passius que no injecten trànsit a la xarxa (actuen en mode promiscu, escoltant tot el trànsit de xarxa).
- **Basats en màquina** (*Host IDS*). Monitoren una màquina (o diverses, en el qual cas s'anomenen *multihost*) i recullen dades del sistema operatiu (per exemple, el registre d'esdeveniments). Consumeixen recursos de la màquina en la qual s'han instal·lat. Com que treballen amb el sistema

L'eina Tripwire, descrita en l'apartat "Detecció de codi maliciós" d'aquesta mateixa unitat, és un IDS basat en màquina.

operatiu i el sistema de fitxers de la màquina, poden detectar atacs que els IDS de xarxa no detecten. Solen incloure mecanismes de verificació de la integritat de fitxers.

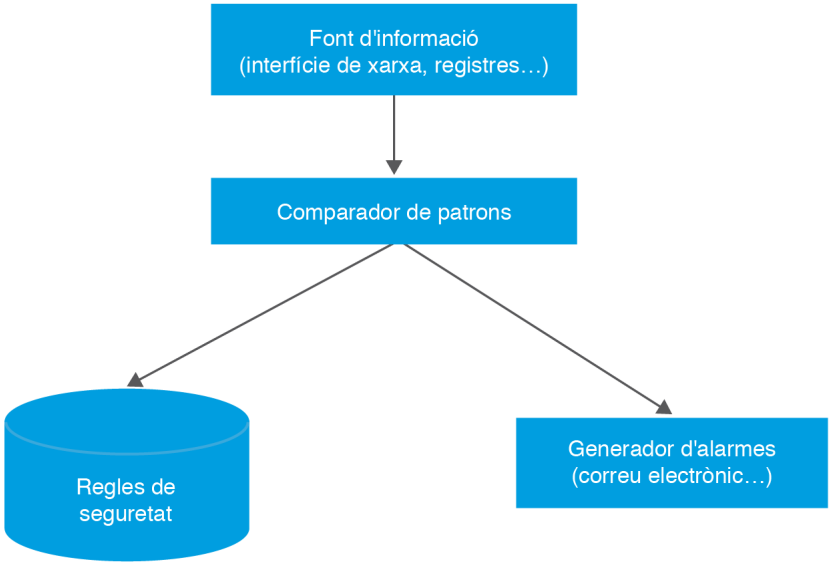
- **Basats en aplicacions**. Monitoren els fitxers de registre d'una aplicació específica per detectar activitats sospitoses (per exemple, els *logs* d'un servidor de l'FTP). Consumeixen molts recursos de la màquina.

Segons el tipus d'anàlisi que realitzen

Una vegada recollida la informació, cal analitzar-la. Segons el tipus d'anàlisi que es realitzi, també tenim diferents tipus d'IDS (no són mútuament excloents):

- **Basats en firmes**. L'anàlisi s'efectua cercant firmes (**patrons d'atac**) que permetin identificar un atac ja conegut. Aquests tipus de IDS requereixen que les bases de dades de firmes siguin actualitzades constantment. A la figura 1.22 es pot veure l'arquitectura bàsica d'aquest tipus IDS.
- **Basats en anomalies**. En aquest cas, l'IDS cerca comportaments anòmals a la xarxa (un escaneig de ports, paquets mal formats...).
- **Segons el tipus de resposta de l'IDS:**
  - **Resposta passiva**. L'IDS enregistra l'alarma generada o avisa el responsable.
  - **Resposta activa**. Aquest IDS, a més de les accions de la resposta passiva, té capacitat de reacció i pot bloquejar les accions intrusives.

FIGURA 1.22. Esquema general d'un IDS basat en firmes

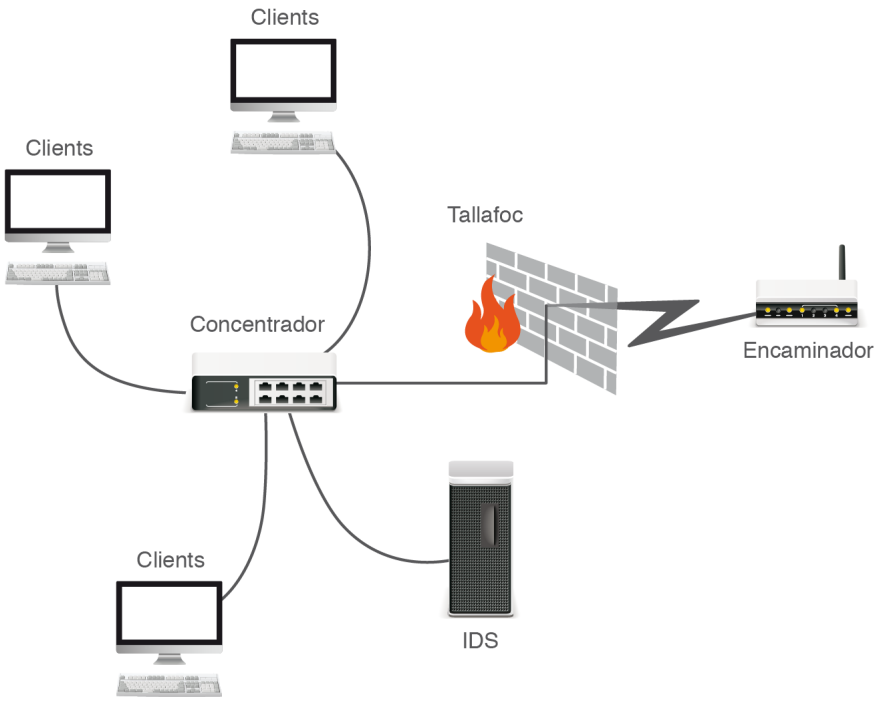


Els IDS poden enviar i obtenir informació d'altres elements (tallafocs, encaminadors...) de la xarxa (**propietat d'interoperabilitat**) i són capaços de relacionar

esdeveniments independents i que vistos de forma aïllada poden no significar cap amenaça pel sistema (**propietat de correlació**).

En la figura 1.23 podem veure una ubicació típica d'un IDS en una xarxa amb concentrador.

Figura 1.23. Ubicació d'un IDS en una xarxa



L'anàlisi dels registres dels IDS és clau quan es realitza un **test de penetració**. El personal que duu a terme aquestes proves analitza els *logs* que enregistren els IDS quan el sistema és sotmès a diversos atacs i extreu conclusions per millorar la seguretat del sistema. Més formalment, els tests de penetració són proves que avaluen la seguretat d'un sistema informàtic simulant que és atacat per personal extern de l'organització (*outsiders*) així com per personal intern (*insiders*). Al personal extern se'l suposa no autoritzat (i, per tant, s'estudia com pot accedir un usuari no autoritzat), mentre que al personal intern se'l suposa algun permís d'accés.

Els **sistemes de prevenció d'intrusos (IPS)** permeten establir polítiques de seguretat per protegir la xarxa dels atacs. Es poden considerar una extensió dels IDS.

Els tests de penetració es poden realitzar des de dos vessants diferents (o bé un terme mig de tots dos):

- Proves de **caixa negra** (*black box*): s'assumeix que no es té cap coneixement previ del sistema que s'ha de testar.

- Proves de **caixa blanca** (*white box*): s'assumeix el coneixement total del sistema a testar.

Esquers (honeypots i honeynets)

Un *honeypot* és un sistema informàtic (o programa) que es posa de manera deliberada a l'accés públic per estudiar les pautes dels seus possibles atacants. Aquests sistemes no poden contenir cap informació important i necessiten eines passives d'auditoria que permetin conèixer, amb posterioritat a l'atac, què ha passat en el sistema. Freqüentment, aquests sistemes també contenen directoris o noms de fitxers amb identificacions llamineres, que despertin la curiositat dels atacants. A més de la seva finalitat d'anàlisi, també poden utilitzar-se per distreure l'atenció dels possibles atacants del veritable sistema, que no ha de ser accessible a través del sistema utilitzat com a esquer. Els *honeypots* no es troben, en general, completament protegits, i les aplicacions i dispositius es configuren amb les opcions per defecte i solen presentar múltiples forats de seguretat.

La translació del concepte de *honeypot* a una xarxa s'anomena *honeynet*. En aquest cas, els atacants, a més de servidors no completament assegurats, també poden trobar dispositius perifèrics a la xarxa, com encaminadors o tallafocs.

1.6 Les xarxes públiques. Seguretat en la connexió

Una xarxa pública és una xarxa de comunicacions que pot ser usada per qualsevol a un preu molt reduït. Aquesta xarxa està gestionada per una operadora de telecomunicacions i, per tant, la informació que hi viatja és susceptible de ser 'observada' durant el seu trànsit fins al destí. Cal prendre mesures per evitar-ho.

Per garantir la impossibilitat que la informació pugui ésser interceptada, les dades no haurien de viatjar a través de les xarxes públiques. Les xarxes no públiques s'anomenen connexions dedicades, les quals són molt costoses i poc flexibles als canvis. No obstant això, és possible usar xarxes públiques i alhora impedir que la informació pugui ésser interceptada, fent que sigui incomprensible (mitjançant tècniques de xifrat), excepte pel receptor autoritzat.

1.6.1 Pautes i pràctiques segures

L'ús de les xarxes públiques requereix l'establiment de relacions de confiança en un entorn gairebé anònim i intangible per definició. En el cas del comerç electrònic, aquesta relació de confiança no només ha de servir per protegir la nostra privacitat, sinó per conformar un espai de seguretat en què les transaccions econòmiques siguin viables. Aquesta és la principal motivació de la **signatura electrònica**.

La **signatura electrònica**, basada en la criptografia de clau pública, permet que un emissor pugui enviar missatges a un receptor complint 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**: certesa que el missatge no s'ha modificat durant la transmissió.
- **No repudi**: 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 evita aquesta possibilitat.

Podeu trobar més informació sobre els **esquemes de clau pública** en la unitat "Seguretat física, lògica i legislació".

Aquestes tres propietats són essencials perquè la signatura digital gaudeixi de confiança en un entorn tan intangible com Internet. Si volem fer activitats tan delicades, com, per exemple, participar en unes votacions electròniques, és imprescindible garantir les tres propietats abans esmentades. Observem que moltes vegades l'entorn en què se signa un document de manera **manuscrita** ofereix en realitat menys garanties que els criptosistemes de clau pública, que presenten una gran robustesa. Suposem, per exemple, el cas de les votacions electròniques. En el món real, el votant introdueix físicament una papereta de vot dins d'una 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.

Funcionament d'un criptosistema de clau pública

Quan un usuari A vol **enviar un missatge** a un usuari B, xifra el missatge fent servir la clau pública de B (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 (que només ell té).

Totes les claus públiques s'obtenen d'un directori públic i, per tant, no podem garantir a qui pertanyen efectivament.

Quan l'usuari emissor vol **signar un missatge**, empra 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 dut a terme per l'usuari B, utilitzarà la clau pública de l'usuari A (coneguda per tots els usuaris del criptosistema).

No repudi

És important observar que, una vegada s'ha signat un missatge, quan la signatura sigui verificada per l'usuari receptor, l'usuari emissor no podrà negar l'emissió del missatge (propietat de no repudi). Les autoritats de certificació, a més d'emetre certificats, també els poden revocar.

Fixem-nos que el punt feble d'aquest protocol es produeix quan hem de fer ús d'una clau pública. Per exemple, quan l'usuari B de l'exemple (el receptor) vol comprovar la identitat de l'emissor mitjançant la clau pública de l'usuari A, com pot saber que la clau que utilitza pertany realment a A?

Autoritats de certificació

Per resoldre el problema de la identitat de l'emissor, es requereix la participació d'una tercera part (anomenada **autoritat de certificació**) que confirmi l'autenticitat de la clau pública d'un usuari determinat. Aquesta certificació s'aconsegueix mitjançant 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 i confirma la seva identitat en qualsevol transacció.

Les autoritats de certificació s'estructuren de forma jeràrquica, de manera que l'autoritat de certificació arrel és autosignada (és a dir que no té cap altra autoritat que la certifiqui) i a cada nivell inferior s'hi poden trobar autoritats de certificació (una o més) que poden signar certificats d'entitat final (persones, aplicacions de programari) o certificats d'altres autoritats de certificació subordinades.

El protocol que descriu tots els processos organitzatius que calen per gestionar els certificats digitals s'anomena **Infraestructura de Clau Pública** (PKI).

Obtenció d'una identificació electrònica

Com a usuaris, és possible obtenir un certificat digital que ens permeti identificarnos a la xarxa i efectuar operacions diverses, com per exemple, fer tràmits amb l'administració a través de les seves oficines virtuals (sense necessitat d'haver-hi d'anar en persona), signar correus i realitzar, entre d'altres, transaccions segures per Internet.

Hi ha diversos organismes autoritzats per expedir aquestes identificacions electròniques, entre els quals cal esmentar l'**Agència Catalana de Certificació**.

Per a més informació sobre la identificació electrònica visiteu el web www.idcat.cat.

Quan anem personalment a la seu física d'aquesta entitat ens proporcionen un programari en un dispositiu com el que podeu veure a la figura 1.24. Seguint les instruccions adjuntes, el podrem instal·lar als nostres ordinadors i començar a utilitzar la nostra signatura digital. Tot i que, com s'ha vist, la teoria dels criptosistemes de clau pública no és senzilla, per usar el nostre certificat no necessitem tenir cap coneixement criptogràfic.

FIGURA 1.24. Clauer idCAT: llapis de memòria que conté la identificació electrònica d'un usuari

Llei de signatura electrònica

A Espanya, la Llei 59/2003 de signatura electrònica, reconeix tres tipus de signatura electrònica:

- **Simple**: permet identificar el firmant (autenticació).
- **Avançada**: permet identificar la persona que signa i detectar qualsevol modificació en les dades signades (autenticació i integritat).
- **Reconeguda**: és la signatura més completa. Es basa en un certificat reconegut i es genera mitjançant un dispositiu segur de creació de signatures. S'equipara a la signatura manuscrita.

2. Implantació de tècniques d'accés remot

Existeix un conjunt de configuracions de seguretat, ja siguin de programari, de maquinari o mixtes, que permeten l'accés segur a la xarxa d'informació des de l'exterior. Sense aquesta possibilitat, la xarxa perdria un dels seus aspectes essencials i no hi hauria la possibilitat d'usar o compartir els seus recursos des de localitzacions remotes. A més de poder efectuar aquesta connexió, cal que les tècniques que s'usin puguin garantir que l'accés remot sigui segur.

2.1 Seguretat perimètrica

Qualsevol xarxa de comunicacions està interconnectada amb altres. El punt on s'enllacen dues xarxes és un dels seus punts més dèbils. Per tant, s'ha de tenir especial cura a assegurar aquestes zones.

Amb l'establiment de seguretat perimètrica es busca:

- Rebutjar connexions a serveis crítics.
- Permetre només determinat trànsit (com per exemple, el correu electrònic) o només entre determinats nodes.
- Proveir la xarxa d'un únic punt d'interconnexió amb l'exterior.
- Tenir un control i dirigir el trànsit entrant exclusivament als sistemes adients dins de la intranet.
- Ocultar sistemes o serveis vulnerables que poden ser complicats de protegir dels atacs de l'exterior.
- Auditar el trànsit entre l'exterior i l'interior.
- Dificultar l'accés a informació que permeti saber coses de la xarxa com ara noms de sistemes, topologia de la xarxa, tipus de dispositius de xarxa o comptes d'usuaris interns.

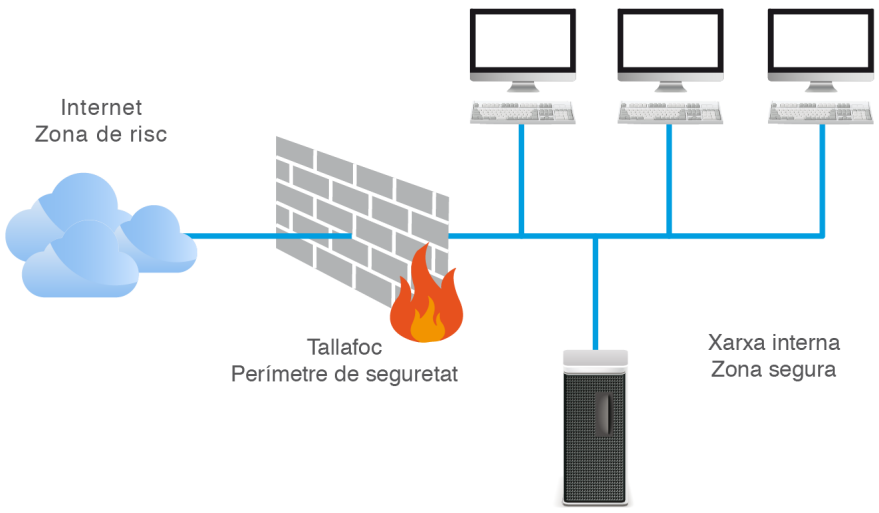
La **seguretat perimètrica** és un dels mètodes de defensa d'una xarxa. Es basa en l'establiment de recursos de seguretat en la zona de contacte de la xarxa amb l'exterior de l'organització. Això permet l'accés d'usuaris interns o externs a determinats serveis.

2.1.1 Elements bàsics de la seguretat perimètrica

Els elements bàsics que configuren la seguretat perimètrica, que es poden veure a la figura 2.1, són els següents:

- **Zona de risc o xarxa externa**. És aquella part que es considera que pot posar en risc el sistema informàtic. Usualment es considera Internet com la zona de risc.
- **Zona segura o xarxa interna**. És la part que volem protegir: els usuaris finals de sistemes, els servidors que contenen dades privades i tots els altres sistemes que no volem que siguin coneguts pel "món exterior".També se'n diu *xarxa protegida*, *xarxa de confiança* o *xarxa interna*.
- **Perímetre de xarxa o tallafoc**. El perímetre de xarxa és la part que separa la zona segura de la de risc. Genèricament s'anomena *tallafoc* al perímetre de xarxa. Entenem per tallafoc, per tant, un sistema o xarxa que aïlla una xarxa d'una altra.

FIGURA 2.1. Elements de seguretat de xarxa



Partint d'aquesta definició, doncs, un tallafoc pot ser un encaminador, un equip que executa un programa especial o qualsevol altre dispositiu o xarxa de dispositius en què es duu a terme un conjunt d'activitats per controlar el trànsit entrant i sortint. Així, les funcions del tallafoc les poden dur a terme dispositius com programes, encaminadors o ordinadors dedicats exclusivament a les tasques de filtració de paquets (servidors intermediaris o *proxy*).

Equip bastió

L'equip que està directament connectat a altres xarxes, com per exemple Internet, s'anomena *equip bastió* (*host bastion* en anglès). És el més vulnerable, i per tant la primera línia de defensa de la xarxa.

La creació d'aquesta zona perimètrica o tallafoc s'ha de fer tenint en compte tant l'estructura de la xarxa com els serveis que han de quedar disponibles per als usuaris.

Els tallafocs són, probablement, un dels elements més importants per a la seguretat de la nostra xarxa, i hem de considerar, a l'hora d'instal·lar-los, els aspectes següents:

- No s'han d'emprar en lloc d'altres eines, sinó conjuntament amb aquestes. Hem de tenir en compte que el tallafoc serà el punt que rebrà tots els atacs sobre el nostre sistema.
- En centralitzar una bona part de les mesures de seguretat de la xarxa en un únic sistema (no cal que sigui un únic dispositiu), si aquest es veu compromès, la xarxa quedarà exposada als atacs dels intrusos.
- Pot proporcionar una falsa sensació de seguretat. No per instal·lar un tallafoc podem assumir que la xarxa és segura i prescindir de vigilar els equips interns de la xarxa.

Un sistema tallafoc realitza les activitats següents:

- **Filtrat de trànsit d'entrada i sortida**. Aquest filtrat es pot fer tant a nivell de connexió, de la capa de xarxa (conegut com a *filtrat de paquets*) o de la capa d'aplicació. Es realitza una inspecció de les capçaleres dels paquets IP. El criteri per deixar-los passar es basa principalment en una combinació de la seva adreça IP d'origen, adreça IP de destinació, port d'origen i port de destinació (de servei).
- **Ocultació** de la configuració de la xarxa a l'exterior.
- **Servidor intermediari**. Es un programari o dispositiu que actua en nom d'un altre. Per exemple, si un ordenador A fa una petició a un ordenador C de fora de la xarxa, no li ho demana directament. A fa la petició a un ordinador B (*proxy*) i aquest la fa a C. Aquesta funcionalitat permet tenir una memòria cau, control d'accés i registre de trànsit.
- **Monitoratge**. Com que tot el trànsit d'entrada i sortida passa pel sistema tallafoc, és possible motoritzar moltes coses, com per exemple connexions, adreces IP, ports o llocs web. Amb el monitoratge es busca descobrir els intents d'atacs i trames sospitoses i registrar els tipus de paquets rebuts, així com la freqüència de paquets, adreces font i destinació, intents d'ús de protocols protegits, intents de falsificació, trames rebudes des d'encaminadors desconeguts... Com que la quantitat de fitxers de registre generats pot ser molt gran, cal considerar l'ús d'eines que automatitzin el monitoratge.

En general, cal prendre unes decisions bàsiques en la configuració d'un tallafoc.

En primer lloc, cal definir una política de seguretat i implementar el nivell de monitoratge i de control desitjat en l'organització. S'ha d'indicar bàsicament què s'ha de permetre i què s'ha de denegar. Existeix la possibilitat d'emprar una política restrictiva, en què es denega tot allò que explícitament no es permet o una política amb permís, en la qual es permet tot, excepte el que s'ha negat explícitament.

D'altra banda, la configuració i el nivell de seguretat potencial del tallafoc depèn de l'ús del dispositiu. Així, si connecta dues subxarxes diferents la política serà diferent que si ha de filtrar els paquets de l'organització amb l'exterior.

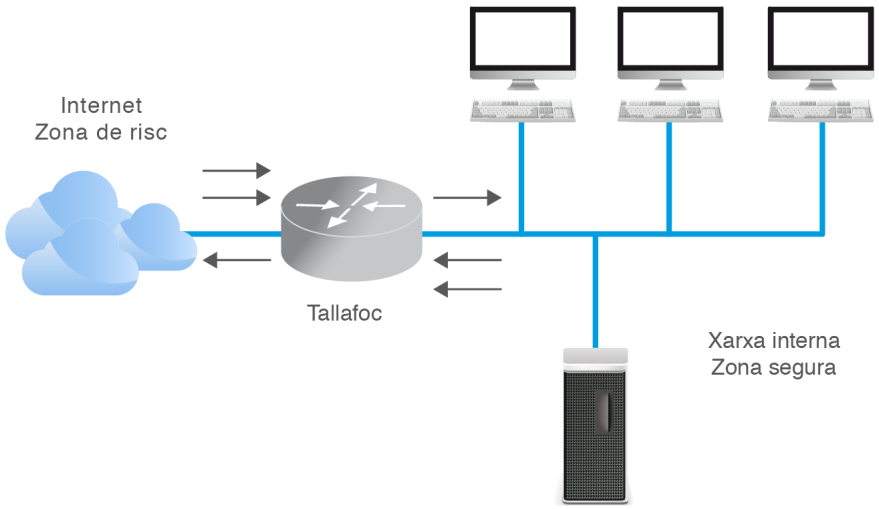
Per últim, cal tenir en compte que la inversió ha d'ésser proporcional al valor estimat del que desitgem protegir. Un sistema de tallafoc pot ser molt barat o costar milers d'euros.

2.1.2 Perímetres de xarxa. Zones desmilitaritzades

El perímetre de xarxa, com hem comentat, conté el que genèricament s'anomena *sistema tallafoc*. Aquest, però, pot ser un o més dispositius amb diverses configuracions d'arquitectures de seguretat possibles.

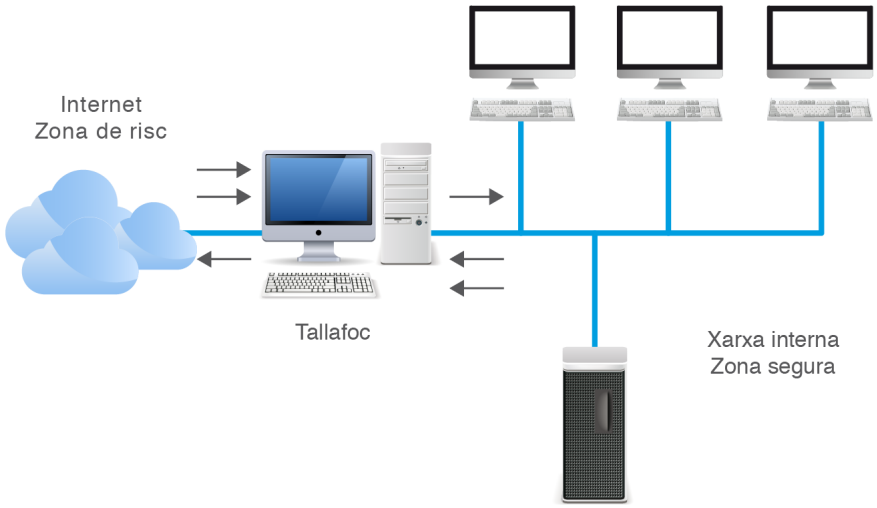
- ***Tallafoc de filtrat de paquets***. És la configuració més simple, tal com es veu a la figura 2.2. Es col·loca un dispositiu que disposa d'una única interfície de xarxa. L'encaminador extern està configurat per enviar les dades al dispositiu i els clients interns hi envien també les dades de sortida. L'encaminador avalua les dades segons unes regles de seguretat. Aquest sistema és conegut en anglès com a *screeneing router*.

FIGURA 2.2. Tallafoc en configuració de filtrat de paquets



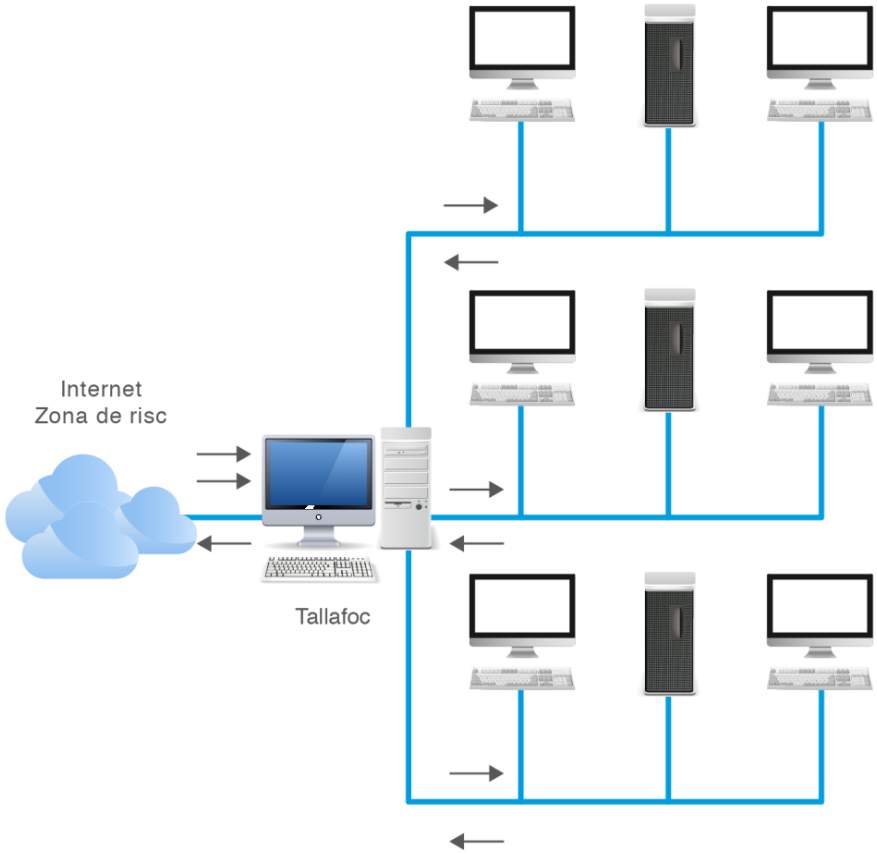
- ***Amfitrió de dues bases (dual-homed host)***. En aquesta arquitectura s'instal·la un dispositiu que té almenys dues interfícies de xarxa. L'avantatge d'usar aquest esquema és que crea una ruptura entre les xarxa externa i interna, la qual cosa permet que tot el trànsit d'entrada i sortida passi per l'equip. El sistema necessita un servidor intermediari per a cadascun dels serveis que vulguem tenir actius. L'esquema bàsic es pot veure a la figura 2.3.

Figura 2.3. Tallafoc en configuració dual-homed



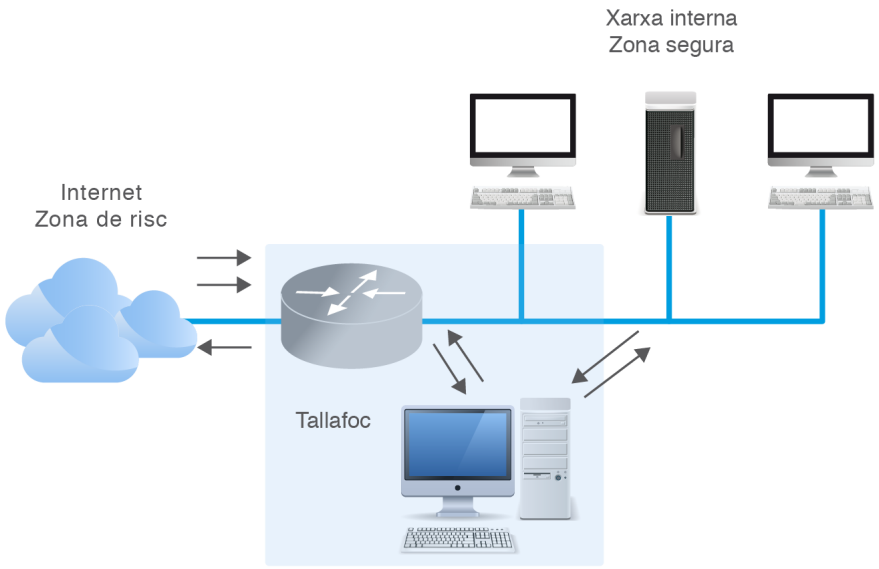
- ***Amfitrió multi-base (multihomed host bastion)***. L'evolució del cas anterior significa tenir més d'una interfície de xarxa en el dispositiu. Habitualment una interfície de xarxa va a la xarxa externa i la resta a la xarxa interna. Aquesta arquitectura permet distribuir el trànsit per les diferents interfícies de xarxa depenent de la destinació. Afegeix un nivell més alt de seguretat, tal com es pot veure a la figura 2.4.

Figura 2.4. Tallafoc en configuració multihomed



- ***Amfitrió de monitoratge (screened host)***. Com es pot veure a la figura 2.5, combina dos elements de seguretat. Un encaminador, connectat a la xarxa insegura i que realitza un filtrat de paquets, i un equip, accessible des de l'exterior on hi ha el servidor intermediari de la xarxa. D'aquesta manera, el filtrat es fa en un equip, protegint la xarxa, i l'accés als serveis es fa en un segon nivell, amb el sistema *proxy*.

FIGURA 2.5. Tallafoc en configuració screened host

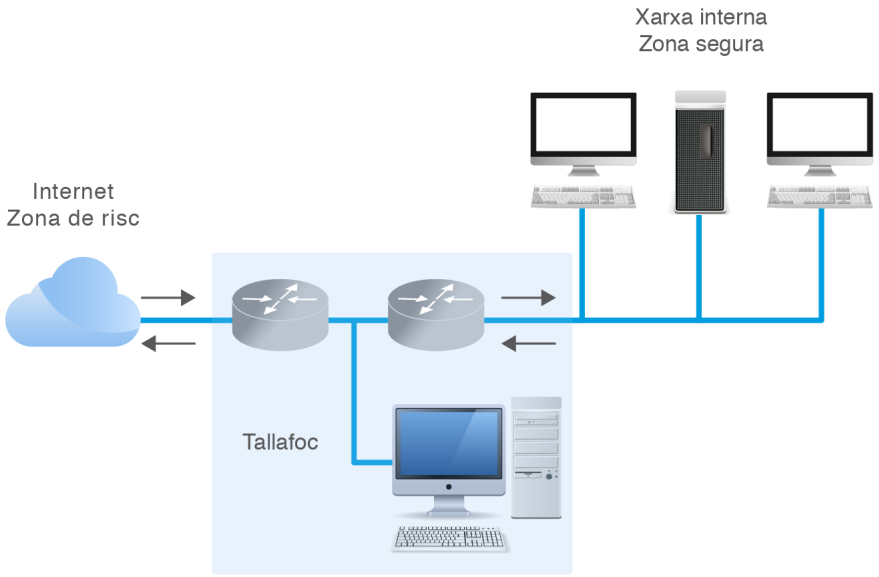


- ***Subxarxa protegida (screened subnet)***. Un pas més en l'arquitectura de seguretat consisteix en que entre la xarxa interna i l'externa hi hagi tot un subsistema que incorpori seguretat d'entrada, seguretat de sortida i el conjunt de serveis que es vol que siguin visibles des de l'exterior. No només aïlla la xarxa interna i externa, sinó que es crea una xarxa intermèdia. Afegeix una xarxa perimetral que aïlla la xarxa interna d'Internet. Aquesta xarxa intermèdia s'anomena **DMZ o zona desmilitaritzada**.

  L'objectiu d'una DMZ és que les connexions que provenen de la xarxa interna i les que provenen de la xarxa externa estiguin permeses. En canvi, les connexions des de la DMZ només estan permeses cap a la xarxa externa. Per tant, els equips (*hosts*) de la DMZ no poden connectar amb la xarxa interna. Això permet que els equips de la DMZ puguin donar serveis a la xarxa externa i a la vegada protegeixen la xarxa interna en el cas que intrusos comprometin la seguretat dels equips situats a la zona desmilitaritzada.

  D'aquesta manera es redueixen considerablement els efectes d'un atac al sistema. En les arquitectures anteriors, tota la seguretat estava centrada en l'equip bastió i si la seguretat es veia compromesa, la resta de la xarxa queda automàticament exposada. Com que l'equip bastió és un objectiu interessant per a molts atacants, l'arquitectura DMZ és un intent d'aïllar-la en una xarxa perimètrica de manera que l'intrús que accedeixi a aquesta màquina no aconsegueixi un accés total a la subxarxa protegida. L'esquema bàsic és a la figura 2.6.

FIGURA 2.6. Tallafoc en configuració screened subnet



En aquesta xarxa perimetral es poden incloure sistemes que facin molt ús de connexió a la xarxa externa. Poden ser, entre altres, servidors de correu, servidors web o DNS. Aquests dispositius seran els únics elements visibles des de l'exterior. D'aquesta manera un atacant hauria de trencar la seguretat d'ambdós encaminadors per accedir a la xarxa protegida. També, si és necessari, es poden definir diverses xarxes perimetrals en sèrie. En aquest escenari, els serveis de menor fiabilitat es posaran a les xarxes més externes.

Les regles de filtrat han de ser diferents en cada nivell. Altrament, no obtindríem major seguretat, ja que si s'aconsegueix trencar-ne una es poden trencar totes.

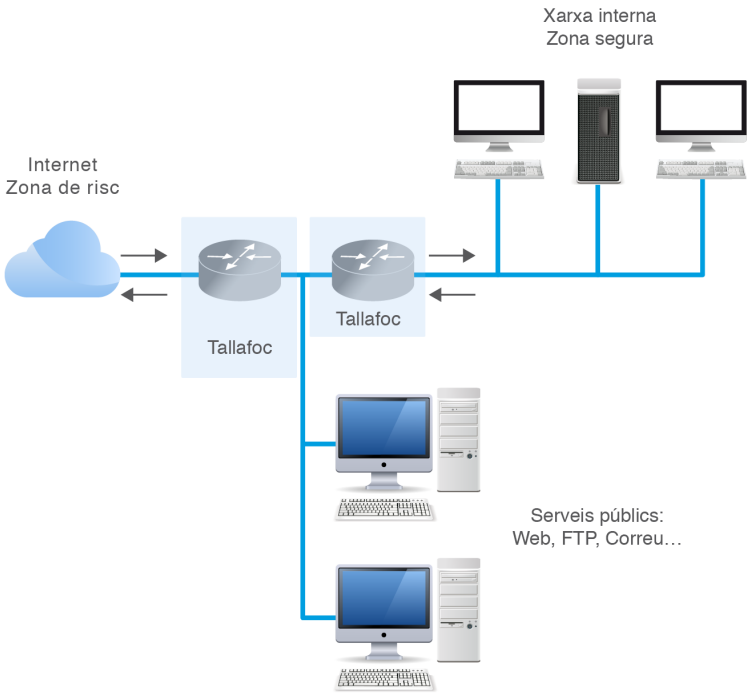
Les arquitectures **DMZ** són les més usades per la seguretat que proporcionen, tot i que són les més complexes de gestionar.

2.1.3 Arquitectura feble de subxarxa protegida

Existeixen diverses arquitectures DMZ. L'arquitectura feble de subxarxa protegida n'és una. Els elements es col·loquen tal com mostra la figura 2.7.

S'utilitzen dos encaminadors, anomenats *exterior* i *interior*, connectats a la xarxa perimètrica. En aquesta xarxa perimètrica, que constitueix el sistema tallafoc, s'inclou l'equip bastió i també s'hi poden incloure sistemes que requereixin un accés controlat, com el servidor web o el servidor de correu. Aquests seran els únics elements visibles des de fora de la xarxa. L'encaminador exterior bloqueja el trànsit no desitjat entre la xarxa perimètrica i la xarxa externa, mentre que l'interior fa el mateix però amb el trànsit entre la xarxa interna i la perimètrica. Un atacant hauria de trencar la seguretat d'ambdós encaminadors per accedir a la xarxa protegida.

FIGURA 2.7. Tallafoc en configuració d'arquitectura feble de subxarxa protegida



Alguns dels avantatges d'aquesta arquitectura són:

- Evitar l'existència d'un un únic punt dèbil. Ara cal trencar més d'un element de seguretat per accedir a la xarxa interna.
- Els serveis que s'han de veure des d'Internet estan a la DMZ.
- La xarxa interna està oculta i no és visible des de la xarxa externa.

L'arquitectura, però, no està exempta de problemes:

- És possible implementar una zona desmilitaritzada amb un únic encaminador que tingui tres o més interfícies de xarxa. Aquesta arquitectura no és gens recomanable perquè si es compromet aquest element es trenca tota la nostra seguretat. La idea de la DMZ és que cal comprometre dos encaminadors, tant l'extern com l'intern.
- Tota la seguretat està basada en els dos encaminadors. Existeixen arquitectures amb elements més segurs que un encaminador.

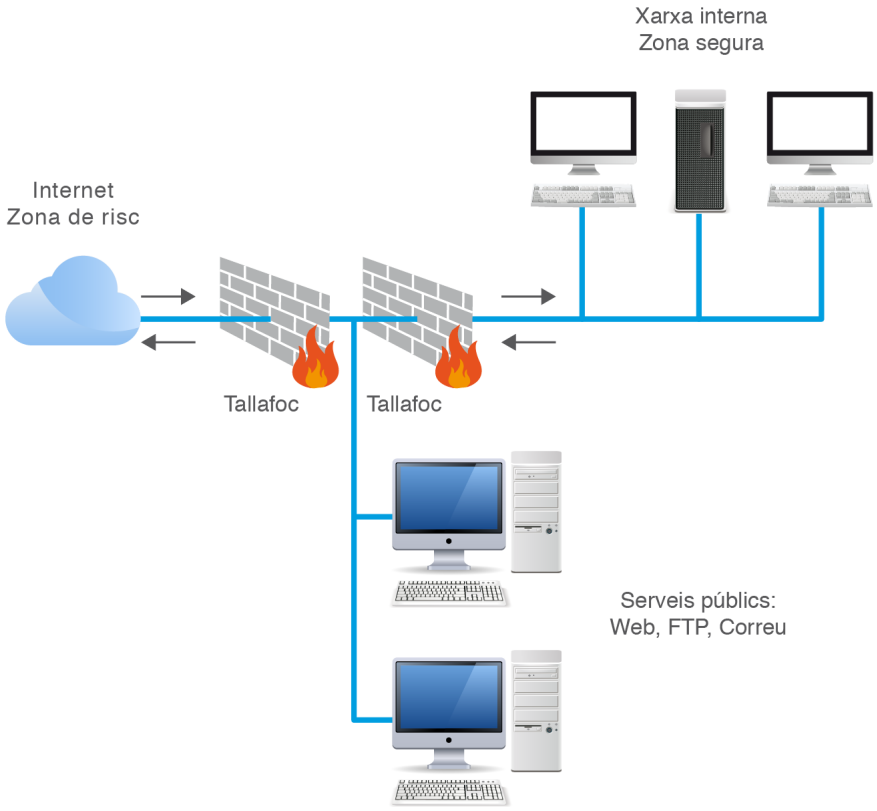
La configuració de DMZ amb un únic encaminador amb tres interfícies de xarxa s'anomena *three-legged firewall*.

2.1.4 Arquitectura forta de subxarxa protegida

L'arquitectura DMZ es basa en dos encaminadors. El principal problema és que els encaminadors són menys segurs que un conjunt de dispositius correctament

configurats. És a dir, un tallafoc. En la figura 2.8 podem veure com es col·loquen els elements per configurar l'arquitectura de seguretat.

Figura 2.8. Tallafoc en configuració d'arquitectura forta de subxarxa protegida



La complexitat d'aquesta arquitectura comporta problemes com la gestió, el cost o el rendiment del trànsit amb la xarxa externa. Alguns dels avantatges són la seva elevada modularització i l'augment de seguretat que comporta.

2.2 Xarxes privades virtuals. VPN

Una **xarxa privada virtual**o VPN (*Virtual Private Network)* és una xarxa privada que s'estén a diferents punts remots mitjançant l'ús d'infraestructures públiques de transport (com per exemple, Internet). La transmissió de paquets de dades es realitza mitjançant un procés d'encapsulació i, per seguretat, de xifrat, ja que no cal oblidar que les dades circulen durant un temps per trams de xarxa pública. Aquests paquets de dades de la xarxa privada viatgen a través d'un "túnel" definit a la xarxa pública. És a dir, s'aprofita el baix cost de l'accés a Internet, s'afegeixen tècniques de xifratge fort per aconseguir seguretat i se simulen les clàssiques connexions punt a punt.

Així, un usuari (una sucursal de l'organització, un teletreballador, un representant comercial...) connectat a través d'Internet a la xarxa corporativa de l'organització,

establint un túnel VPN, pot funcionar com si estigués dins de l'organització a tots els efectes de connectivitat.

En el cas d'accés remot des d'un equip, la VPN permet a l'usuari accedir a la seva xarxa corporativa i li assigna al seu ordinador remot les adreces i privilegis d'aquesta xarxa, encara que la connexió s'hagi efectuat mitjançant una xarxa pública com Internet.

La característica que converteix la connexió "pública" en "privada" és el que s'anomena un *túnel*, terme referit a que únicament ambdós extrems són capaços de veure el que es transmet pel túnel, convenientment xifrat i protegit de la resta d'Internet. La tecnologia de túnel xifra i encapsula els protocols de xarxa que s'utilitzen en els extrems sobre el protocol IP. D'aquesta manera podem operar com si es tractés d'un enllaç dedicat convencional, de forma transparent per a l'usuari.

2.2.1 Beneficis i inconvenients de les VPN envers les línies dedicades

Una connexió VPN permet tenir una connexió de xarxa amb totes les característiques de la xarxa privada a la qual ens volem connectar. El client VPN passa a ser un equip igual que la resta dels connectats al sistema. Tindrà, per tant, tots els permisos i directrius de seguretat d'un ordenador de la xarxa. Tot plegat té un seguit d'avantatges i alguns inconvenients.

Avantatges:

- **Seguretat**: és possible assegurar diversos serveis amb aquest mecanisme.
- **Mobilitat**: tenim una connexió segura entre usuaris mòbils i la nostra xarxa fixa, amb independència de la localització geogràfica.
- **Transparència**: permet la interconnexió d'ordenadors en un sistema informàtic, però també de diferents xarxes. Tot de manera transparent per a l'usuari final, ja que la configuració es pot fer només en l'entorn de passarel·la (sistema de maquinari i programari per interconnectar dues xarxes que utilitzen protocols diferents).
- **Simplicitat**: una VPN aconsegueix que l'equip sigui vist per tota la xarxa, incloent servidors, la qual cosa simplifica l'administració d'equips remots.
- **Estalvi econòmic**: el trànsit segur de paquets per xarxes públiques té un cost econòmic sensiblement menor que la creació d'una xarxa dedicada.

Inconvenients:

- **Fiabilitat**: la dependència del proveïdor de xarxa (ISP) pot produir fallades en la xarxa que poden deixar incomunicats recursos de la nostra VPN.

- **Confiança**: si la seguretat d'un node o subxarxa que forma part d'una VPN queda compromesa es veurà afectada la seguretat de tots els components de la xarxa.

2.2.2 Nivell de xarxa a VPN: SSL, TLS i IPSec

Com hem comentat, per implementar una VPN necessitem un protocol que xifri les comunicacions per evitar que puguin ser vistes per terceres persones. Existeixen diversos protocols criptogràfics per fer comunicacions punt a punt (VPN) a través d'Internet.

SSL

El *Secure Sockets Layer* o SSL ens dona autenticació i privacitat de la informació entre extrems a Internet mitjançant l'ús de criptografia. Habitualment, només s'autentica (es garanteix la seva identitat) el servidor, mentre que el client es manté sense autenticar.

Etapes bàsiques de l'SSL:

- Negociar entre les parts l'algorisme que s'utilitzarà en la comunicació. En aquesta etapa, client i servidor negocien els algorismes criptogràfics a utilitzar. Alguns dels algorismes més usats són RSA, Diffie-Hellman, DSA, RC2, RC4, IDEA (*International Data Encryption Algorithm*), DES (*Data Encryption Standard)*, Triple DES i AES (*Advanced Encryption Standard*) o SHA.
- Intercanviar les claus.
- Fer la transmissió.

TLS

El *Transport Layer Security* o TLS és una evolució del protocol SSL. La connexió es fa mitjançant un canal xifrat entre el client i servidor. D'aquesta manera l'intercanvi d'informació es realitza en un entorn segur i lliure d'atacs. Normalment, el servidor és l'únic que és autenticat, garantint així la seva identitat. El client es manté sense autenticar, ja que per a l'autenticació mútua es necessita una infraestructura de claus públiques.

IPSec

L'*Internet Protocol Security* o (IPSec) és un conjunt d'estàndards industrials que comproven, autentiquen i xifren les dades en els paquets IP. IPSec aporta diverses propietats: confidencialitat mitjançant el xifratge de trànsit IP, autenticació i

prevenció contra els atacs de reproducció i integritat mitjançant el rebuig del trànsit modificat. L'IPSec utilitza certificats (signats digitalment per una entitat emissora de certificats) per comprovar la identitat d'un usuari, equip o servei, que enllacen de forma segura una clau pública a l'entitat que disposa de la clau privada corresponent.

2.2.3 Nivell d'aplicació a VPN. L'SSH

El *Secure Shell* o SSH és un protocol que permet als equips establir una connexió segura, de manera que un client (un usuari o fins i tot un equip) pot obrir una sessió interactiva en una màquina remota (servidor) per enviar ordres o fitxers a través d'un canal segur.

- Les dades que circulen entre el client i el servidor estan **xifrades**, la qual cosa en garanteix la confidencialitat (ningú més que el servidor i el client poden llegir la informació que s'envia per la xarxa).
- **El client i el servidor s'autentifiquen mútuament** per assegurar que les dues màquines que es comuniquen són, de fet, aquelles que les altres parts creuen que són. L'intrús informàtic ja no pot adoptar la identitat del client o del servidor.

Una connexió SSH s'estableix en diverses fases:

- Es determina la **identitat** del servidor i del client per establir un canal segur (capa segura de transport). El client inicia sessió en el servidor.
- Establiment d'un **canal segur**. L'establiment d'una capa segura de transport comença amb la fase de negociació entre el client i el servidor per posar-se d'acord en els mètodes de xifratge que volen utilitzar. El protocol SSH està dissenyat per treballar amb un gran nombre d'algorismes de xifrat, per això, tant el client com el servidor han d'acordar primer els algoritmes que admeten.
- **Autenticació**. Un cop s'ha establert la connexió segura entre el client i el servidor, el client s'ha de connectar al servidor per obtenir un dret d'accés. Hi ha diversos mètodes:
- El mètode més conegut és la **contrasenya** tradicional. El client envia un nom d'accés i una contrasenya al servidor mitjançant la connexió segura i el servidor verifica que l'usuari en qüestió té accés a l'equip i que la contrasenya subministrada és vàlida.
- Un mètode menys conegut, però més flexible, és l'ús de **claus públiques**. Si el client tria la clau d'autenticació, el servidor crearà un desafiament (*challenge)* i donarà accés al client si aquest és capaç de desxifrar el desafiament amb la seva clau privada.

2.3 Servidors d'accés remot

Un **servidor d'accés remot** és un equip que permet a altres equips connectar-s'hi i a través seu permet l'accés a dispositius o informació que estan a la xarxa. La connexió es pot fer, per exemple, per via telefònica o per Internet.

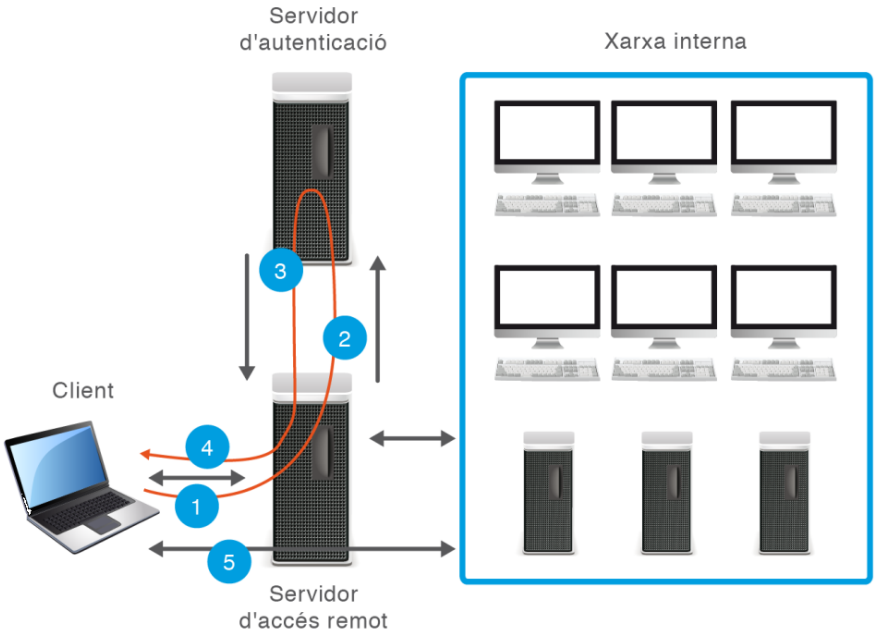
Els servidors d'accés remot també s'anomenen *servidors de comunicacions*. El terme anglès es *Remote Access Server* (RAS).

El servidor RAS controla les línies d'accés, com per exemple mòdems o altres canals de comunicació de la xarxa, perquè les peticions connectin amb la xarxa. El servidor reconeix la petició de la xarxa i realitza l'autenticació i els procediments necessaris per registrar un usuari a la xarxa i permetre-li l'accés als recursos.

Una vegada l'usuari s'ha autenticat, pot accedir a les unitats i impressores compartides com si estigués connectat físicament a la xarxa de l'organització. El servidor RAS conté múltiples canals de comunicació junts. Els canals són bidireccionals i, per tant, diversos equips es poden connectar a un únic recurs o un únic equip es pot connectar a múltiples recursos.

En la figura 2.9 es poden veure els passos necessaris per accedir als recursos de la xarxa.

FIGURA 2.9. Passos per poder accedir a recursos remots des d'un client



Les xarxes de banda ample com ADSL han deixat obsolet l'ús dels mòdems a través de la línia telefònica.

1. El primer pas (tal com es veu a la figura 2.9) és la connexió a l'equip. Es pot fer via mòdem (ja obsolet) o per una xarxa pública com Internet.

2. L'autenticació es realitza mitjançant un servidor d'autenticació, que garanteix que els elements són qui diuen que són. Aquest servidor d'autenticació pot ser un procés dins del mateix servidor d'accés remot, pot ser un altre servidor de l'organització o fins i tot un servidor aliè. Aquest darrer cas s'aplica amb els dipòsits de claus en estructura de clau asimètrica.

3. El servidor d'autenticació dona el vistiplau a les entitats, i envia al servidor d'accés remot els privilegis i credencials que la connexió, ara amb l'usuari conegut, té.
4. El servidor d'accés remot notifica al client que ha estat correctament identificat i que pot iniciar les peticions de recursos remots.
5. Una vegada autenticades les entitats, el servidor d'accés remot proveeix la comunicació entre el client i els recursos sol·licitats (la xarxa interna).

2.3.1 Protocols d'autenticació

La major part dels sistemes informàtics i xarxes mantenen de una manera o altra una relació d'identitats personals (usuaris) associades normalment amb un perfil de seguretat, rols i permisos. L'autenticació d'usuaris és el pas més crític en la connexió a un servidor d'accés remot ja que cal verificar la identitat de l'entitat que demana permís per accedir als recursos. Els sistemes d'autenticació permeten a aquests sistemes assumir amb una seguretat raonable que qui s'està connectant és qui diu ser. Això, posteriorment, permet que les accions que s'executin en el sistema puguin relacionar-se amb aquesta identitat i aplicar els mecanismes d'autorització i d'auditoria oportuns.

Un protocol d'autenticació és un tipus de protocol criptogràfic que té el propòsit d'autenticar (identificar) de manera unívoca entitats que desitgen comunicar-se de forma segura. Els protocols d'autenticació es negocien immediatament després de determinar la qualitat de l'enllaç i abans de negociar el nivell de xarxa.

L'autenticació és el pas preliminar per tenir accés als recursos remots.

El procés general d'autenticació consta dels passos següents:

- L'usuari sol·licita accés al sistema.
- El sistema demana a l'usuari que s'autentiqui.
- L'usuari aporta les credencials que l'identifiquen i permeten verificar l'autenticitat de la identificació.
- El sistema valida segons les seves regles si les credencials aportades són suficients per donar accés a l'usuari o no.

Alguns dels protocols d'autenticació més usats són PAP, CHAP, EAP, PEAP i Kerberos.

PAP

SPAP

El SPAP (*Shiva Password Authentication*) és el protocol d'autenticació de contrasenya de Shiva. És una variant del PAP. El client envia una contrasenya xifrada al servidor d'accés remot. Aquest desxifra la contrasenya i contesta en clar per autenticar al client d'accés remot.

El PAP (*Password Authentication Protocol*) és un protocol d'autenticació simple en el qual el nom d'usuari i la contrasenya s'envien al servidor d'accés remot en text clar (sense xifrar). No es recomana utilitzar PAP, ja que les contrasenyes es poden llegir fàcilment. El PAP només s'usa per connectar a servidors d'accés remot antics basats en Unix que no admeten mètodes d'autenticació més segurs.

CHAP

El CHAP (*Challenge Handshake Authentication Protocol*) és un mètode d'autenticació usat per servidors als quals s'accedeix a través del protocol PPP (*Point-to-Point Protocol*). El CHAP verifica la identitat del client amb un procés de tres etapes. Periòdicament repeteix el procés de verificació.

L'MS-CHAP és una variant del protocol d'autenticació CHAP usat per Microsoft.

- S'estableix l'enllaç i l'autenticador envia un missatge per demanar a l'usuari que s'identifiqui.
- L'equip usuari respon amb un valor calculat, una funció resum d'un sol sentit, com per exemple la suma de comprovació MD5.
- L'autenticador verifica la resposta amb el resultat d'un càlcul propi del *hash*. Si el valor coincideix, l'autenticador informa de la verificació, si no, anul·la la connexió.
- Cada cert temps, a l'atzar, l'autenticador realitza una nova comprovació de veracitat, tot repetint el procés.

EAP: autenticació extensible

L'EAP (*Extensible Authentication Protocol*) és un protocol per donar suport a mecanismes d'autenticació. Ofereix funcions per poder negociar els mecanismes d'autenticació escollits. Aquests mecanismes són anomenats mètodes EAP. Està definit en el memoràndum RFC 3748.

L'EAP s'ha fet molt popular en xarxes sense fil, com per exemple l'estàndard IEEE 802.11, WPA o WPA2.

PEAP: protocol d'autenticació extensible protegit

El PEAP (*Protected Extensible Authentication Protocol)* és un protocol de la família de protocols EAP. Utilitza seguretat de nivell de transport (TLS) per crear un canal xifrat entre un client d'autenticació PEAP (com un equip amb connexió sense fill) i un autenticador PEAP (per exemple un servei d'autenticació remota com RADIUS).

Per millorar els protocols EAP així com la seguretat de xarxa, el PEAP proporciona:

- Protecció de la negociació del mètode EAP. Aquesta es realitza entre el client i el servidor usant un canal TLS. D'aquesta manera s'impedeix que un intrús insereixi paquets entre el client i el servidor. El canal TLS xifrat també ajuda a evitar atacs per denegació de servei.
- Autenticació mútua.
- Protecció contra la creació d'un punt d'accés sense fils (WAP) no autoritzat.
- Reconnexió ràpida, que redueix el temps de retard entre la sol·licitud d'autenticació d'un client i la resposta del servidor d'autenticació.

El procés d'autenticació PEAP entre el client i l'autenticador PEAP es fa en dues etapes. Primer es configura un canal segur entre el client i el servidor d'autenticació. En la segona es produeix l'autenticació EAP entre el client i l'autenticador EAP.

Kerberos

El procediment usat per Kerberos s'anomena *autenticació mútua*. Tant el client com el servidor verifiquen la identitat de l'altre.

Kerberos és un protocol d'autenticació de xarxes basat en el protocol de Needham-Schroeder. Permet a dos ordinadors en una xarxa insegura demostrar la seva identitat. Kerberos es basa en criptografia de clau simètrica i necessita d'una tercera part de confiança.

Hi ha extensions del protocol Kerberos que permeten utilitzar criptografia de clau asimètrica.

La tercera part de confiança s'anomena *centre de distribució de claus* o KDC. Consta de dues parts lògiques separades. Un servidor d'autenticació i un servidor de tiquets. Els tiquets usen per demostrar la identitat dels usuaris. El sistema manté una base de dades de claus secretes. Cada entitat, ja sigui client o servidor la comparteix i és coneguda només per ell i Kerberos. El coneixement d'aquesta clau serveix per provar la identitat de l'entitat i assegurar la comunicació.

El funcionament, bàsicament, és el següent. El client s'autentica a sí mateix contra el servidor d'autenticació. El client rep la verificació i l'utilitza per demostrar al servidor de tiquets la seva identitat. El servidor de tiquets crea un tiquet, l'encripta amb les claus de l'usuari i li envia. A partir d'aquest moment ja es pot fer ús del servei.

El tiquet es configura perquè caduqui al cap d'un temps, habitualment unes hores. Un tiquet compromès, per tant, només serviria a l'intrús durant un breu període de temps.

2.3.2 Configuració de paràmetres d'accés

La connexió d'un equip client a una xarxa necessita diversos paràmetres per assegurar que la connexió es realitza correctament. Aquests paràmetres bàsicament han de contenir els elements per autenticar-se i els elements que ens permeten establir la connexió amb l'equip d'accés remot. Serà l'equip remot, usant el servidor d'autenticació, el que gestionarà els nostres privilegis efectius dins de la xarxa de l'organització.

En l'equip client és necessari:

Al web d'aquesta unitat podeu consultar l'annex "Xarxes Privades Virtuals" on s'explica pas a pas la configuració d'una xarxa pública virtual o VPN.

- El protocol de comunicació que haurà d'usar el client per connectar-se al servidor d'accés remot. A vegades l'equip client no té el controlador amb el protocol i cal instal·lar-lo. Passa , per exemple, amb l'IPSec en Windows XP.
- Els elements d'autenticació de l'entitat, que usualment són l'usuari i la contrasenya.

- El nom o la IP de l'equip d'accés remot amb qui farem la connexió.
- Elements addicionals, com per exemple el certificat digital si s'utilitzen protocols que requereixin criptografia de clau pública.

2.3.3 Servidors d'autenticació

El servidor d'autenticació és un dispositiu que controla qui pot accedir a una xarxa informàtica. Ha de proveir a la xarxa les funcions d'autorització, privacitat i no repudi. L'autorització determina els privilegis atorgats a una entitat o usuari i, per tant, a quins objectes o dades l'usuari pot tenir accés. La privacitat assegura que la informació es divulgui només a persones autoritzades. El no repudi es refereix al fet que el servidor d'autenticació pot registrar tots els accessos a la xarxa i les dades d'identificació. D'aquesta manera, un usuari no pot negar que ha accedit a un equip o que n'ha modificat les dades. Molt sovint, el no repudi és un requisit legal.

El servidor d'autenticació verifica mitjançant un protocol d'autenticació la identitat de l'equip que desitja connectar-se. Una vegada feta l'autenticació, llavors un servidor d'accés remot subministra els recursos.

El servidor d'autenticació conté un "diposit" (algun tipus de base de dades) amb els usuaris, permisos i credencials que el servidor d'accés remot usarà per saber el nivell de privilegis a assignar a la connexió.

Servidor d'autenticació

Un servidor d'autenticació pot estar en un servidor d'accés a la xarxa informàtica, una part d'un tallafoc o un altre tipus de maquinari per controlar l'accés a la xarxa. Independentment del tipus de màquina que allotja el programa d'autenticació, el terme servidor d'autenticació continua sent generalment utilitzat per referir-se a la combinació de maquinari i programari que realitza la funció d'autenticació.

Per tant, independent del protocol d'autenticació usat, el servidor d'autenticació ha de tenir emmagatzemada informació relacionada amb l'entitat (ja sigui un usuari o un equip remot). Existeixen, des d'aquest punt de vista, diferents servidors d'autenticació.

Entre els servidors d'autenticació més coneguts trobem:

- ***OpenLDAP***: és una implementació lliure i de font pública del protocol *Lightweight Directory Access Protocol* (LDAP) desenvolupada pel projecte OpenLDAP. L'LDAP és un protocol de comunicació independent de la plataforma.
- ***Active Directory***: és el nom utilitzat per Microsoft com a magatzem centralitzat d'informació d'un dels seus dominis d'administració.
- ***Novell Directory Services***: també conegut com eDirectory, és la implementació de Novell utilitzada per gestionar l'accés a recursos en diferents servidors i ordinadors d'una xarxa.
- ***Red Hat Directory Server***: és un servidor basat en l'LDAP que centralitza la configuració d'aplicacions, perfils d'usuaris, informació de grups i polítiques, així com informació de control d'accés, dins d'un sistema operatiu independent de la plataforma.

Tallafocs i servidors intermediaris

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

Seguretat i alta disponibilitat

Índex

Introducció **5**

Resultats d'aprenentatge **7**

1 Tallafocs **9**
1.1 Definicions importants . . . 10
1.1.1 Amenaces . . . 10
1.1.2 Tipus d'atacants . . . 12
1.1.3 Atacs comuns . . . 13
1.1.4 Els tallafocs més comuns . . . 14
1.2 Característiques i tipus de tallafocs . . . 15
1.2.1 Característiques del tallafoc . . . 15
1.2.2 Tipus de tallafocs . . . 16
1.3 Funcions principals del tallafoc . . . 20
1.4 Configuració i utilització del tallafoc . . . 22
1.4.1 Model de desenvolupament d'un tallafoc . . . 22
1.4.2 Filtratge de paquets de dades . . . 28
1.4.3 Instal·lació del tallafoc. Ubicació . . . 35
1.4.4 Regles de filtratge del tallafoc . . . 45
1.4.5 Proves de funcionament. Sondeig . . . 60
1.4.6 Registres d'esdeveniments d'un tallafoc . . . 64
1.4.7 Registre d'esdeveniments amb IPTables . . . 64
1.4.8 Registre d'esdeveniments amb NFTables . . . 65
1.4.9 Anàlisi de registres . . . 65
1.4.10 Activitat a investigar . . . 65
1.5 Exemples de tallafoc . . . 66
1.5.1 IPChains . . . 66
1.5.2 IPTables . . . 67
1.5.3 NFTables . . . 67
1.5.4 Equip bastió . . . 67
1.5.5 Uncomplicated Firewall (ufw) . . . 68
1.5.6 Gufw . . . 68
1.5.7 Firewall Builder . . . 69
1.5.8 Shorewall . . . 70
1.5.9 IPFire . . . 70
1.5.10 Tallafoc de Microsoft Windows . . . 72

2 Servidors intermediaris **73**
2.1 Característiques i tipus de servidors intermediaris . . . 74
2.2 Funcions principals dels servidors intermediaris . . . 75
2.2.1 Gestió de peticions . . . 75
2.2.2 Gestió de la velocitat de resposta . . . 76
2.2.3 Filtratge . . . 76

2.2.4 Emmascarar la identitat . . . 76
2.2.5 Continguts a demanda . . . 76
2.3 Configuració i utilització de servidors intermediaris . . . 77
2.3.1 Tipus de servidors intermediaris . . . 77
2.3.2 Exemples de servidors intermediaris . . . 80
2.3.3 Instal·lació de servidors intermediaris . . . 81
2.3.4 Configuració de filtres . . . 83
2.3.5 Configuració de l'emmagatzematge en memòria cau d'un servidor intermediari . . . 87
2.3.6 Mètodes d'autenticació d'un servidor intermediari . . . 89
2.3.7 Instal·lació i configuració de clients de servidors intermediaris . . . 91
2.3.8 Interpretació i utilització de documentació tècnica . . . 95

Introducció

Vivim en un món basat en la transmissió d'informació. Aquesta informació viatja per diferents mitjans i pot despertar l'interès de persones amb intencions no gaire bones. És imprescindible protegir-la, i no tan sols a l'hora d'emmagatzemar-la, sinó també durant el seu transport. Fa uns anys la solució era fàcil: aïllar-nos d'aquest ésser incipient que creixia lentament anomenat Internet i blindar les petites xarxes locals que es començaven a implantar... Però avui ja no poder aïllar-nos d'Internet: treballem vint-i-quatre hores connectats a la xarxa, i les xarxes locals són submons que contribueixen a la seva complexitat.

La unitat formativa "Tallafocs i servidors intermediaris" es desenvolupa dins el mòdul professional *Seguretat i alta disponibilitat*. Abans de treballar els continguts aquí presentats és recomanable conèixer la unitat formativa "Seguretat física, lògica i legislació" i la unitat formativa "Seguretat activa i accés remot", ambdues també incloses en aquest mòdul.

Aquesta unitat us ajudarà a iniciar-vos en la seguretat de les xarxes utilitzant tallafocs i servidors intermediaris. Es tracta de dos elements que són grans desconeguts, quan en realitat són part indispensable de les xarxes. És necessari entendre quines funcions tenen, quins passos s'han de seguir per instal·lar-los i quina és la metodologia correcta per fer-ne el manteniment.

L'organització de la unitat formativa es basa en dues parts diferenciades: "Tallafocs" i "Servidors intermediaris". En els dos casos s'estudiaran les seves característiques i funcions, els diferents tipus que es poden trobar, com es realitzen les configuracions bàsiques i com s'utilitzen. El material inclou exemples pràctics.

El tallafoc és l'element defensiu decisori de la xarxa informàtica. Com a tècnics haureu de ser capaços de gestionar els tallafocs amb seguretat. N'haureu de treure el màxim profit possible per protegir la xarxa.

Els servidors intermediaris principalment s'encarreguen d'emmagatzemar informació que els usuaris demanden a servidors externs; aquesta acció permet millorar la velocitat d'accés a la informació.

Per garantir la seguretat a la xarxa també caldrà conèixer la funció i el funcionament dels protocols TCP/IP, tenir clars conceptes com ara *datagrama*, *capçalera* o *adreça IP* i saber utilitzar eines com ip, ping, route o nslookup. La seguretat i l'eficiència de la xarxa depèn en un alt grau de la correcta utilització de tallafocs i servidors intermediaris.

Resultats d'aprenentatge

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

1. Implanta tallafocs per assegurar un sistema informàtic, analitzant-ne les prestacions i controlant-ne el trànsit cap a la xarxa interna.

- Descriu les característiques, tipus i funcions dels tallafocs.
- Descriu les característiques, tipus i funcions dels tallafocs.
- Classifica els nivells en els quals es realitza el filtratge de trànsit.
- Planifica la instal·lació de tallafocs per limitar els accessos a determinades zones de la xarxa.
- Configura filtres en un tallafocs a partir d'un llistat de regles de filtratge.
- Revisa els registres d'esdeveniments de tallafocs, per verificar que les regles s'apliquen correctament.
- Prova diferents opcions per implementar tallafocs, tant de programari com de maquinari.
- Diagnostica problemes de connectivitat en els clients provocats pels tallafocs.
- Elabora documentació relativa a la instal·lació, configuració i utilització de tallafocs

2. Implanta servidors intermediaris aplicant-hi criteris de configuració que garanteixin el funcionament segur del servei.

- Identifica els tipus de servidors intermediaris, les seves característiques i funcions principals.
- Instal·la i configura un servidor cau.
- Configura els mètodes d'autenticació en el servidor intermediari.
- Configura un servidor intermediari en mode transparent.
- Utilitza el servidor intermediari per establir restriccions d'accés web.
- Soluciona problemes d'accés des dels clients fins al servidor intermediari.
- Realitza proves de funcionament del servidor intermediari, monitorant la seva activitat amb eines gràfiques.
- Configura un servidor intermediari en mode invers.
- Elabora documentació relativa a la instal·lació, configuració i ús de servidors intermediaris.

1. Tallafocs

Les xarxes estan formades per multitud de dispositius, alguns dels quals juguen un paper important en el seu correcte funcionament. Dins de l'àmbit de la seguretat cal estudiar un dispositiu molt especial: el tallafoc. El tallafoc està gairebé sempre present en una xarxa, ja sigui gran o petita, empresarial o domèstica. Però sovint l'usuari n'ignora la seva presència, mentre que en altres ocasions sap que hi és però desconeix per a què serveix.

El **tallafoc** serveix per protegir la xarxa de les amenaces que es puguin presentar.

La seva invenció és fruit de la necessitat: uns atacs virals a importants entitats nord-americanes van propiciar la creació dels tallafocs com a instrument per defensar-se de la nova amenaça. De llavors ençà, el terme *tallafoc* s'ha mantingut, però l'eina ha anat evolucionant. Els tallafocs estan en constant evolució a causa del desenvolupament d'una altra entitat tecnològica: Internet.

De tallafocs n'hi ha de diversos tipus. El seu disseny i la seva evolució depenen de la idiosincràsia de cada xarxa. No només cada xarxa presenta unes determinades peculiaritats, sinó que també varia l'ús que els usuaris en fan, el contingut i naturalesa de la informació que hi circula.

Per a una visió més tècnica del tallafoc consulteu l'RFC 2979: www.ietf.org/rfc/rfc2979.txt

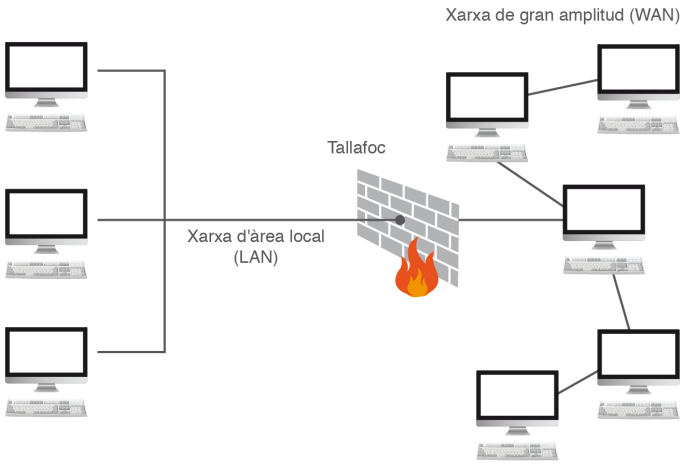
El tallafoc compleix una sèrie de funcions necessàries, però el seu ús implica dominar certs aspectes sinó es vol crear problemes a la xarxa.

El tallafoc es va concebre amb la intenció de donar protecció a la xarxa. Partint d'aquesta base, tot administrador de xarxa es pot formular la pregunta: necessito instal·lar un tallafoc a la meva xarxa? Des de tots els punts de vista la resposta és clara: sí.

Tallafoc és la traducció literal del terme anglès *firewall*, que s'usa en aquest context per primera vegada el 1988.

L'esquema més habitual que s'utilitza per representar un tallafoc és el mostrat en la figura 1.1. Com es pot observar, s'acostuma a utilitzar un mur de maons vermells com a símbol de l'equip tallafoc.

FIGURA 1.1. Representació d'una xarxa amb un tallafoc



1.1 Definicions importants

Abans de començar a tractar els aspectes més rellevants dels tallafocs és important parlar d'una sèrie de termes imprescindibles per entendre'ls. No és possible comprendre la rellevància d'aquests dispositius sense ser conscients de les diferents amenaces de les xarxes, els tipus d'atacants i els atacs més comuns.

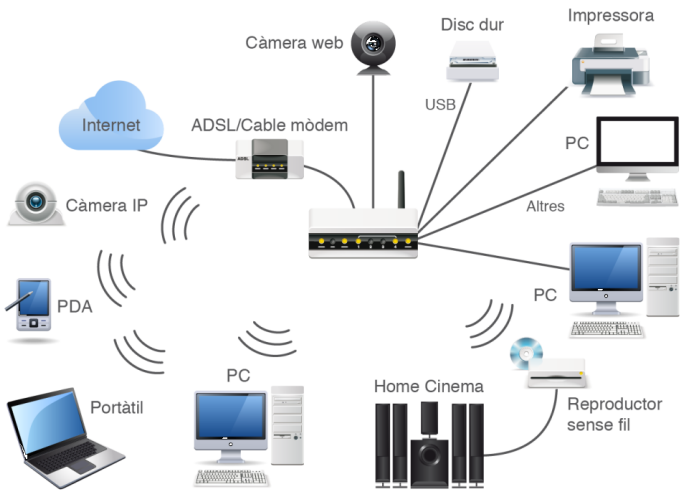
Una vegada presentades algunes de les situacions comprometedores de la seguretat de la xarxa es veurà encara més clara la necessitat d'utilitzar tallafocs.

1.1.1 Amenaces

Per fer front a una amenaça cal estudiar prèviament l'origen de l'amenaça, les eines que utilitza, l'entorn on es desenvolupa i els mecanismes de defensa de què disposem. L'establiment d'una estratègia defensiva és fonamental per garantir la seguretat de la xarxa que volem protegir.

La gestió de la seguretat es pot enfocar com un joc on hi ha una sèrie de regles inamovibles i d'altres que apareixen amb l'evolució tecnològica. Així, fa un cert temps cap tècnic de xarxa s'havia de preocupar per accessos no permesos a la xarxa utilitzant dispositius mòbils i resulta que avui en dia es pot accedir a una xarxa des de punts no estàtics. De fet, la majoria de dispositius que pertanyen a la xarxa són mòbils. Si analitzem el trànsit de xarxa en un àmbit docent descobrim que més de la meitat d'equips connectats són telèfons mòbils, tauletes i portàtils que hi accedeixen amb comunicacions sense fil. Internet està en constant evolució i les persones encarregades de gestionar la seguretat de les xarxes no poden estancar-se i adoptar una actitud passiva davant d'aquests canvis. En la figura 1.2 es pot veure com accedeixen a la xarxa dispositius que utilitzen multitud de tecnologies.

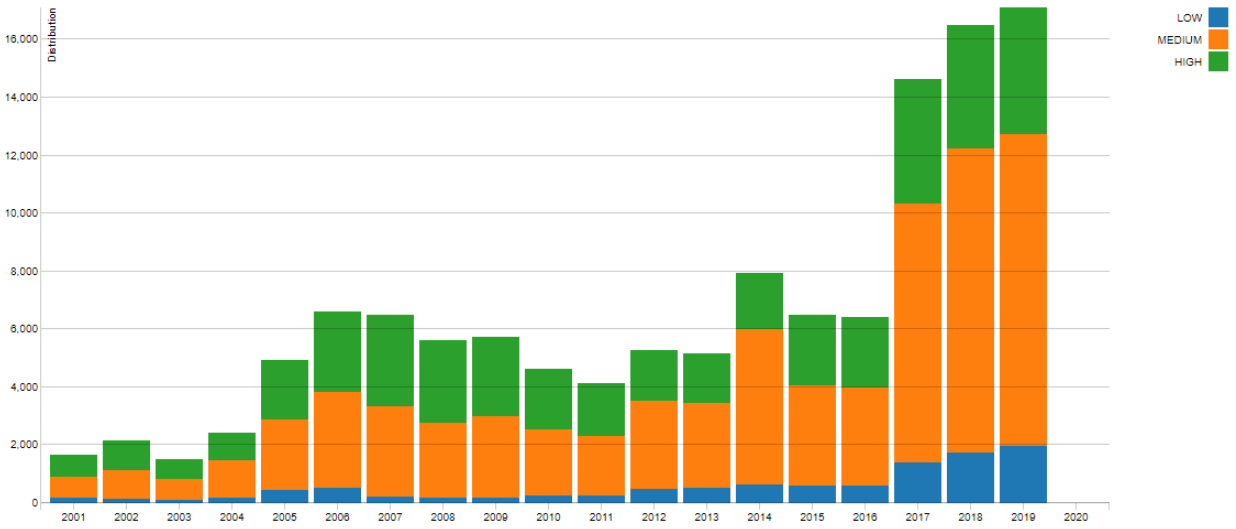
FIGURA 1.2. A les xarxes actuals hi accedeixen tota mena de tecnologies



La National Vulnerability Database (NVD) és el repositori de dades de gestió de vulnerabilitat del govern dels Estats Units d'Amèrica. Es va crear l'any 2000 per l'Institut Nacional d'Estàndards i Tecnologia, que s'abreuja NIST (National Institute of Standards and Technology) i també és del govern dels Estats Units.

A la figura figura 1.3 es pot observar el nombre de les vulnerabilitats anuals trobades entre els anys 2000 i 2019. Les dades dibuixen tres períodes: 2000 a 2004, 2005 a 2016 i 2017 a 2019. Cadascun d'aquests períodes té un nombre d'incidències anual significativament superior al període anterior.

FIGURA 1.3. Nombre de vulnerabilitats trobades cada any.



Font: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

L'increment de la població amb accés a la tecnologia i a Internet, el desenvolupament de nous camps tecnològics vinculats a les xarxes informàtiques i l'augment del coneixement d'aquestes tecnologies per un ampli ventall de perfils són algunes de les causes més probables del creixement del nombre d'incidents registrats. Aquests incidents no només són provocats per persones aïllades, sinó

que últimament proliferen organitzacions que actuen de forma coordinada, com és el cas d'Anonymous.

Anonymous és el pseudònim utilitzat per diverses persones i grups que reivindiquen la llibertat d'expressió i la independència d'Internet. Alguns consideren que no tots els seus actes estan dins de la llei.

Igual que en qualsevol indústria hi ha un recurs molt útil en el disseny d'estratègies de protecció: categoritzar els atacants i els atacs.

1.1.2 Tipus d'atacants

La seguretat d'una xarxa es pot veure compromesa per l'actuació d'un atacant novell o expert. Que la xarxa sigui xarxa víctima potencial d'un atac dependrà de la rellevància de les dades que hi circulen i de les relacions socials de les persones que hi interactuen.

Llocs web de grans corporacions o d'esdeveniments polítics, econòmics i socials són un blanc força comú d'atacs.

Bàsicament existeixen dues categories d'atacants: els *black hats* i els *script kiddies*. Els ***black hats*** són experts que posseeixen moltes i variades habilitats i coneixements, i s'han de considerar una amenaça molt seriosa. Si l'administració d'una xarxa té la sospita de que un *black hat* els està estudiant cal adoptar mesures urgents. Els ***script kiddies*** són molt més nombrosos que els *black hats* i se'ls atribueixen la majoria d'atacs, però són una amenaça molt menor, ja que són considerats programadors inexperts que només aprofiten codi creat per altres.

Motivacions de l'atac

Les motivacions dels atacants són força variades. Poden anar des de la recerca d'un benefici econòmic fins a l'afany d'accedir a un recurs per fer-ne ús personal.

Els principals riscos d'un xarxa són la pèrdua de la **integritat** de les dades, la pèrdua de la **confidencialitat** i la pèrdua de la **disponibilitat** dels recursos.

La pèrdua de la **integritat** de les dades es produeix quan un atac aconsegueix modificar dades, programes o fins i tot el sistema operatiu. Aquesta pèrdua és especialment greu quan no s'ha detectat l'atac. Això pot provocar que es continuï treballant amb dades que no són les correctes o fins i tot que hagi instal·lat dins la xarxa un programa que permeti accessos no autoritzats. La pèrdua de **confidencialitat** consisteix en sostraure informació privilegiada i fer-ne ús, per exemple revelant els continguts. Si una empresa aconsegueix de manera fraudulenta informació confidencial de la competència, com per exemple els plànols d'un artefacte que està tenint gran èxit de vendes, pot utilitzar aquesta informació per fabricar una rèplica millorada del producte i assolir una posició avantatjosa en el mercat. La pèrdua de **disponibilitat** dels recursos es relaciona normalment amb un atac de denegació de servei.

Els atacs de denegació de servei s'identifiquen amb l'acrònim DoS, sigles de *denial of service*, i normalment es manifesten en atacs per inundació SYN, inundació ICMP, SMURF i inundació UDP.

1.1.3 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:

1. **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, cal buscar sistemes que estiguin generant trànsit amb destinació al port 25 d'altres sistemes d'Internet.

2. **Denegació 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 sol·licitar 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 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, consegüentment, 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.

3. **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, 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.

4. **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` a Linux, ho podríem fer mitjançant les ordres següents:

```
1 # tcpdump –nni enp0s3 –s 0 –w /tmp/captura 'port 80'
```

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
```

Codi corrupte

El warez és un programari amb drets d'autor que es distribueix il·lícitament. El malware és el conjunt de programes maliciosos. S'hi inclouen els virus, els cucs, els cavalls de Troia, les eines d'intrusió (rootkits) i el programari de publicitat (adware), entre d'altres.

L'ordre `strings` extreu les cadenes de text d'un fitxer binari.

Per poder fer els atacs que s'han descrit més amunt, cal 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 font pública ClamAV per analitzar els sistemes.

1.1.4 Els tallafocs més comuns

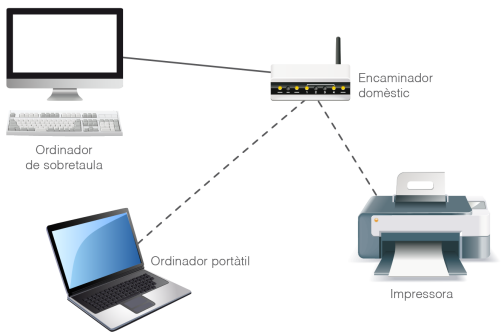
En el moment d'instal·lar un tallafoc és bàsic poder respondre tres preguntes: quines regles de tallafoc necessitem? On col·locarem el tallafoc? Quants tallafocs necessita la xarxa?

Les necessitats de la xarxa indicaran quin és el tipus de tallafoc més idoni per instal·lar. Així podem instal·lar un **tallafoc en encaminador**, un **tallafoc en un sola màquina** o un **tallafoc en més d'una màquina**.

Quan s'aprofita l'encaminament de dades per realitzar un filtratge d'aquestes dades s'està protegint la xarxa. Aquesta manera de treballar no és gaire recomanable, ja que aquest procés es limita a estudiar únicament l'adreça IP del paquet. L'encaminador està fent una tasca que a priori hauria de fer un tallafoc. Però en xarxes de mida reduïda és una estratègia força comuna. Tot i ser una tècnica molt simple de dissenyar i d'implementar, presenta una sèrie de problemes greus: la defensa té una carència de profunditat evident, no existeix la flexibilitat i tant les màquines públiques com les privades conviuen en la mateixa xarxa.

La xarxa de la figura 1.4 només té un encaminador. En una xarxa d'aquestes dimensions és molt probable que haver d'instal·lar i gestionar un tallafoc no sigui del tot adient.

FIGURA 1.4. Xarxa de dimensions reduïdes amb un encaminador



1.2 Característiques i tipus de tallafocs

El tallafoc és un dispositiu que presenta algunes característiques genèriques i d'altres de particulars, que permeten classificar-lo en diferents tipus. Hi ha una sèrie de característiques que s'han de conèixer per comprendre què significa utilitzar un tallafoc a la xarxa. Existeixen diferents tipus de tallafocs que es poden trobar en el mercat. Serà tasca de l'administrador escollir quin és el tallafoc més adient per a la xarxa.

1.2.1 Característiques del tallafoc

En general, els tallafocs presenten una sèrie de característiques comunes. Aquestes característiques són la implementació, el nivell de la gestió de seguretat que ofereix de la xarxa i el pressupost.

La **implementació** del tallafoc és possiblement la característica més important. La xarxa ha de seguir una política de seguretat que marcarà el nivell de protecció a aplicar. Una empresa que treballa amb dades sensibles haurà d'aplicar una política de seguretat rigorosa, mentre que en un entorn domèstic s'aplicarà un nivell de seguretat menor.

Tallafoc domèstic

Amb l'arribada d'Internet a les llars, l'ús del tallafoc ha esdevingut imprescindible per protegir els nostres equips, però la sofisticació d'un tallafoc domèstic no té res a veure amb la d'un tallafoc empresarial.

En determinades xarxes són necessaris tallafocs que permetin la gestió de la seguretat de la xarxa des del punt de vista del monitoratge, el control de la redundància i el nivell de control a aplicar. El **monitoratge** és una gran ajuda per detectar problemes, intrusions o un mal ús de la xarxa. La **redundància** a diferents nivells permet l'assegurament de la informació. És important, per tant, que el tallafoc permeti la redundància necessària i detecti i elimini, en canvi, la que resulti contraproduent. El **nivell de control** a aplicar a la xarxa necessita de reflexió: s'ha de decidir què es permetrà i que es negarà.

> Hi ha dos tipus de nivell de control: el restrictiu i el permissiu. El control **restrictiu** denega tot el que no es permet explícitament, mentre que el control **permissiu** permet tot allò que no es prohibeix de manera manifesta.

Disposar de segons quin tallafoc pot implicar una despesa no sempre assumible. Un tallafoc pot tenir un cost econòmic nul o de molts milers d'euros (no és difícil trobar-ne per sobre dels 30.000 €). Escollirem un tallafoc o un altre en funció de les necessitats de la xarxa i del nostre pressupost.

Un cop clares les característiques dels tallafocs cal escollir el model més adequat a les nostres necessitats. Formular-nos les preguntes següents ens ajudarà a triar la millor opció:

1. Per la nostra xarxa circulen dades sensibles? Si la resposta és afirmativa haurem d'instal·lar un tallafoc. Avui en dia, la resposta sempre és afirmativa perquè per la nostra xarxa **sempre** hi circularan dades sensibles.

2. Quin grau de complexitat té la nostra xarxa? No hem de confondre una xarxa complexa amb una xarxa gran. Una empresa amb set treballadors i deu ordinadors pot disposar d'una xarxa més complexa que una que té 1.000 treballadors. Com més complexa sigui la xarxa, més eines ha d'oferir el tallafoc per gestionar-la de manera senzilla i eficaç.

3. Quin pressupost podem dedicar al tallafoc? Quan es fa la provisió per als components de la xarxa s'ha de reservar una part del pressupost per al tallafoc. La quantitat dependrà de les respostes a les preguntes anteriors.

La necessitat marca les característiques del tallafocs

Una multinacional amb gran volum de negoci pot necessitar un tallafoc de prestacions elevades i segurament pot invertir-hi una gran quantitat de diners. En canvi, a casa podem utilitzar un ordinador antic que ja no utilitzem amb sistema operatiu Ubuntu i un tallafoc gratuït.

Com es pot veure, el tallafoc és un dispositiu amb unes característiques clarament definides. Quan coneixem la funció del tallafoc ens adonem del seu paper protagonista dins de la xarxa.

1.2.2 Tipus de tallafocs

Els diferents tallafocs que es poden trobar en el mercat es poden agrupar segons el preu, la seva implementació o segons la complexitat que presenta la xarxa.

En una mateixa xarxa poden conviure diferents tipus de tallafocs, ja que aquests desenvolupen tasques bastant específiques segons sigui el cas.

Tipus de tallafocs segons el preu

Actualment es poden trobar tallafocs gratuïts, tallafocs gratuïts als quals se'ls poden afegir mòduls de pagament, tallafocs gratuïts durant un període de temps i tallafocs de pagament.

Poder disposar de tallafocs gratuïts és molt convenient per a aquelles corporacions que no poden invertir gaire en la xarxa, però que necessiten que aquesta ofereixi unes mínimes garanties.

Logotip del programa Shorewall molt utilitzat en xarxes mitjanes i grans.

Les empreses que fabriquen màquines tallafoc generalment també desenvolupen programari tallafoc. La gama de preu és molt àmplia, i la variable que utilitzen aquestes empreses és el nivell de seguretat que garanteixen.

Un tallafoc gratuït no ofereix el suport tècnic que en principi pot oferir un de pagament, però per contra un bon tallafoc per a empreses pot ser molt car.

Tipus de tallafocs segons la implementació

En el mercat existeixen tallafocs de maquinari i de programari. Així, podem descarregar un tallafoc gratuït d'Internet, o bé comprar un paquet de programari o comprar una màquina que faci aquesta funció.

Les marques més reconegudes de màquines tallafoc són SonicWALL, Barracuda, Check Point, Cisco, RSA, Juniter i Watchguard. Els preus mitjans d'equips professionals estan al voltant dels 6.000 €, però aquestes marques tenen models que poden sobrepassar els 50.000 €. En la figura 1.5 es mostra un model de tallafoc de l'empresa SonicWALL, especialitzada en el sector de la seguretat.

Logotip de Check Point que comercialitza tant màquines com programes tallafocs.

FIGURA 1.5. Model de tallafoc de la marca SonicWALL

Les màquines tallafoc poden tenir objectius de defensa genèrics o poden estar dedicades a un servei determinat. En aquest segon cas, per exemple, cal citar tallafocs dissenyats específicament per a serveis de correu que tenen com a objectiu controlar el correu brossa.

Correu brossa

El correu brossa o spam són missatges de correu que arriben a un client que no els ha sol·licitat. L'spamming genera importants pèrdues econòmiques a les empreses que el pateixen.

Tipus de tallafocs segons la complexitat

La confidencialitat és una característica tant important de les xarxes que en moltes ocasions les defineix. L'administrador de la xarxa prendrà les decisions que tinguin a veure amb la seguretat en funció de la complexitat de la xarxa i de la importància de les dades que s'han de protegir.

Tenint en compte aquesta complexitat es poden identificar tres grans grups de tallafocs:

1. Els tallafocs personals
2. Els tallafocs de departament
3. Els tallafocs d'empresa

El **tallafoc personal** s'instal·la generalment en àmbits domèstics o negocis molt petits. Aquest tallafoc normalment ha de protegir un únic ordinador o una petita xarxa, fins i tot és probable que s'instal·li en el mateix equip de treball. Alguns sistemes operatius inclouen un tallafoc instal·lat pensat per a ús domèstic. Algunes empreses comercialitzadores d'equips informàtics, d'equips de xarxa o de sistemes operatius inclouen tallafocs preinstal·lats en els seus productes.

Els sistemes operatius de Microsoft incorporen un programa amb les funcionalitats pròpies d'un tallafoc personal.

El **tallafoc de departament** ofereix una sèrie de serveis a una xarxa informàtica. El volum de dades que ha de gestionar aquest tipus de tallafoc comença a ser important i el manteniment i configuració del tallafoc requereix coneixements tècnics.

El **tallafoc empresarial** pot ser un equip molt potent o bé el conjunt format per diversos tallafocs de departament. L'ús i manteniment d'aquest tipus de tallafoc exigeix molta dedicació. Generalment l'administració de la xarxa acaba per automatitzar processos per gestionar aquests tallafocs, ja que habitualment el volum de dades que hi circulen és massa gran per fer-ho sense suport automàtic. Actualment existeixen en el mercat empreses que centren el seu negoci en la fabricació d'aquests equips. Generalment són equips que han de ser operats per treballadors amb una formació específica i un alt grau de coneixements de xarxa.

La taula 1.1 resumeix les característiques més remarcables dels diferents tipus de tallafocs.

TAULA 1.1. Resum de característiques dels diferents tipus de tallafocs

	Tallafoc personal	**Tallafoc de departament**	**Tallafoc empresarial**
Nombre de màquines	1 o cap	1	1 o més
Complexitat	Baixa	Alta	Molt alta
Requeriments tècnics	No	Recomanable	Imprescindible
Actualització	Constant	Constant	Constant

Quin tallafoc escollir

Arriba un moment en què tot administrador d'una xarxa ha de prendre una decisió crucial: quin tallafoc instal·lo? Haurà de tenir en compte les qüestions següents:

1. La política de seguretat que se segueixi
2. El nivell de control
3. El pressupost

La **política de seguretat** a aplicar depèn bàsicament de les dades sensibles que circulin per la xarxa. Si, per exemple, hi circulen dades personals, caldrà aixecar totes les barreres necessàries per no posar en perill la integritat i confidencialitat d'aquestes dades. En aquest cas, doncs, s'haurà d'establir una política de seguretat rígida. Val a dir que un tallafoc no és l'únic element en una política de seguretat: un altre aspecte molt important és l'accés dels usuaris a la xarxa amb dispositius extraïbles, la visibilitat de dades des de dispositius d'oficina o l'accés al recinte de persones alienes a l'empresa.

Pel que fa al nivell de control d'una xarxa es pot adoptar una postura restrictiva o una postura permissiva. El tipus de tallafoc a implementar dependrà de si s'adopta una postura restrictiva o una postura permissiva pel que fa al nivell de control.

FIGURA 1.6. Tallafoc de gama alta de Cisco

El **pressupost** és una dada que sempre marca l'elecció dels equips que conformen la xarxa. En el mercat es poden trobar tallafocs de preus molt diversos i en ocasions resulta difícil triar la millor opció. En la figura 1.6 hi ha un exemple de tallafoc amb moltes prestacions i que implica disposar d'un alt pressupost. Depenent del requeriment de la xarxa, un equip d'aquest perfil hi tindria cabuda.

Escollir el tallafoc adient és una tasca complexa que requerirà un temps de reflexió.

Exemple de decisió

A l'hora d'escollir un tallafoc és convenient que ens fem aquestes preguntes: De quin pressupost disposo? Circulen dades especialment sensibles per la xarxa? El tallafoc que s'utilitzarà serà un programa o una màquina? El tallafoc escollit cobreix totes les necessitats de la xarxa o s'ha de complementar amb un altre tallafoc?

Suposem que una empresa de nova creació que es dedica a la fabricació artesanal de cotxes us demana assessorament. Disposen d'una petita xarxa informàtica que consta de cinc ordinadors personals que s'utilitzen en tasques de producció i administració. Un d'aquests ordinadors fa tasques de servidor (dóna accés a Internet, emmagatzema les dades personals dels clients i realitza còpies de seguretat). Acaben d'incorporar en plantilla a una persona que ha finalitzat el grau mitjà d'informàtica. La pregunta que us fan és: com protegim les dades de l'empresa?

Solució

1. De quin pressupost disposo? Resposta: com a màxim es poden invertir 500 € en la protecció de la xarxa.
2. Circulen dades especialment sensibles per la xarxa? Resposta: Sí. A més, durant una visita a l'empresa es detecta un punt d'accés sense cables.
3. El tallafoc que s'utilitzarà serà un programa o una màquina? Resposta: La màquina que fa de servidor està força atapeïda. Es fa un estudi de rendiment i es valora afegir un equip que realitzi tasques de tallafoc.
4. El tallafoc escollit cobreix totes les necessitats de la xarxa o s'ha de complementar amb un altre? Resposta: Encara no s'ha escollit el tallafoc, però ja se sap que serà una màquina que no excedeixi dels 500 €, que haurà de filtrar el trànsit d'entrada i sortida de la xarxa i que possiblement tregui serveis al servidor actual. Amb un tallafoc n'hi haurà prou.

1.3 Funcions principals del tallafoc

La funció principal d'un tallafoc és la **defensa de la xarxa**. Un tallafoc ha de preveure un atac i parar els accessos no autoritzats a la xarxa. Eliminar virus no és feina del tallafoc, però sí que ho és proporcionar seguretat i protecció davant de l'entrada de virus.

El concepte *entitat* fa referència a una empresa, a una societat, una corporació o qualsevol persona o grup de persones que disposin d'una xarxa informàtica.

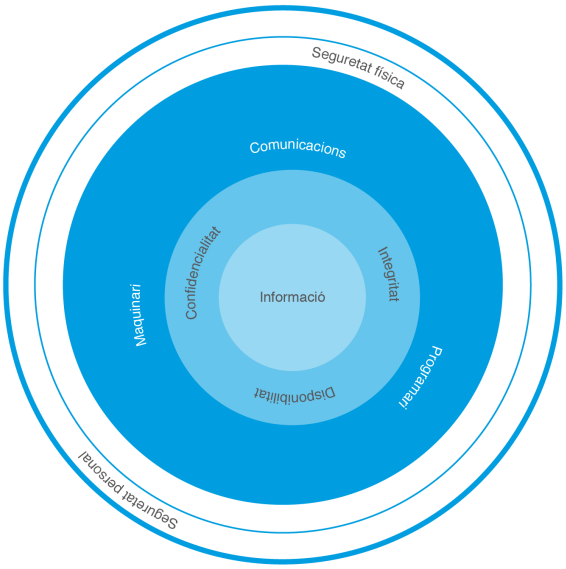
Des del punt de vista de l'entitat que utilitza la xarxa, el tallafoc és l'instrument que assegura la **confidencialitat**, la **integritat** i la **disponibilitat** de les dades que estan viatjant per la xarxa o bé que estan emmagatzemades en els dispositius que pertanyen a la xarxa.

La **confidencialitat** d'una part o de la totalitat de la informació que circula o s'emmagatzema en un xarxa ha d'estar protegida. La **integritat** de les dades indica si podem tenir la certesa de que la informació no ha estat modificada sense permís. La **disponibilitat** de les dades significa que s'hi pot accedir.

Habitualment, la relació existent entre aquests tres conceptes es representa en forma de triangle. A la figura 1.7 es veuen factors bàsics en la gestió de la informació i els seus atributs de seguretat:

1. La seguretat personal és el factor més extern i estarà marcat per l'educació de l'usuari en la matèria.
2. La seguretat física marcarà l'accés a dispositius
3. Programari, maquinari i comunicacions estan al mateix nivell i permeten accedir a la disponibilitat, confidencialitat i integritat de la informació.

Figura 1.7. Triangle dels conceptes confidencialitat, integritat i disponibilitat



Confidencialitat, **integritat** i **disponibilitat** són els tres atributs de la seguretat de la informació.

Un tallafoc s'encarrega de contenir els atacs a la xarxa i d'identificar l'atacant. Per aconseguir-ho pot filtrar el trànsit estudiant les adreces IP o el servei que s'està utilitzant.

L'RGPD, del 27 d'abril de 2016, garanteix la protecció de les dades personals.

Tot i que l'ús de tallafoc presenta més avantatges que inconvenients, cal comentar aquests últims per tal de assolir una comprensió més completa del seu funcionament. L'ús del tallafoc pot provocar problemes de fiabilitat, de rendiment o de flexibilitat.

Una de les normes que se segueix en el disseny de xarxes segures és, primer de tot, comprovar la correcta connectivitat general i a continuació aplicar les polítiques de seguretat. La pràctica ens demostra que la fiabilitat de la xarxa pot disminuir a causa del tallafoc. Fer passar tot el trànsit de xarxa per un mateix punt té un gran risc, ja que aquest punt concentra el risc d'incidents. Si per error el trànsit no pot traspassar el tallafoc, la xarxa deixa d'estar disponible, i això contradiu el mateix sentit de la xarxa.

Una situació per desgràcia bastant recurrent és la que s'esdevé en xarxes ben dissenyades i implementades, però que presenten un baix rendiment quan arriben a la frontera del tallafoc. Per què passa, això? Per què el rendiment de la xarxa és tan baix? Es pot donar el cas que el tallafoc provoqui un coll d'ampolla, a causa en molts casos d'una línia lenta (no és inusual que s'utilitzi el mateix ample de banda de la xarxa per conduir tot el trànsit al tallafoc) perquè el tallafoc té instal·lades unes interfícies de baixa velocitat o bé perquè el mateix tallafoc està per sota del perfil de rendiment de la xarxa.

Per naturalesa, una xarxa ha de presentar una certa flexibilitat. És curiós que puguem estudiar la progressió i l'estratègia d'una empresa limitant-nos a observar la configuració i utilització que fa de la tecnologia. La xarxa informàtica és una eina al servei de l'empresa i, com aquesta, pot canviar al llarg del temps. Els tallafocs poden ser un handicap en aquesta evolució. Les capacitats d'una xarxa poden veure's limitades per la presència del tallafoc.

Com podem solucionar els problemes de fiabilitat, rendiment i flexibilitat? Una manera de sortejar els inconvenients dels tallafocs és usar diversos tallafocs en diferents zones de la xarxa i no deixar així la xarxa depenent d'un únic tallafoc.

Combinació de mesures

Es pot avaluar la fortalesa de la xarxa estudiant la implicació i varietat de mesures defensives aplicades. Podem fer treballar els tallafocs en combinació amb altres mesures de seguretat.

És força comú trobar programes que disposen d'estructures de seguretat pròpies a priori suficients. Aquests programes treballen independentment del tallafoc, sense relacionar-s'hi, però en conjunt formen un bloc operatiu.

1.4 Configuració i utilització del tallafoc

Configurar i utilitzar el tallafoc no són tasques senzilles, almenys en un inici. És important treballar correctament per no convertir un projecte engrescador en un malson. Perquè, efectivament, realitzar aquesta tasca de manera incorrecta pot generar uns problemes tant greus que la xarxa quedi anul·lada o que, si més no, perdi flexibilitat i capacitat de servei.

Per treballar de manera coherent i avançar amb pas segur cal entendre el model de desenvolupament d'un tallafoc i assajar els passos descrits per tal d'aprofitar al màxim el temps dedicat.

1.4.1 Model de desenvolupament d'un tallafoc

L'establiment i configuració d'un tallafoc ha de seguir una sèrie de passos. És important respectar l'ordre d'aquestes fases si es pretén desenvolupar una eina pràctica i eficaç. Els passos són:

1. Especificació dels requisits
2. Justificació
3. Disseny arquitectònic
4. Disseny de directives
5. Implementació
6. Prova
7. Administració i manteniment

Prenent aquests punts com a guia es tindran més probabilitats d'èxit en la implementació d'un tallafoc.

Especificació dels requisits

Cal documentar la funció del tallafoc. Aquesta afirmació no és trivial, ja que dedicar un cert temps a pensar quines són les amenaces i riscos específics que es volen evitar amb el tallafoc és molt important.

Una xarxa concreta es veurà amenaçada per determinades entitats i en una major o menor quantia. L'elecció del tallafoc s'ha de fer en una escala lògica dins el sistema al qual pertany.

Algunes de les tasques que li podem demanar al tallafoc són:

1. Bloquejar l'entrada i sortida de trànsit d'un segment de xarxa.
2. Bloquejar l'entrada i sortida de trànsit amb adreces IP privades.
3. Bloquejar l'accés a un determinat amfitrió.
4. Bloquejar l'accés a determinat trànsit que vagi a un determinat amfitrió.

Un tallafoc no pot anul·lar una xarxa, ha de permetre que aquesta doni servei als seus usuaris.

Haureu de redactar en un document els requisits específics de la vostra xarxa.

Exemple de requisits

Un exemple de redactat dels requisits d'un tallafoc podria ser la següent:

La nostra xarxa ha de garantir determinats serveis als usuaris interns de la xarxa i als usuaris externs de la xarxa. Els usuaris interns podran accedir sempre a Internet, al servidor que allotja els cursos virtuals i al servidor de fotografies. Els usuaris externs només podran accedir al servidor que allotja els cursos virtuals.

Justificació

Cal justificar la implementació d'un tallafoc? Aquesta comporta una despesa de temps d'estudi, instal·lació, configuració i manteniment, i també pot suposar una despesa econòmica en cas que el tallafoc no sigui gratuït. Per acabar, també suposa una despesa organitzativa. Per tant, cal justificar la necessitat que tenim del tallafoc.

Això implica analitzar la seguretat de la xarxa, fer una valoració de les amenaces i els riscos i fer una proposta en funció de la informació obtinguda. És una tasca molt important, ja que és al tècnic a qui es demanaran responsabilitats si es produeix un atac que compromet la seguretat de la xarxa.

La seguretat d'una xarxa és un assumpte que implica molta agilitat i requereix quantiosos esforços tècnics i humans. La varietat d'atacs i la seva continuïtat forcen els administradors de la xarxa a buscar i aplicar contínuament mesures defensives. Una baixada en la intensitat i efectivitat d'aquestes mesures pot resultar fatal per a la xarxa.

La justificació de l'ús d'un tallafoc es realitzarà per escrit i es lliurarà a la direcció de l'organització.

Documentació de les necessitats

Suposem que, després de realitzar una anàlisi de les dades que circulen i s'emmagatzemen en una xarxa informàtica i el perfil d'usuari que hi accedeix, veiem la necessitat d'instal·lar-hi un tallafoc. El nivell de seguretat actual que s'aplica és insuficient i hem comprovat que la xarxa no disposa dels recursos necessaris per detectar una intrusió i que tampoc no la podria evitar o contrarestar, ni assegurar la informació. S'afegiria a l'escrit de justificació de la necessitat d'un tallafoc un informe tècnic amb aquestes dades.

Disseny arquitectònic

L'arquitectura que segueixen la majoria de tallafocs depèn de les característiques de cada xarxa en particular i del seu entorn.

El **disseny arquitectònic** consisteix a decidir quina és l'arquitectura de tallafoc més adient perquè sigui òptim.

Seguir aquests passos pot ser de molta ajuda per desenvolupar el disseny arquitectònic:

1. Estudiar les arquitectures de tallafoc candidates.
2. Fer la simulació de com funcionaria cada una d'elles en la nostra xarxa.
3. Ordenar les arquitectures de millor a pitjor segons les nostres necessitats.
4. Implementar la tecnologia candidata realitzant les modificacions necessàries per emmotllar-la de la forma més eficient a la xarxa.

El disseny arquitectònic implica en moltes ocasions una revisió del pla i una nova justificació, ja que es pot donar el cas que una vegada implementada una tecnologia sorgeixin vulnerabilitats que no es poden corregir amb l'opció escollida inicialment.

Disseny de directives

A més del correcte estudi de necessitats, cal fer un bon disseny de directives. Hem de dedicar temps i esforços a aquesta fase, ja que és la base del futur funcionament del sistema de defensa.

El **disseny de directives** és el responsable de l'especificació detallada de com ha d'actuar un tallafoc davant de paquets que tenen determinades característiques.

El disseny de directives implica pensar les regles que gestionaran el funcionament del tallafoc. Consisteix bàsicament a:

1. Identificar les màquines que tindran permís per accedir a determinats serveis.
2. Identificar les característiques del trànsit de dades.
3. Documentar el procés especificant el tractament de la informació per part del tallafoc.

La tasca de documentació és important. I és especialment important documentar el disseny de directives, encara que el tallafoc s'apliqui sobre una xarxa petita. Elaborar aquesta documentació facilitarà la detecció de problemes i incompatibilitats de la nostra gestió.

Un exemple de regles seria:

```
1 -A FORWARD -o enp0s3 -i enp0s4 -d 192.168.0.8 -p tcp --dport 80 -j ACCEPT
2 -A FORWARD -o enp0s3 -i enp0s5 -d 192.168.0.8 -p tcp --dport 80 -j ACCEPT
3 -A FORWARD -o enp0s3 -i enp0s6 -d 192.168.0.8 -p tcp --dport 80 -j ACCEPT
4 -A FORWARD -o enp0s3 -i enp0s4 -d 192.168.0.8 -p tcp --dport 22 -j DROP
5 -A FORWARD -o enp0s3 -i enp0s4 -d 200.168.0.5 -p tcp --dport 80 -j DROP
6 -A FORWARD -o enp0s3 -i enp0s7 -d 192.168.0.8 -p udp --dport 80 -j DROP
7 -A FORWARD -o enp0s3 -i enp0s8 -d 192.168.0.8 -p tcp --dport 80 -j ACCEPT
8 -A FORWARD -o enp0s3 -i enp0s8 -d 200.100.0.6 -p udp --dport 80 -j DROP
```

Les línies de codi defineixen unes regles determinades. Abans d'inserir-les en el tallafoc ha calgut realitzar un treball previ de disseny. Aplicar regles de forma errònia pot causar greus problemes de funcionament a la xarxa.

Hi ha dos corrents bàsics en el disseny de directives: tallafocs amb perfils restrictius i tallafocs amb perfils permissius. Els tallafocs restrictius bloquegen els paquets que no coincideixen amb les regles. Els tallafocs permissius accepten els paquets que no coincideixen amb les regles. Quin perfil és millor? La resposta no és senzilla. A priori es podria considerar que una política restrictiva és més segura, però aquesta política pot no proporcionar la flexibilitat necessària per al funcionament normal de la xarxa.

Per començar a dissenyar directives es pot utilitzar una plantilla com la de la taula 1.2

TAULA 1.2. Plantilla exemple

Acció	Interfície	Estat	TCP	Protocol	Origen	PortO	DestinacióPortD	Comentari

- **Acció**: defineix l'acció a realitzar. Generalment els paquets es poden acceptar, rebutjar, eliminar o registrar.
- **Interfície**: indica la interfície a la qual arriba un paquet entrant o la interfície a la qual es dirigeix un paquet sortint. Amb la versió *v197* del gestor de dispositius de Linux *systemd/udev*, s'assignaran de forma automàtica i predictible noms estables per a les interfícies de xarxes locals Ethernet (en), WLAN(wl) i WWAN(ww). Això és un canvi respecte a la forma tradicional d'anomenar les interfícies de xarxa (*eth0*, *eth1*, *wlan0*, ...) que s'ha realitzat per solucionar problemes de configuració, mantenint ara les interfícies el mateix nom, tot i reiniciar l'ordinador. Aquesta nova nomenclatura s'utilitza ja a partir d'Ubuntu 16 i Debian 9. Per exemple, l'antiga interfície *eth0* ara s'anomenarà *enp0s3*, on **en** indica el tipus de xarxa, en aquest cas Ethernet (en) - les altres que opcions poden ser: WLAN(wl) i WWAN(ww). La **p** indica el tipus de bus (en aquest cas, PCI): el p0 és el primer bus i la **s** indica en quin slot està. En aquest nou sistema hi ha 5 esquemes en funció de la informació proporcionada pel maquinari per escollir la manera d'anomenar les interfícies de xarxa; el cinquè i darrer d'aquests esquemes les anomena segons l'antiga nomenclatura.

Podeu ampliar la informació de la versió *v197* del gestor de dispositius de Linux *systemd/udev* a la secció "Annexos", a l'enllaç "Nomenclatura consistent pels dispositius de xarxa" del web del mòdul".

- **Estat**: per a tallafocs que disposen d'estat (l'antic tallafoc IPChains, per exemple, no en disposava), s'indica l'estat de la connexió. Genèricament aquest valor serà *nova*, *establerta* o *relacionada*.
- **TCP**: identifica indicadors de TCP (*Transmission Control Protocol*). Poden ser-ho SYN o ACK.
- **Protocol**: indica el protocol a tractar. Aquests poden ser TCP, UDP, ICMP o *tots*.

- **Origen**: indica l'adreça IP origen del paquet. L'adreça 0.0.0.0 indica que s'accepta qualsevol adreça IP.
- **PortO**: indica el port d'origen per als protocols TCP i UDP, però també el tipus de datagrama ICMP en el cas que es tracti d'un paquet ICMP.
- **Destinació**: indica l'adreça IP de destinació del paquet. L'adreça 0.0.0.0 indica que s'accepta qualsevol adreça IP.
- **PortD**: indica el port de destinació per als protocols TCP i UDP, però també el tipus de datagrama ICMP en el cas que es tracti d'un paquet ICMP.
- **Comentari**: en aquesta columna es poden afegir comentaris per donar justificació o explicació a l'acció.

  La plantilla proposada és força genèrica i pot servir com a punt de partida, però finalment cada responsable de seguretat crearà la seva pròpia plantilla per tal d'ajustar-la a les seves necessitats.

La taula 1.3 reflecteix la especificació de requisits següent: els usuaris interns podran accedir sempre a Internet, al servidor que allotja els cursos virtuals i al servidor de fotografies. Els usuaris externs només podran accedir al servidor que allotja els cursos virtuals.

TAULA 1.3. Quadre resum de directive

Acció	Interfície	Estat	TCP	Protocol	Origen	PortO	Destinació	PortD	Comentari
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	Sortida Internet	Tots	Permetre l'accés a Internet
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	IP del servidor de cursos virtuals	Tots	Permetre l'accés al servidor de cursos virtuals
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	IP del servidor de fotografies	Tots	Permetre l'accés al servidor de fotografies
Acceptar	1	Establerta	El que calgui	El que calgui	La xarxa externa	Tots	IP del servidor de cursos virtuals	El que calgui	Permetre l'accés al servidor de cursos virtuals
Denegar	0	Tot	Tot	Tot	Tot	Tot	Tot	Tot	Denegar tot el que no s'hagi permès abans
Denegar	1	Tot	Tot	Tot	Tot	Tot	Tot	Tot	Denegar tot el que no s'hagi permès abans

Quan es dissenyen directives cal tenir molt clar l'ordre en el qual s'escriuen, ja que si, per exemple, primer ho deneguem tot ja no podrem permetre res: haurem eliminat tot el trànsit.

En aquest punt caldrà realitzar una revisió del disseny abans d'entrar a la fase d'implementació. És molt important no cometre errors durant la fase de disseny. Tot error no detectat a temps pot afectar a la feina realitzada.

Implementació

La implementació del tallafoc consisteix a aplicar les directives dissenyades al tallafoc escollit. En aquest procés es duu a la pràctica la teoria desenvolupada en el disseny segons les possibilitats físiques reals del tallafoc.

L'esforç de la implementació se centra en configurar el tallafoc de tal manera que compleixi les directives dissenyades.

El més important en aquesta fase és decidir quin tipus de tallafoc utilitzar. Decidides les directives caldrà escollir el programa o màquina tallafoc que permeti realitzar les accions dissenyades. En resum, les variables que ens ajudaran a seleccionar el tallafoc poden ser:

- Funcions que el tallafoc ha de realitzar (bàsicament NAT, registre i control)
- Estabilitat del tallafoc
- Rendiment del tallafoc
- Facilitat d'ús del tallafoc
- Documentació disponible
- Cost econòmic i tecnològic

Una porta gran i robusta amb un aspecte bastant agressiu. És el que instal·laríem a casa? No s'ha de confondre valor i preu. S'ha d'escollir el que la xarxa necessiti.

Avaluant aquestes variables es podrà decidir justificadament quin tallafoc implementar.

Prova

En aquesta fase es prova si el disseny de directives ha estat el correcte i si la seva implementació en el tallafoc compleix els objectius.

Durant el procés de prova s'han de realitzar accions permeses i no permeses per comprovar la correcta resposta del tallafoc. A causa d'errors de disseny o d'errors d'implementació, un tallafoc pot treballar de forma incorrecta i permetre accions prohibides i denegar accions permeses.

No realitzar proves genera problemes

Són innumerables les ocasions en què un usuari inexpert instal·la un tallafoc i deixa sense accés a Internet a tots els usuaris d'una xarxa. Ha provat el tallafoc abans? Segurament no. Ha realitzat tots els passos que s'han de seguir en el procés d'implantació d'un tallafoc? Segurament tampoc.

Administració i manteniment

Una vegada dissenyat, implementat i provat un tallafoc, cal realitzar tasques d'administració i manteniment. La xarxa informàtica presenta moviments continus de dades i evolucions constants, i això justifica que el tallafoc s'hagi d'anar estudiant i millorant.

Val la pena dedicar una mica de temps a experimentar amb diverses aplicacions gratuïtes, com Webmin (figura 1.8), que simplifica molt la gestió d'un tallafoc i permet guanyar molt temps en els processos de configuració i seguiment d'esdeveniments de la xarxa.

FIGURA 1.8. Pàgina inicial de Webmin

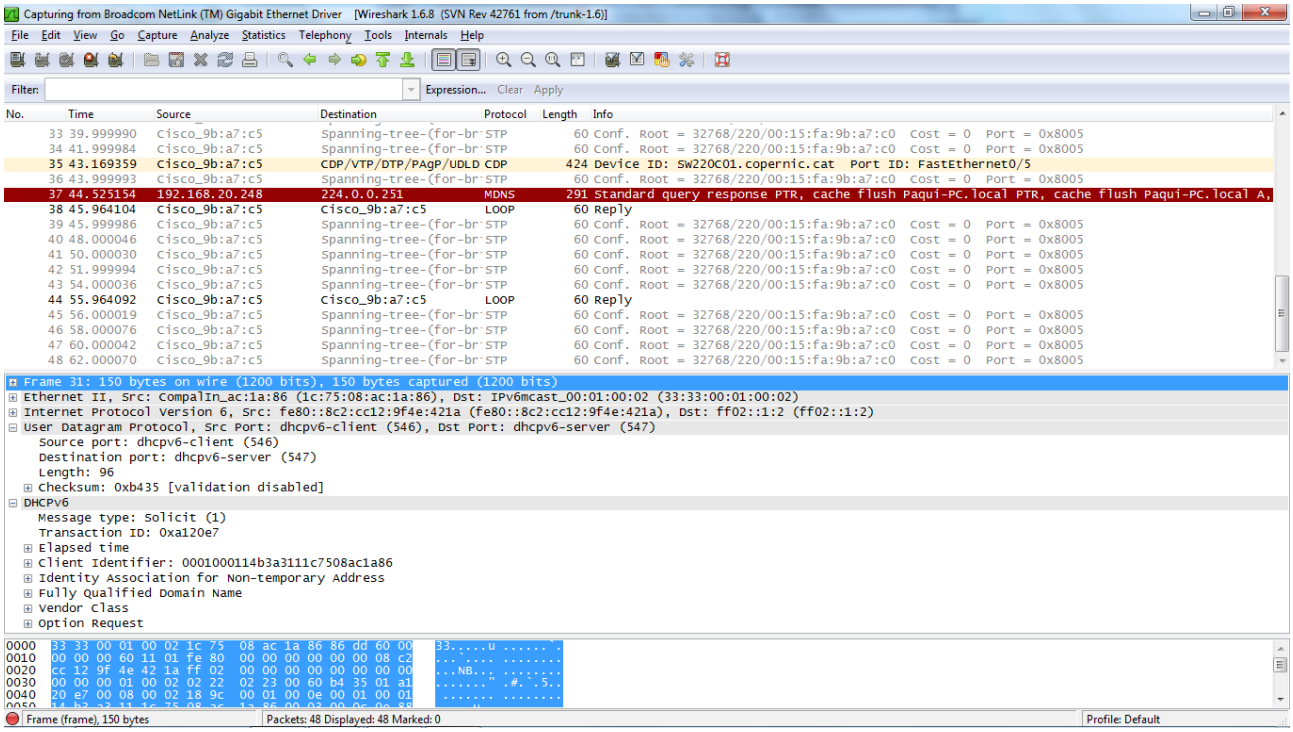
La lectura dels registres generats pel tallafoc ajudarà a comprovar els intents d'accions no permeses, i la continua revisió de les directives i l'actualització de versions, tant de programari com de maquinari, faran menys vulnerable el tallafoc.

1.4.2 Filtratge de paquets de dades

Per fer el filtratge dels paquets de dades cal veure amb una mica de detall com viatgen les dades. Els principals datagrames que es desplacen per la xarxa informàtica són datagrames IP, ICMP, UDP i TCP. No oblidem que els tallafocs filtren paquets, per tant, si volem extreure informació valuosa de les dades que ens acabarà retornant el tallafoc hem de ser capaços d'analitzar amb coneixement de causa aquesta informació.

Per estudiar els paquets que circulen per la xarxa és recomanable usar programes tipus Wireshark. En la figura 1.9 apareix una imatge de la pantalla principal d'aquest programa quan està en funcionament.

FIGURA 1.9. Captura amb Wireshark de tràfic de xarxa



Datagrames IP

Un datagrama IP *(Internet Protocol)* està format per dues parts: la capçalera i el cos. La capçalera està formada per sis paraules o més de 32 bits. Dins del cos hi ha el missatge, per exemple un missatge TCP/IP.

A la capçalera es pot trobar la informació següent:

- **Versió IP**: són 4 bits que indiquen el número de versió del protocol IP. Tot i que actualment es treballa de forma habitual amb la versió 4 d'IP, ja fa temps que s'ha iniciat el canvi a la versió 6.
- **Longitud de capçalera**: són 4 bits que indiquen la longitud de la capçalera. Per realitzar aquesta acció s'empren paraules de 32 bits, sent la longitud mínima d'una capçalera de 20 bytes.
- **Tipus de servei**: són 8 bits que

s'utilitzen per indicar si el datagrama ha de ser reenviat o s'ha de realitzar qualsevol altra acció.

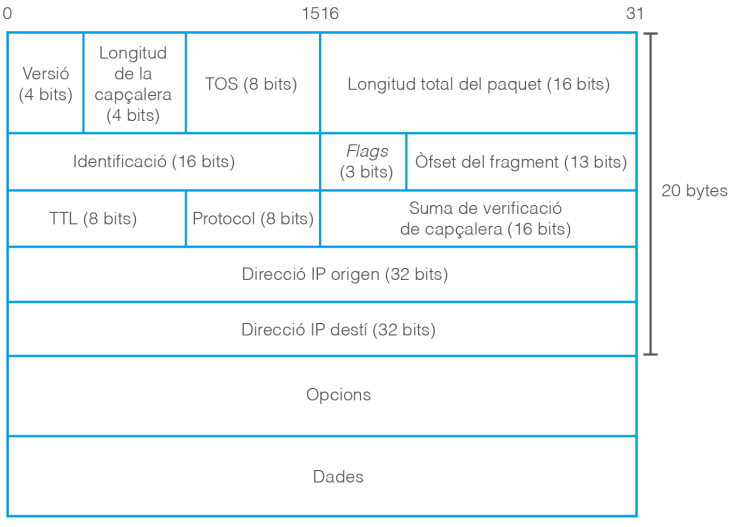
- **Longitud de datagrama**: són 16 bits que indiquen la longitud del datagrama IP en bytes. És important tenir en compte que aquesta longitud inclou la capçalera i el cos.
- **Identificador de paquet**: són 16 bits que identifiquen a quin datagrama pertanyen els paquets d'informació.

- **Indicador de fragmentació**: són 3 bits que indiquen si el datagrama està fragmentat o no. Aquest indicador s'utilitza sobretot per comprovar si tots els fragments del datagrama han arribat a la destinació quan es rep l'últim fragment.
- **Desplaçament de fragmentació**: són 13 bits que s'utilitzen per indicar la posició del fragment dins del datagrama.
- **Temps de vida**: són 8 bits que s'utilitzen per evitar que els datagrames circulin indefinidament dins d'una xarxa. Aquest valor decreix en una unitat cada vegada que el paquet travessa un encaminador. En arribar el valor zero, el paquet ja no es reenvia i es retorna un missatge d'error.
- **Protocol**: són 8 bits que indiquen el tipus de dades contingut. Alguns exemples són 1 per ICMP, 6 per TCP o 17 per UDP.
- **Suma de comprovació**: són 16 bits que s'utilitzen per comprovar la integritat de la capçalera. Aquest camp no indica res sobre la integritat del cos del missatge.
- **IP origen**: són 32 bits que indiquen l'adreça IP de la màquina que ha enviat el datagrama.
- **IP destinació**: són 32 bits que indiquen l'adreça IP de la màquina a qui va destinat el datagrama.
- **Opcions i farcit**: es tracta d'un camp de longitud variable que pot indicar diferents opcions d'IP. S'ha d'omplir fins arribar a 32 bits.

Un datagrama es pot fragmentar en paquets d'informació. Tots els paquets d'informació que pertanyin a un mateix datagrama tindran el mateix identificador de paquet.

En la figura 1.10 es mostra l'estructura d'un datagrama IP. Aquesta estructura s'acaba aprenent gairebé de memòria quan es realitza el filtratge de paquets que circulen per una xarxa.

FIGURA 1.10. Capçalera d'un paquet IP



http://www.cisco.com/

Datagrames ICMP

Els datagrames ICMP *(Internet Control Message Protocol)* s'utilitzen principalment per realitzar proves de xarxa o retornar codis d'error. Els datagrames ICMP no viatgen sols per la xarxa, sinó que són transportats dins del cos dels datagrames IP.

Dins d'un datagrama ICMP es pot trobar la informació següent:

- **Tipus de missatge**: són 8 bits que indiquen el tipus de missatge ICMP.
- **Codi de missatge**: són 8 bits que s'utilitzen per proporcionar informació detallada del tipus de missatge ICMP.
- **Comprovació de suma**: són 16 bits que s'utilitzen per comprovar la integritat del missatge ICMP.
- **Dades ICMP**: té una longitud variable i el seu contingut variarà segons el tipus de missatge.

Per a més informació sobre els datagrames ICMP consulteu l'RFC 792.

Alguns dels tipus de missatge que existeixen són:

- 0: resposta ECO.
- 3: no es pot arribar a la destinació.
- 4: s'ha arribat a la destinació.
- 5: redireccionament.
- 8: ECO.
- 11: temps de vida esgotat.
- 12: problema amb algun paràmetre.
- 13: data i hora.
- 14: resposta de data i hora.
- 15: sol·licitud d'informació.
- 16: resposta d'informació.

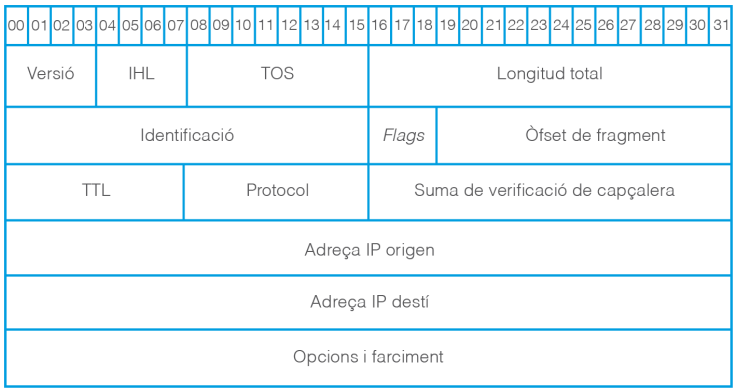
Alguns codis de missatge són:

- 0: no es pot arribar a la xarxa.
- 1: no es pot arribar a la màquina de destinació.
- 2: protocol inassolible.
- 3: port inassolible.
- 4: és necessari fragmentar la informació.

- 5: error en la ruta d'origen.

En la figura 1.11 es mostra l'estructura d'un datagrama ICMP. Com es pot observar, va precedit per la capçalera IP.

FIGURA 1.11. Capçalera d'un datagrama ICMP



Datagrames UDP

Els datagrames UDP s'utilitzen principalment en protocols com DHCP, BOOTP o DNS. El protocol UDP (*User Datagram Protocol*), situat a la capa 4 del model OSI, permet l'enviament de datagrames sense haver establert connexió prèviament. Això és possible ja que el protocol UDP conté a la capçalera tota la informació necessària per realitzar l'adreçament. Els datagrames UDP no viatgen sols per la xarxa, sinó que són transportats dins del cos dels datagrames IP. Aquest protocol no treballa amb confirmació d'entrega ni de recepció, ni es preocupa de controlar el flux del trànsit. Treballant amb UDP els paquets que es transmeten poden arribar de forma desordenada a la destinació i allà s'hauran d'ordenar correctament.

Dins d'un datagrama UDP es pot trobar la informació següent:

- **Port d'origen**: són 16 bits que indiquen quin és el port origen del datagrama.
- **Port de destinació**: són 16 bits que indiquen quin és el port de destinació del datagrama.
- **Longitud del datagrama**: són 16 bits que indiquen la longitud en bytes del datagrama. Aquest valor és el total de sumar la capçalera i les dades del datagrama UDP.
- **Suma de comprovació**: són 16 bits que indiquen la integritat de la capçalera IP, la capçalera UDP i les dades UDP.
- **Dades UDP**: és de longitud variable segons les necessitats.

La figura 1.12 mostra l'estructura d'un datagrama UDP.

FIGURA 1.12. Capçalera d'un datagrama UDP

La comunicació entre entre aplicacions per UDP requereix l'ús de ports. Els ports possibles per al protocol UDP són els que van del 0 al 65535.

La raó per la qual els ports vàlids per al protocol UDP van del 0 al 65535 és que a l'estructura del paquet UDP es dediquen 16 bits per marcar aquest valor. I $2^{16} = 65535$.

Si per exemple es necessita emetre veu o imatge generalment s'utilitzarà el protocol UDP. Treballant amb UDP es prioritza la velocitat a la generació d'errors o a la pèrdua d'informació.

Datagrames TCP

Els datagrames TCP *(Transport Control Protocol)* s'utilitzen principalment en la comunicació entre equips de xarxa on s'ha de garantir el lliurament de dades de manera ordenada i sense errors. Els datagrames TCP no viatgen sols per la xarxa, sinó que són transportats dins del cos dels datagrames IP.

Dins d'un datagrama TCP es pot trobar la informació següent:

- **Port d'origen**: són 16 bits que indiquen el port origen del datagrama.
- **Port de destinació**: són 16 bits que indiquen el port de destinació del datagrama.
- **Número de seqüència**: són 32 bits que indiquen la posició del datagrama dins del grup de dades. Aquest número serveix per acoblar els datagrames quan arribin a la destinació en ordre i detectar si s'ha produït algun error.
- **Número de reconeixement**: són 32 bits que s'utilitzen per informar al receptor del datagrama que el remitent ha processat els datagrames anteriors. Aquest camp s'utilitza per garantir el lliurament dels datagrames.
- **Desplaçament de dades**: són 4 bits que indiquen la mida de la capçalera TCP. Aquesta quantitat es mesura en paraules de 32 bits.
- **Indicadors TCP**: són 8 bits que s'utilitzen per indicar diferents condicions i esdeveniments.
- **Finestra**: són 16 bits que s'utilitzen per sincronitzar la comunicació entre equips que tenen diferents velocitats de dades.
- **Suma de comprovació**: són 16 bits que s'utilitzen per comprovar la integritat de la capçalera i les dades.
- **Punter urgent**: són 16 bits que s'utilitzen quan l'indicador URG està establert.

- **Dades**: és de longitud variable i conté les dades.

A la taula 1.4 es mostren alguns dels indicadors i la seva descripció.

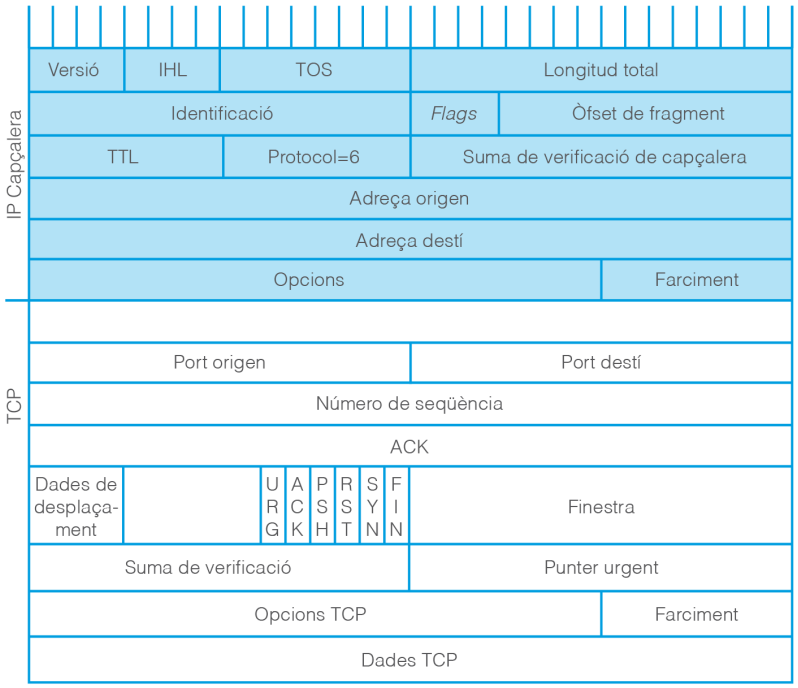
TAULA 1.4. Indicadors TCP

Posició del bit	Indicador	Descripció
0	SYN	Indica l'inici d'una connexió TCP.
1	ACK	El número de reconeixement indica el número de seqüència dels proper byte de dades.
2	RST	Indica que el remitent ha interromput la connexió.
3	PSH	Indica que el receptor ha de permetre que les dades siguin disponibles per a la capa d'aplicació.
4	URG	Identifica dades que s'han de processar urgentment.
5	FIN	Indica que el remitent ha completat la comunicació i procedirà a tancar la connexió.
6-7	RES	En determinades ocasions s'utilitza per indicar que la xarxa està congestionada.

El protocol TCP l'utilitzen protocols com HTTP, SMTP, SSH o FTP. A més és emprat per navegadors, programes d'intercanvi de fitxers o clients FTP.

En la figura 1.13 es mostra l'estructura d'un datagrama TCP.

FIGURA 1.13. Capçalera d'un datagrama TCP



Quan s'estableix una comunicació entre una aplicació emissora i una aplicació receptora és necessari assignar com a mínim un número de port vàlid a cada extrem. Els ports possibles per al protocol TCP són els que van del 0 al 65535.

La raó per la qual els ports vàlids per al protocol TCP van del 0 al 65535 és que a l'estructura del paquet TCP s'hi dediquen 16 bits per marcar aquest valor: 2^{16} = 65535.

1.4.3 Instal·lació del tallafoc. Ubicació

La decisió d'instal·lar o no un tallafoc no comporta grans maldecaps. En la majoria d'ocasions la resposta és clara: sí, necessites instal·lar un tallafoc. El que no és tan evident és on s'ha d'instal·lar el tallafoc.

Una xarxa informàtica segueix una arquitectura de disseny i una norma d'implementació on cada component està ubicat on pertoca. No es tracta d'endollar aparells a la xarxa i esperar que facin la seva tasca. Caldrà analitzar on s'haurà d'ubicar el tallafoc dins la xarxa perquè aquest sigui més efectiu.

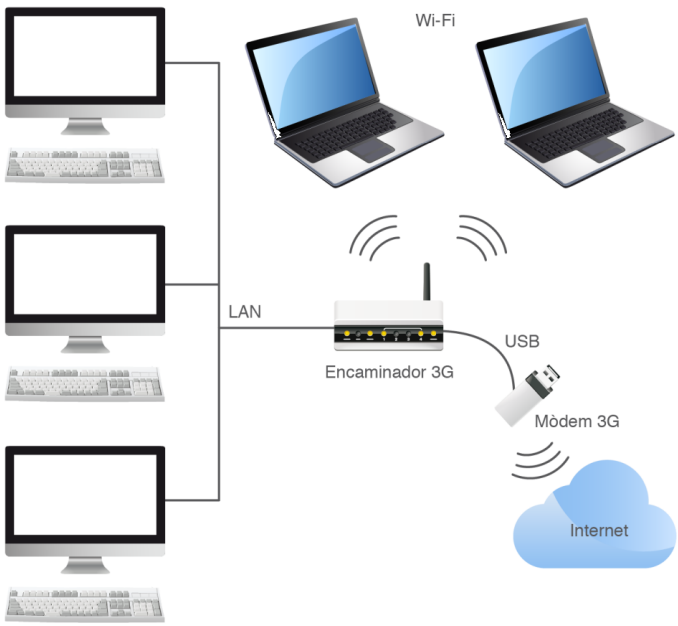
Existeixen una sèrie d'arquitectures força comunes que han estat provades abastament, la qual cosa ens proporciona una valuosa informació sobre els seus avantatges i inconvenients. Es comenten tres arquitectures: el tallafoc d'encaminador, el tallafoc d'una única màquina i el tallafoc de múltiples màquines.

Tallafoc d'encaminador

Aquesta és possiblement l'arquitectura de tallafoc més simple que hi ha. Es tracta d'aprofitar les característiques d'un encaminador per realitzar tasques de tallafoc. Un encaminador s'encarrega de reenviar paquets seguint una política, i reenviar paquets es pot considerar una forma molt simple de filtrar paquets pensant en la protecció de la xarxa.

En la figura 1.14 es pot observar una xarxa a la qual accedeixen diversos dispositius però no s'observa cap tallafoc. Això no vol dir que no hi sigui, ja que l'encaminador segurament estigui realitzant tasques de tallafoc.

FIGURA 1.14. Xarxa amb encaminador



Un estudiant de xarxes veurà de seguida que aquesta arquitectura no és gaire potent, ja que el filtratge consisteix a analitzar únicament les adreces IP. Però no hi ha cap dubte que és una solució barata, senzilla i eficaç fins a cert nivell, a part d'estar a l'abast de tot usuari que usi un encaminador.

Las raons que ens fan descartar l'ús d'aquesta arquitectura són bàsicament tres:

- No és una arquitectura flexible.
- Les màquines públiques i privades comparteixen xarxa.
- La defensa té una greu manca de profunditat.

La falta de flexibilitat d'aquesta arquitectura està condicionada per les característiques de l'encaminador. Un encaminador que només faci reenviament de paquets no es pot programar per bloquejar o acceptar paquets en funció dels ports que s'utilitzin. Tot el que s'ofereixi a la part interna de la xarxa quedarà exposat a l'exterior.

Quan les màquines públiques i privades comparteixen una mateixa xarxa, la seguretat de la part privada es veu compromesa. Des d'una màquina pública es possibilita l'accés sense limitacions a la part privada.

Quan es parla de manca de profunditat fa referència a que només es proporciona una capa de seguretat. Si algun intrús supera l'encaminador, la xarxa queda completament oberta, sense cap altra mesura defensiva.

Llistes d'accés de Cisco

Les llistes d'accés per filtrar adreces IP i filtrar el trànsit d'una xarxa es poden aplicar en alguns dels sistemes operatius de Cisco.

Les llistes d'accés són conegudes popularment com ACL (*Access Control List*).

Hi ha diversos conceptes que s'han de tenir clars per poder treballar amb ACL. L'ús de llistes d'accés està molt estès i amb raó, ja que és un mecanisme molt pràctic. Però corre la idea errònia de que les ACL són molt complexes i difícils d'entendre. Segurament el més difícil d'entendre són les màscares que s'utilitzaran. La màscara es pot utilitzar com:

- Màscara revertida
- ACL de sumari
- ACL de sumari parcial

1) Màscara revertida: s'utilitza amb les adreces de xarxa per especificar què es permet i què es denega. Les màscares s'inicien amb el valor 255 per especificar tot un segment de xarxa i van decreixent segons les restriccions. Les màscares que s'utilitzen en ACL no són exactament les màscares de xarxa que habitualment

s'utilitzen en el disseny de xarxes. Les màscares que s'utilitzen en ACL s'anomenen *màscares revertides*, *màscares inverses* o *màscares wildcard*. Si es tradueix el valor de la màscara a codi binari, el resultat determina quines adreces són les que s'han de tenir en compte en el processament de trànsit. Els zeros indiquen que l'adreça ha de ser considerada, i els uns, que "tant se val". Per determinar la màscara revertida es pot restar a la màscara 255.255.255.255 la màscara de xarxa corresponent.

Exemple de màscara revertida

1. Es disposa de l'adreça de xarxa 192.168.0.0 amb màscara de xarxa 255.255.255.0 i amb la màscara revertida 0.0.0.255.
2. Es tradueix 192.168.0.0 a binari:

   11000000.10101000.00000000.00000000
3. Es tradueix 0.0.0.255 a binari:

   00000000.00000000.00000000.11111111
4. Els tres primers octets de la màscara revertida indiquen que s'han d'agafar exactament els valors de l'adreça IP (192.168.0).
5. L'últim octet de la màscara *wildcard* indica que "tant se val" el valor dels últims vuit octets. Això vol dir que es processarà qualsevol adreça de xarxa que vagi de la 192.168.0.1 a la 192.168.0.255.
6. Per trobar la màscara revertida que s'ha utilitzat només cal restar a la màscara 255.255.255.255 la màscara de xarxa corresponent, que en aquest cas és 255.255.255.0, sent el resultat 0.0.0.255.

2) ACL de sumari: es pot fer un sumari d'un conjunt de subxarxes que es vegin afectades per una ACL. En comptes d'escriure una ACL per a cada subxarxa a tractar es pot fer una ACL que aglutini el màxim de subxarxes.

Exemple d'ACL de sumari

Es desitja dissenyar una ACL que cobreixi les subxarxes següents:

- 192.168.80.0/24
- 192.168.81.0/24
- 192.168.82.0/24
- 192.168.83.0/24

Es pot veure que l'únic octet diferent a tots els casos és el tercer (té els valors 80, 81, 82 i 83) i per això serà el que utilitzem per calcular la máscara revertida.

Passem a binari l'octet que canvia (que en aquest cas és el tercer):

- 80 -> 01010000
- 81 -> 01010001
- 82 -> 01010010
- 83 -> 01010011

Per determinar la *wildcard* cal detectar els bits que mai canvien i els que sí canvien. En aquest cas els sis primers bits no canvien i els últims dos sí.

A més, es pot observar que els valors que canvien són tots els possibles valors que es poden obtenir amb dos bits (0, 1, 2, 3 i 4).

Tant se val quin valor tinguin els dos últims bits d'aquest tercer octet, i això és així perquè tots els possibles valors estan contemplats. Això es tradueix en que la màscara revertida serà 00000011 o, el que és el mateix, 3.

El valor complet de la màscara revertida que cobreix aquestes quatre subxarxes és 0.0.3.255.

La línia completa que definiria l'ACL seria:

```
1 access-list acl_permetre permit ip 192.168.80.0 0.0.3.255
```

Utilitzar /24 és el mateix que utilitzar 255.255.255.0 i el que indica és que la màscara té vint-i-quatre uns: 11111111.11111111.11111111.00000000

3) ACL de sumari parcial: en determinats casos no es pot realitzar un sumari que englobi totes les subxarxes a tractar i caldrà fer-ho per parts.

Exemple d'ACL de sumari parcial

Es desitja dissenyar una ACL que cobreixi les següents subxarxes:

- 192.168.86.0/24
- 192.168.87.0/24
- 192.168.88.0/24
- 192.168.89.0/24

Es pot veure que l'únic octet diferent a tots els casos és el tercer (té els valors 86, 87, 88 i 89) i per això serà el que utilitzem per calcular la màscara revertida. Passem a binari l'octet que canvia (el tercer):

- 86 -> 01010110
- 87 -> 01010111
- 88 -> 01011000
- 89 -> 01011001

Per determinar la màscara revertida caldrà detectar els bits que mai canvien i els que sí canvien. En aquest cas els quatre primers bits no canvien i els últims quatre sí.

En aquest cas es detecta que no apareixen tots els possibles valors que es poden generar amb tres bits: només es treballa amb 0110, 0111, 1000 i 1001.

Si no estan contemplats tots els valors cal dividir la màscara revertida. Es pot observar que l'única diferència entre les dues primeres subxarxes és l'últim bit:

- 86 -> 01010110
- 87 -> 01010111

Això permet establir la *wildcard* 0.0.1.255. La línia completa que definiria l'ACL seria:

```
1 access-list acl_permetre permit ip 192.168.86.0 0.0.1.255
```

En el cas de les dues últimes subxarxes també és l'últim bit el que canvia:

- 88 -> 01011000
- 89 -> 01011001

Això permet establir la màscara revertida 0.0.1.255. La línia completa que definiria l'ACL seria:

```
access-list acl_permetre permit ip 192.168.88.0 0.0.1.255
```

El funcionament de les ACL és molt simple: quan el trànsit de xarxa entra a l'encaminador es compara amb les llistes d'accés que l'encaminador té configurades. Val a dir que les ACL estan ordenades i es llegeixen en ordre. L'encaminador compara el trànsit amb totes les regles fins que troba alguna que coincideix amb les característiques del trànsit. Si es dóna el cas de que no coincideix el trànsit amb cap regla de la llista se li denega el pas.

L'ACL següent permet el trànsit que surt de qualsevol equip que pertany a la xarxa 192.168.0.0 i que vagi a qualsevol equip de la xarxa 192.168.1.0, i la resta de trànsit es denega.

```
access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
```

I el cas següent té el mateix resultat, però s'indica en dos passos: primer s'indica el trànsit permès i a continuació s'especifica que la resta de trànsit s'ha de denegar.

```
access-list 102 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 102 deny ip any any
```

Les ACL es poden utilitzar per filtrar el trànsit d'una forma més concreta. Per exemple la línia següent permetria el trànsit Telnet entre una màquina amb adreça de xarxa 192.168.1.26 i una altra màquina amb adreça de xarxa 192.168.0.5. Cal destacar que per indicar una màquina concreta es pot utilitzar l'etiqueta *host* i evitar d'aquesta manera utilitzar màscares revertides.

```
access-list 101 permit tcp host 192.168.1.26 host 192.168.0.5 eq telnet
```

Si no volem ser tant estrictes podem permetre qualsevol tipus de trànsit TCP:

```
access-list 101 permit tcp host 192.168.1.26 host 192.168.0.5
```

O de trànsit UDP:

```
access-list 101 permit tcp host 192.168.1.26 host 192.168.0.5
```

El tractament de diferents protocols a nivell de subxarxa segueix el mateix procediment. Per permetre el trànsit IP entre dues subxarxes hem d'escriure:

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
```

Denegació total

Les ACL només tenen efecte si s'apliquen a les interfícies d'un encaminador. També cal recordar que una llista d'accés té una denegació total de forma implícita al final del llistat.

Un altre conjunt de conceptes bàsics per entendre i aplicar les ACL són els que indiquen si el trànsit a tractar és d'entrada o sortida o si el que s'estudia és l'origen d'aquest trànsit o bé la seva destinació:

- ***In***: fa referència al trànsit que arriba a la interfície de l'encaminador i que provarà de travessar-lo. L'origen del paquet és la procedència del paquet i la destinació és on vol anar una vegada travessi l'encaminador.
- ***Out***: fa referència al trànsit que ha travessat l'encaminador i surt per una de les seves interfícies. En aquest cas l'origen és la procedència del trànsit (fora de l'encaminador) i la destinació és cap a on va aquesta informació.
- ***Inbound***: l'encaminador analitza el paquet d'informació que rep. Si el paquet és permès es continuarà processant el paquet. Si aquest paquet no és permès es descartarà.
- ***Outbount***: després de rebre i encaminar el paquet cap a la interfície correcta, l'encaminador analitza el paquet i el compara amb el llistat d'ACL. Si el paquet és permès es transmet. Si el paquet no és permès es descarta.

Tallafoc d'una màquina

Implementar un tallafoc en una màquina té el gran avantatge de permetre separar la xarxa protegida en dues subxarxes:

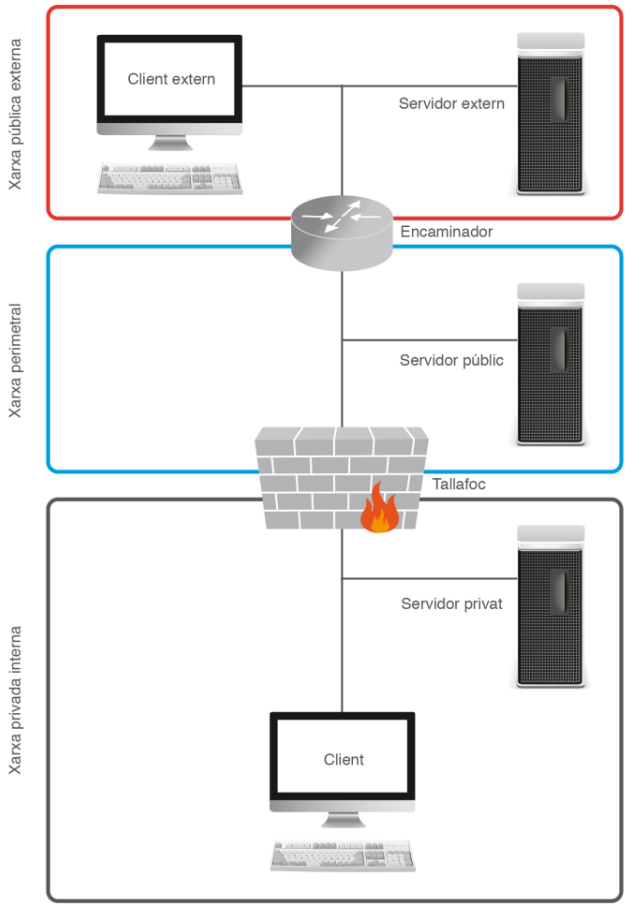
- Una xarxa privada interna.
- Una xarxa perimetral, coneguda popularment com a *zona desmilitaritzada* (DMZ).

Són possibles dues arquitectures quan s'ubica un tallafoc en una màquina:

- Arquitectura de tallafoc exposat.
- Arquitectura de tallafoc d'apantallament.

En una **arquitectura de tallafoc exposat**, la xarxa privada interna està protegida pel tallafoc, que pot filtrar i reenviar els paquets que circulen en ambdós sentits: cap a la xarxa perimetral i cap a la xarxa privada interna. En la figura 1.15 es pot observar que a la xarxa perimetral s'hi han ubicat els servidors públics per tal d'aïllar-los dels servidors privats i dels clients interns de la xarxa. Si la xarxa pateix un atac cap a un servidor públic, la xarxa privada interna no patirà un perill immediat.

Figura 1.15. Tallafoc exposat

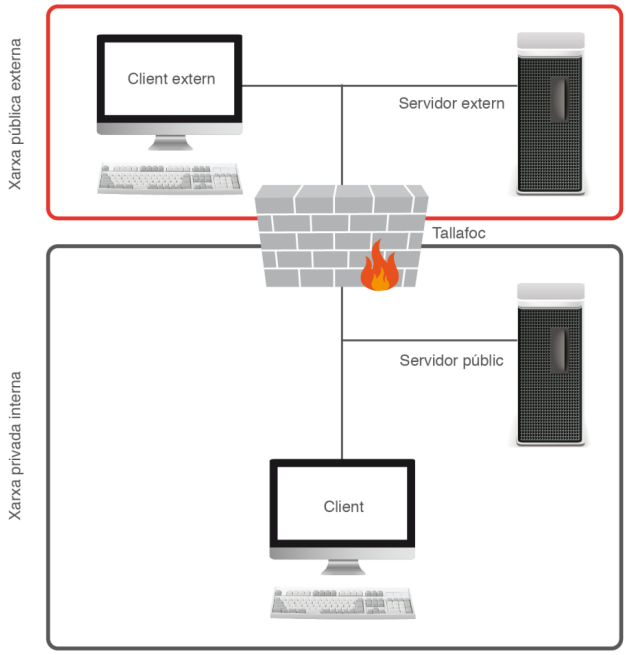


El perill més gran que presenta l'arquitectura de tallafoc exposat és l'exposició dels servidors públics. Aquests han de disposar d'un reforç especial en les seves configuracions per tal de resistir atacs.

En moltes ocasions s'assigna als servidors públics que veuen reforçada la seva seguretat el nom d'**equips bastió.**

L'arquitectura de tallafoc d'**apantallament** és similar a la de tallafoc exposat, la gran diferència és que els servidors públics se situen darrere del tallafoc, com es pot veure en la figura 1.16. Aquesta acció redueix la vulnerabilitat dels atacs. En aquest cas, però, existeix el risc que si un servidor públic és atacat, la xarxa privada interna es veu compromesa.

FIGURA 1.16. Tallafoc apantallat



Són avantatges de les dues arquitectures que:

- Tot i ser més cares que el tallafoc d'encaminador continuen sent barates.
- Ofereixen més flexibilitat que el tallafoc d'encaminador.
- Les màquines privades estan protegides pel tallafoc.

Un avantatge de l'arquitectura de tallafoc d'apantallament respecte al tallafoc exposat és que els servidors públics també estan protegits pel tallafoc.

Són inconvenients de les dues arquitectures que es tracta d'una defensa vulnerable que només depèn del tallafoc.

Un inconvenient del tallafoc exposat és que els servidors públics són vulnerables.

Un inconvenient del tallafoc d'apantallament és que els equips de la xarxa d'àrea local (LAN) són vulnerables si un servidor públic es veu compromès.

Tallafoc de múltiples màquines

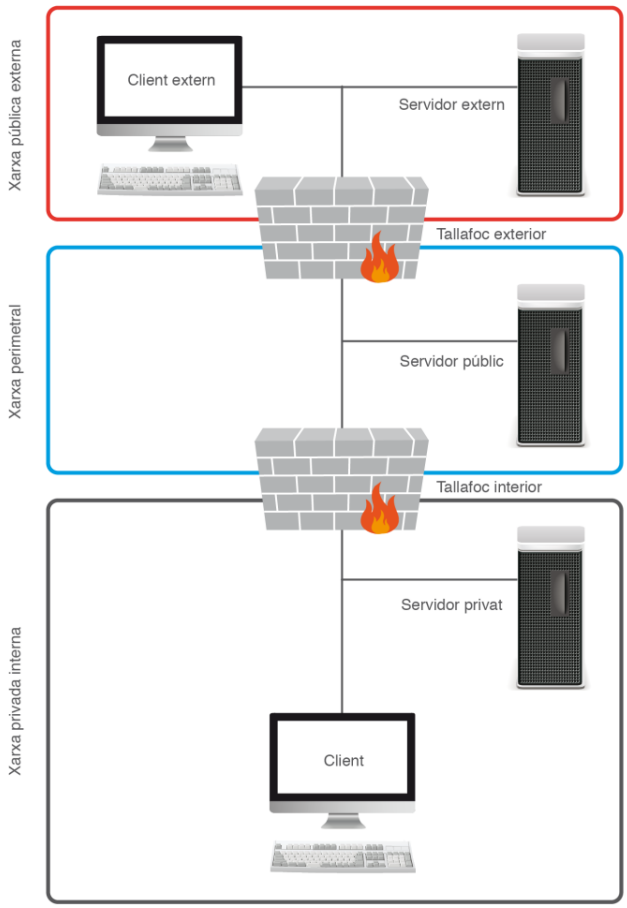
En determinades circumstàncies, amb una única màquina dedicada a funcions de tallafoc la xarxa continua exposada a vulnerabilitats. En aquests casos és interessant utilitzar tallafoc de múltiples màquines.

Un tallafoc de múltiples màquines consisteix a utilitzar més d'un equip per protegir les màquines de la xarxa, la qual cosa proporciona una major seguretat.

Existeixen dues arquitectures de tallafoc de múltiples màquines: el tallafoc de xarxa apantallada i el tallafoc de tres direccions.

La figura 1.17 mostra un exemple de tallafoc de xarxa apantallada, on s'utilitzen un tallafoc interior, conegut com a *tallafoc d'obstrucció*, i un tallafoc exterior, conegut com a *tallafoc de porta d'enllaç*. El tallafoc d'obstrucció separa la xarxa privada interna de la xarxa perimetral. El tallafoc de porta d'enllaç separa la xarxa perimetral de la xarxa pública externa.

Figura 1.17. Tallafoc de xarxa apantallada



Cal destacar que la diferència entre un tallafoc exposat i un tallafoc de xarxa apantallada és la substitució de l'encaminador per un segon tallafoc. Aquest segon tallafoc protegeix els servidors públics de les amenaces externes.

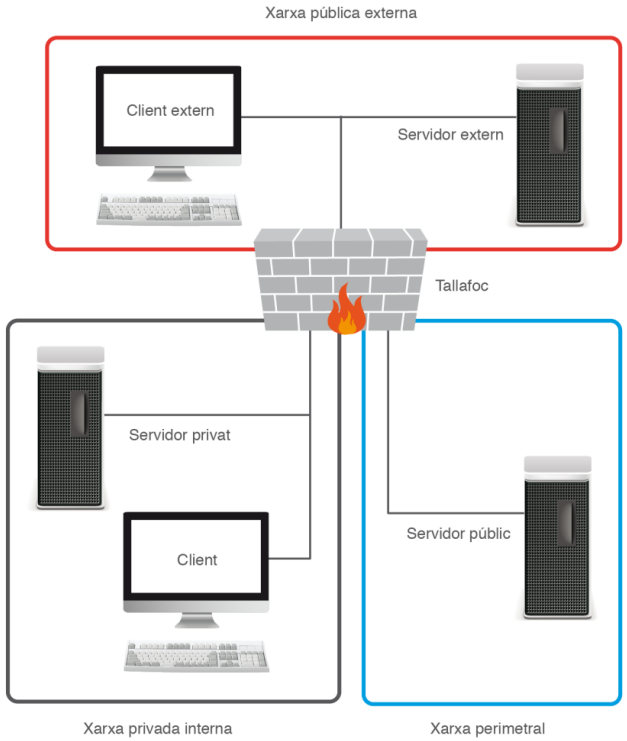
L'arquitectura de tallafoc de xarxa apantallada protegeix els servidors públics i les màquines privades i ofereix una defensa estructurada en diverses capes. L'inconvenient que presenta, però, és que resulta més car que les arquitectures que utilitzen una sola màquina.

El tallafoc de tres direccions fa seus els avantatges del tallafoc de xarxa apantallada i els de les arquitectures d'una màquina. És una única màquina amb tres targetes de xarxa: una per a la xarxa pública externa, una per a la xarxa perimetral i una última per a la xarxa privada interna.

L'arquitectura de tallafoc de tres direccions, tal com es pot observar en la figura 1.18, assegura que els servidors públics i les màquines privades estaran protegits per un tallafoc, la defensa es continua estructurant en diverses capes i la

implantació és més barata que en el cas de l'arquitectura en xarxa apantallada. Aquesta arquitectura continua sent més cara que una arquitectura d'una sola màquina, ja que l'equip que s'utilitza de tallafoc ha de tenir almenys tres targetes de xarxa i la seva configuració i administració és més complexa que l'arquitectura de xarxa apantallada.

FIGURA 1.18. Tallafoc de tres direccions



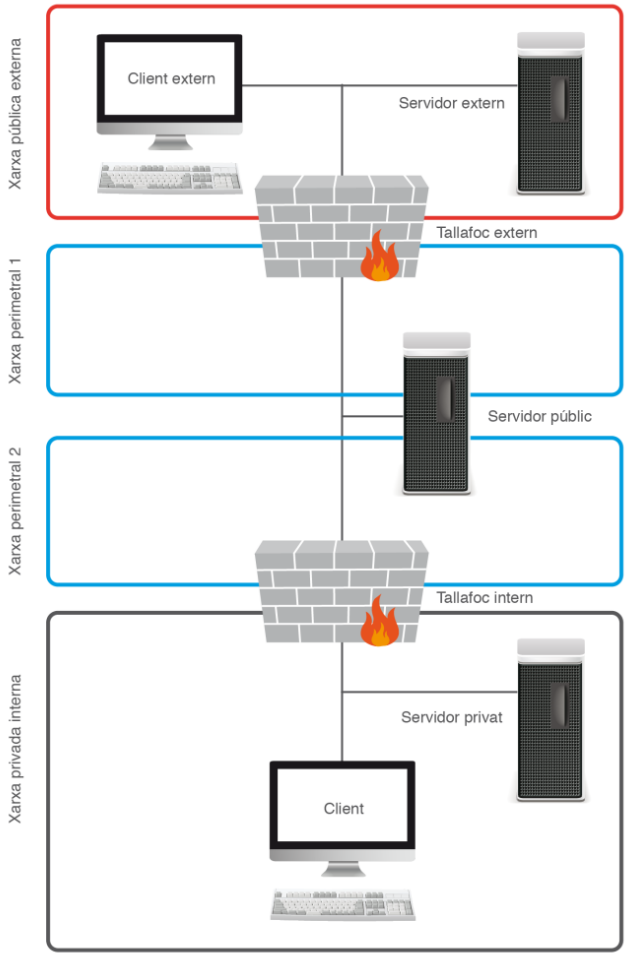
Altres arquitectures

Amb el decurs del temps les necessitats de seguretat de les xarxes van demanant solucions que no s'ajusten exactament a les arquitectures bàsiques d'una màquina o de múltiples màquines. Així, sorgeixen arquitectures modelades segons circumstàncies molt particulars. A continuació s'enumeren algunes de les arquitectures més populars.

- **Arquitectura de xarxa apantallada dividida**: consisteix a utilitzar una arquitectura de xarxa apantallada i substituir els servidors públics per servidors públics amb dues targetes de xarxa. En aquest, com es pot observar en la figura 1.19, s'utilitzen els servidors públics com a capa de defensa per als servidors privats. El servidor públic fa d'enllaç entre les xarxes perimetrals.
- **Arquitectura de xarxa apantallada múltiple**: consisteix a utilitzar una arquitectura de xarxa apantallada dividida i utilitzar més d'un equip entre les xarxes perimetrals.
- **Arquitectura de tallafoc empresarial**: consisteix a afegir redundància des de la xarxa privada interna a les xarxes públiques externes. Tot i que aquesta

arquitectura està clarament basada en una arquitectura de xarxa apantallada, el nivell de seguretat és enorme.

FIGURA 1.19. Tallafoc de xarxa apantallada dividida



1.4.4 Regles de filtratge del tallafoc

Per una xarxa hi circulen paquets d'informació. A l'inici del paquet s'indica la destinació, qui l'ha enviat, de quin tipus de paquet es tracta... A aquesta part del paquet l'anomenem *capçalera*.

> La **capçalera** se situa a l'inici del bloc d'informació del paquet i conté dades suplementàries necessàries per a la correcta gestió del bloc d'informació.

Filtrar paquets consisteix a analitzar la capçalera del paquet i decidir la destinació de tot el paquet analitzat.

Actualment, molts llocs web implementen comunicació encriptada, inicialment amb **SSL** i, posteriorment, amb **TSL**. Evidentment, aquesta comunicació encriptada és necessària en alguns casos, com quan volem realitzar compres per Internet

o volem accedir al nostre banc. Però, a més d'aquests casos on l'encriptació és necessària, també s'utilitza en casos on, en principi, no ho és, com, per exemple, en connectar-se a Google per a realitzar una consulta. En tenir, però, comunicacions encriptades, el tallafoc no pot filtrar els paquets segons el seu contingut, ja que desconeix la informació que contenen. En aquests casos, el tallafoc té més feina de la que tenia anteriorment, ja que també ha de desencriptar la informació. Per desencriptar la informació, el tallafoc necessita **la funcionalitat d'interceptació SSL/TLS**. Hi ha dos mecanismes per desencriptar la informació. Un d'ells utilitza atacs tipus *Man-in the-Middle*, ja que el xifrat de les dades és obligatori, però l'autenticació no ho és; tot i així, normalment s'autentica el servidor. Per a realitzar aquests atacs es poden usar eines com **BurpSuite**. De totes maneres, s'ha de destacar que interceptar tràfic SSL que no sigui nostre sense consentiment o autorització no és legal. Al cas d'un tallafoc d'una organització, s'hauria de demanar permís als usuaris, encara que en fossin empleats. El segon atac consisteix en atacar la fase de negociació de la clau SSL entre el client i el servidor. El client i el servidor negocien un *premaster secret* comú, d'aquest premaster secret es derivarà el master secret que s'utilitzarà per crear les claus criptogràfiques. Si obtenim el premaster secret, aleshores podrem realitzar tots els càlculs per obtenir les claus finals tal i com fan client i servidor. Aquesta opció és la que necessita menys esforç, ja que els navegadors permeten guardar el premaster secret a un fitxer.

A continuació, es mostren 6 protocols de la família SSL/TLS i els problemes que tenen:

- **SSLv2**: prohibit el seu ús per la Internet Engineering Task Force (RFC 6176).
- **SSLv3**: obsolet, no suficientment segur (RFC 7568).
- **TLS1.0**: considerat com a no segur (vulnerable a l'atac BEAST). No s'ha d'usar més. No és acceptat per la norma PCI (juny del 2018).
- **TLS1.1**: no té més problemes de seguretat coneguts, però no ofereix les característiques de xifrat modernes (RFC 5246, secció 1.2).
- **TLS1.2**: no té més problemes de seguretat coneguts i ofereix les característiques modernes de xifrat de tipus AEAD.
- **TLS1.3**: A l'agost de 2018, la Internet Engineering Task Force ha publicat TLS 1.3, que suprimeix les opcions problemàtiques de les versions anteriors de TLS i els seus algorismes no tenen vulnerabilitats conegudes. Aquest hauria de ser el principal protocol a usar a l'actualitat.

Quan es fa un filtratge es pot denegar el paquet, acceptar-lo o bé rebutjar-lo. **Denegar un paquet** consisteix a eliminar-lo i tractar-lo com si mai hagués estat rebut. **Acceptar un paquet** consisteix a deixar-lo passar cap al següent punt del camí. I **rebutjar un paquet** consisteix a eliminar el paquet i avisar l'emissor que el paquet s'ha eliminat.

Podeu analitzar la seguretat SSL/TSL dels Servidors web amb aquesta web: bit.ly/3cOcHZc.

Filtrar paquets aporta seguretat, control i vigilància sobre la xarxa informàtica. **Aporta seguretat** perquè permet restringir el trànsit que arriba a la xarxa. **Permet control** sobre el trànsit intern de la xarxa. I **permet rebre avisos** quan algun aspecte de la xarxa interna no funciona correctament.

Hi ha molts exemples de tallafocs, però és important estudiar els casos d'IPTables i NFTables per entendre millor les regles de filtratge.

Filtratge amb IPTables

IPTables és un tallafoc que requereix un nucli basat en Linux per poder-se executar. El seu ús està molt estès i se'l considera el substitut de l'antic i, en el seu temps, popular IPChains, tot i que en ocasions se'ls pot trobar treballant en equip (IPTables en primera línia de defensa i IPChains en segona línia).

IPTables filtra paquets amb **estat**, dona suport a **emmascarament IP**, a NAT d'origen i de destinació, permet realitzar un registre de paquets i s'executa des de línia d'ordres, tot i que hi ha aplicacions gràfiques que ho poden evitar.

Les regles del tallafoc estan a nivell de nucli, i és el nucli el que ha de decidir què fer amb els paquets d'informació que li arriben.

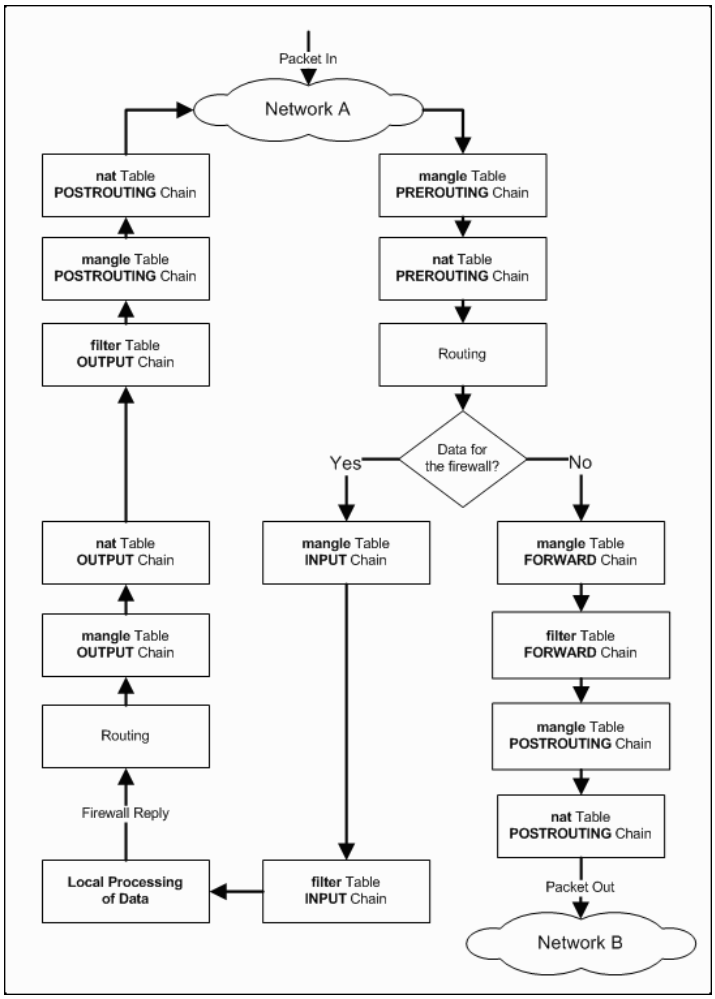
La figura 1.20 mostra esquemàticament el procés que segueix un paquet inspeccionat per IPTables. En ella es pot veure que treballant amb IPTables els paquets poden seguir camins diferents, depenent de l'origen i de la destinació. L'ordre que se segueix és:

1. ***mangle prerouting***: aquesta és la primera cadena que travessen els paquets que arriben al tallafoc. Normalment no s'inclouen regles, per tant, els paquets passen directament a la cadena següent.
2. ***nat prerouting***: aquesta cadena la travessen tots els paquets que arriben al tallafoc. Aquí es poden incloure regles que modifiquin l'adreça IP de destinació o el port de destinació del paquet.
3. ***Camí***: en aquest pas es classifiquen els paquets segons la destinació. Tots aquells paquets que portin una adreça IP de destinació coincident amb una de les interfícies del tallafoc s'enviaran a *filter input*, i la resta s'enviaran a *filter forward*.
4. ***filter forward***: aquesta cadena té per missió processar els paquets que es reenvien una xarxa a una altra. Generalment és aquí on es decideix si es deixa passar un paquet o si es bloqueja.
5. ***nat postrouting***: en aquest pas es tradueixen les adreces de xarxa d'origen i l'emmascarament.
6. ***filter input:*** s'encarrega de tractar els paquets destinats al tallafoc. Conté regles que avaluen si el paquet ha de ser acceptat o bloquejat.
7. ***Procés local***: aquest procés s'executa al tallafoc. El procés podria ser l'origen o la destinació dels paquets.

8. ***mangle output***: només els paquets generats pel tallafoc travessen aquesta cadena.

9. ***filter output***: processa els paquets enviats pel tallafoc. Pot determinar si el paquet ha de bloquejar-se o no.

FIGURA 1.20. Camí que segueixen els paquets a IPTables



Pas a pas

El camí que segueix un paquet a IPTables pot ser:

Entra per *mangle prerouting*. Generalment, aquesta cadena no inclou regles, per tant es passa a la cadena següent. La cadena *nat prerouting* realitza la traducció d'adreces de xarxa de destinació.

El paquet arriba a *routing* i es classifiquen els paquets segons quina sigui la seva destinació: si és el tallafoc, el paquet anirà a *filter input,* però si no, el paquet anirà a *filter forward*. La cadena *filter forward* s'encarrega de processar els paquets que es reenvien entre xarxes. Els paquets que han anat per aquest camí arriben a *mangle postrouting*, que és una cadena amb la capacitat de modificar els paquets abans que aquests abandonin el tallafoc i, a continuació, arriben a *nat postrouting*. *nat postrouting* s'encarrega de traduir les adreces de xarxa i emmascarament. A partir d'aquí el paquet surt cap a la xarxa de destinació.

La cadena *filter input* s'encarrega de processar els paquets que estan destinats al tallafoc. És aquí on es determina si el paquet ha de ser bloquejat o no. Si no es bloqueja, pot rebre un procés local (*Local Processing of Data*) i a continuació ser encaminat cap al *mangle output*, on el paquet es modificarà si és necessari. Després de passar per *mangle output*, el paquet arriba a *filter output*, on serà processat i enviat al tallafoc.

En IPTables els tres tipus de regla de filtratge són **entrada** (*input*), **sortida** (*output*) o **reenviament** (*forward*).

Una característica de les IPTables és que permeten aplicar regles de NAT. Les regles de NAT s'utilitzen per adreçar ports o realitzar canvis en l'IP d'origen o de destinació.

IPTables funciona seguint els passos següents:

1. Es carreguen els mòduls necessaris.
2. S'estableix algun bit.
3. Esborra totes les regles actuals.
4. Estableix les polítiques per defecte per l'acceptació, reenviament i sortida.
5. Per acabar aplica totes les regles del tallafoc.

Un exemple de regla en IPTables on es permeti a qualsevol adreça que entri per la interfície *np0s1* l'accés al port 80 seria:

```
1 iptables –A INPUT –i enp0s3 –s 0.0.0.0/0 –p TCP –dport www –j ACCEPT
```

Si s'analitza la línia anterior:

- `iptables`: nom de l'ordre.
- `-A`: s'utilitza per afegir (*append*) la regla.
- `INPUT`: estat del paquet, que en aquest cas és un paquet d'entrada (*input*).
- `-i np0s1`: interfície de xarxa, que en aquest cas és *enp0s3*.
- `-s 0.0.0.0/0/0:` adreça d'accés, que en aquest cas indica qualsevol adreça d'accés.
- `-p TCP`: tipus de port, que en aquest cas és TCP.
- `-dport`: port de destinació.
- `-j ACCEPT`: què es farà amb el paquet, en aquest cas s'acceptarà.

Per exemple, per no permetre enviar res al tallafoc o el trànsit intern i permetre només el trànsit de sortida:

```
1 iptables –P INPUT DROP
2 iptables –P FORWARD DROP
3 iptables –P OUTPUT ACCEPT
```

Per permetre el trànsit entre la xarxa interna *np0s3* i la xarxa externa *enp0s3*:

```
1 iptables –A FORWARD –i enp0s3 –o enp0s1 –j ACCEPT
```

Per permetre el trànsit entre connexions establertes amb origen a la xarxa *enp0s1* i destinació a la xarxa *enp0s3*:

```
iptables -A FORWARD -i enp0s1 -o enp0s3 -m state --state ESTABLISHED,RELATED -j
     ACCEPT
```

Per permetre l'entrada de paquets al tallafoc i que tinguin com a origen la xarxa interna i interfícies locals:

```
iptables -A INPUT -i enp0s1 -s 0/0 -d 0/0 -j ACCEPT
iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
```

Per no permetre l'entrada per la interfície *enp0s1* a màquines de l'exterior de la nostra xarxa que hagin piratejat adreces de xarxa de la nostra xarxa interna (192.168.0.0/24):

```
iptables -A INPUT -i enp0s1 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i enp0s1 -s 127.0.0.0/8 -j DROP
```

Per acceptar el trànsit de SYN que utilitza el protocol SMTP, l'accés web, l'accés web segur i SSH:

```
iptables -A INPUT -p tcp -s 0/0 -d x.y.z.m/32 --destination-port 25 --syn -j
    ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT
```

Si es disposa d'un servidor DHCP caldrà permetre el seu trànsit amb:

```
iptables -A INPUT -i enp0s1 -p tcp --sport 68 --dport 67 -j ACCEPT
iptables -A INPUT -i enp0s1 -p udp --sport 68 --dport 67 -j ACCEPT
```

Per no permetre cap sol·licitud a ports UDP o TCP:

```
iptables -A INPUT -s 0/0 -d 0/0 -p udp -j DROP
iptables -A INPUT -s 0/0 -d 0/0 -p tcp --syn -j DROP
```

Filtratge amb NFTables

Amb l'aparició d'IPv6 es va crear ip6tables, del qual podem dir que és una adaptació d'IPTables per a IPv6. L'any 2014 apareix NFTables, un nou entorn (*framework*) per a filtrar paquets basat també, com IPTables, en NetFilter. Un dels problemes d'IPTables és la forma complicada d'expressar les regles; per aquest motiu, la sintàxi d'NFTables és més curta i fàcil d'entendre. Per exemple, en lloc de "-p tcp", es posa "tcp", de forma similar a la sintàxi de *tcpdump*.

Podeu ampliar el filtratge amb nftables a: bit.ly/2TVdv5U.

Actualment, el tallafoc IPTables va essent substituït a les instal·lacions pel tallafoc NFTables i aquest procés continua el 2020.

Podem eliminar el tràfic de la xarxa amb la següent regla:

```
nft add rule filter input reject
```

Si no especifiquem cap motiu, s'envia un paquet ICMP que indica "port inaccessible". Podem especificar el motiu pel qual refusem el paquet, per exemple, amb `with icmp type host-unreachable`:

```
nft add rule filter input reject with icmp type host-unreachable
```

Es poden especificar els següents motius:

- **net-unreachable**: Xarxa de destí inaccessible.
- **host-unreachable**: Host inaccessible.
- **prot-unreachable**: Protocol de destí inaccessible.
- **port-unreachable**: Port de destí inaccessible.
- **net-prohibited**: Xarxa prohibida administrativament.
- **host-prohibited**: Host prohibit administrativament.
- **admin-prohibited**: Comunicació prohibida administrativament.

Pel tràfic IPv6 utilitzarem icmpv6, de la següent forma:

```
nft add rule ip6 filter input reject with icmpv6 type no-route
```

Els motius possibles per refusar les conexions en IPv6 són:

- **no-route**: No hi ha ruta al destí.
- **admin-prohibited**: Comunicació prohibida administrativament.
- **addr-unreachable**: Direcció inaccessible.
- **port-unreachable**: Port inaccessible.

Per refusar tant el tràfic IPv4 com el tràfic IPv6 amb una única regla, podem usar la familia **inet** amb una abstracció anomenada **icmpx**. A continuació hi ha un exemple:

```
nft add rule inet filter input reject with icmpx type no-route
```

La regla anterior refusa el tràfic IPv6 amb el motiu "no route" i el tràfic IPv4 amb el motiu "net unreachable". Això és així perquè existeix un mapatge entre els motius de tots dos protocols.

Un exemple d'ordre seria la següent, que guarda el *log* i permet la sortida dels paquets *tcp* amb el port destí 22, que utilitza ssh. Observeu com nftables permet realitzar dues accions en una mateixa regla, en aquest cas fer el log i acceptar el paquet. Amb iptables necessitaríem dues regles per fer el mateix. Cal tenir present, també, que la regla s'avalua d'esquerra a dreta:

```
nft add rule output tcp dport 22 log accept
```

També podem posar un missatge de log:

```
nft add rule filter input tcp dport 22 ct state new log prefix \"Nova connexió
    SSH : \" accept
```

Podem instal·lar NFTables amb: `sudo apt install nftables`

Podem usar ordres NFTables que no facin els canvis permanents o escriure-les en un fitxer, que s'anomena */etc/nftables.conf*, perquè els canvis passin a ser permanents.

Ordres NFTables

Es poden definir interfícies amb: `nft define nomInterfície=interficie`.

També es poden afegir taules amb: `sudo nft add table <familia> <nomTaula>`.

Les *taules* són contenidors de cadenes. El seu nom no té cap significat predefinit. Les *cadenes* són contenidors de regles.

La *família* és opcional; és un concepte que apareix amb nftables i que indica el tipus de tràfic amb el qual treballem. S'admeten les següents famílies: ip, arp, ip6, bridge, inet i netdev.

La **família ip** treballa amb paquets IPv4.

La **família ip6** treballa amb paquets IPv6.

La **família inet** treballa amb paquets IPv4 i IPv6.

La **família arp** treballa amb paquets arp, i ja no fa falta usar una altra ordre a part com era arptables.

La **família bridge** treballa amb paquets que passen per un switch.

La **família netdev** permet classificar els paquets i permet veure tot el tràfic de xarxa. Aquesta funcionalitat aparèix amb nftables al nucli 4.2 de Linux.

Aquesta última família és ideal per eliminar els paquets que provenen d'atacs DDOS, ja que així els eliminem com més aviat millor. L'eliminació dels paquets des de aquí és el doble d'eficient que fer-ho desde la cadena de prerouting d'iptables.

També podem usar aquesta nova família per fer balanceig de càrrega.

Es poden veure les diferents taules existents amb: `sudo nft list tables`.

Es poden eliminar les taules amb: `sudo nft delete table nomTaula`.

Per exemple, es poden crear les típiques taules *filter* per filtrar i *nat* per canviar les adreces IP.

A cada taula es poden crear cadenes com, per exemple, la cadena *prerouting* i la cadena *postrouting* amb: `sudo nft add chain nomTaula nomCadena`.

Les cadenes s'esborren amb: `nft delete chain <família> <tabla> <cadena>`. En aquesta instrucció, la família és opcional.

Cal tenir present, però, que només poden esobrrar-se cadenes buides, és a dir, sense cap regla. Pot buidar-se una cadena amb la instrucció `nft flush chain <família> <tabla> <cadena>`. Novament, la família és opcional.

Podem crear regles amb la instrucció:

```
1 nft add rule <família> <taula> <cadena> position <posició> <identificador> <
      coincidències> <acció>
```

On:

- `position <posició>` i `<familia>` són opcionals.
- La posició indica el *handle* d'una regla ja existent. Aquest és un número intern que identifica les regles d'una cadena.

Si s'indica la posició, la nova regla s'afegirà a continuació de la regla identificada pel *handle*. Si s'omet la posició, la regla s'afegeix al final. Es pot conèixer el *handle* d'una regla amb la instrucció `nft list <taula> filter -n -a`. L'opció `-a` és per demanar que es mostri el *handle* de cada regla i, per tant, al nostre cas, tot i que sintàcticament és opcional, cal posar-la. L'opció `-n` també és opcional i indica que no s'han de realitzar resolucions DNS. És recomanable posar-la per eficiència.

Pot substituir-se `add` per `insert`. En aquest cas, la regla es posaria abans de la regla amb el *handle* indicat per la posició. En cas que no s'indiqués cap posició, es posaria a l'inici de la llista. Després de les *coincidències* venen les declaracions de les accions que executa la regla quan es detecta alguna d'aquestes coincidències. Algunes de les accions que pot executar la regla són: accept, drop, queue, continue, return, jump i goto.

- **accept**: Accepta el paquet i deixa d'avaluar les regles restants.
- **drop**: Elimina el paquet i deixa d'avaluar les regles restants.
- **queue**: Encua el paquet a l'espai d'usuari i deixa d'avaluar les regles restants.
- **continue**: Continua l'avaluació de les regles amb la següent regla de la cadena.
- **return**: Torna de la cadena actual i continua a la següent regla de la darrera cadena. En una cadena base, és equivalent a acceptar.
- **jump <chain>**: Continua a la primera regla de la cadena <chain>.
- **goto <chain>**: Similar a jump, però, després de l'avaluació de la nova cadena, l'avaluació continuarà a la darrera cadena en lloc de fer-ho a la cadena on hi ha la sentència *goto*.

Pel que fa a les *coincidències* o *matches*, hi ha moltes expressions disponibles per a especificar-les, però majoritàriament coincideixen amb les d'iptables. La principal diferència és que no hi ha coincidències genèriques (és a dir, vàlides per a tots els protocols) o implícites (és a dir, referides al protocol indicat amb l'opció corresponent que, al cas de les *iptables*, és *-p* o *–protocol*).

Les *coincidències* s'utilitzen per accedir a certa informació dels paquets i crear filtres segons aquesta informació. Hi ha moltes coincidències previstes.

A continuació teniu una llista no exhaustiva de les coincidències disponibles:

Podeu ampliar la informació de les coincidències a: bit.ly/3cKVVue

- meta (meta propietats, per exemple interfícies)
- icmp (protocol ICMP)
- icmpv6 (protocol ICMPv6)
- ip (protocol IP)
- ip6 (protocol IPv6)
- tcp (protocol TCP)
- udp (protocol UDP)
- sctp (protocol SCTP)
- ct (seguiment de la connexió)

Aquestes coincidències poden tenir diferents arguments. Tot seguit presentem alguns d'aquests arguments:

- meta:
  - oif <índex de la interfície de sortida>
  - iif <índex de la interfície d'entrada>
  - oifname <nom de la interfície de sortida>
  - iifname <nom de la interfície d'entrada>

(*oif* i *iif* accepten arguments de cadena i es converteixen llavors en índex d'interfícies.*oifname* i *iifname* son més dinàmics, però més lents per la coincidència de cadenes)

- icmp:
  - type <tipus icmp>
- icmpv6:
  - type <tipus icmpv6>
- ip:

    - protocol <protocol>
    - daddr <adreça de destí>
    - saddr <adreça d'origen>
- ip6:
    - daddr <adreça de destí>
    - saddr <adreça d'origen>
- tcp:
    - dport <port de destí>
    - sport <port d'origen>
- udp:
    - dport <port de destí>
    - sport <port d'origen>
- sctp:
    - dport <port de destí>
    - sport <port d'origen>
- ct:
    - state <new | established | related | invalid>

Alguns exemples són:

- Acceptem el tràfic *related* (relacionat) i el tràfic *established* (establert):

```
nft add rule inet filter input ct state related,established accept
```

- Posem la politica de descartar el tràfic invàlid:

```
nft add rule inet filter input ct state invalid drop
```

- Acceptem paquets del protocol icmp (és el que utilitza l'ordre *ping*):

```
nft add rule inet filter input ip protocol icmp icmp type echo-request ct state
    new accept
```

- Acceptem el tràfic de la interfície local:

```
nft add rule inet filter input iif lo accept
```

- Acceptem el tràfic SSH pel port 22:

```
nft add rule inet filter TCP tcp dport 22 accept
```

- Refusem el tràfic no procesat per les altres regles. A la primer regla no posem cap motiu. A les altres dues posem, respectivament, els motius `tcp reset` i `prot-unreachable`:

```
nft add rule inet filter input ip protocol udp reject
 nft add rule inet filter input ip protocol tcp reject with tcp reset
 nft add rule inet filter input counter reject with icmp type prot_unreachable
```

`nft` no utilitza */etc/services* per fer coincidir els números dels ports amb els noms, sinó que utilitza una llista interna. Per veure les assignacions de ports desde la línia d'ordres podem usar:

```
nft describe tcp dport
```

Pot esborrar-se una regla d'una cadena amb `nft delete rule <taula> <cadena> handle <handle>`.

Especificació de sets, interfícies i protocols. Canvis permanents a les regles

Un ***set*** és una col·lecció o conjunt d'elements que pot contenir adreces IP o ports. El nom d'un *set* pot tenir fins a 15 caràcters.

Existeixen sets anònims, que s'utilitzen directament a les regles (com per exemple: `dport {22, 80, 443}`) i sets amb nom, que primer es defineixen i després s'utilitzen a les regles.

Es poden crear sets amb nom creant en primer lloc la taula on el posarem, que podem anomenar *filter*, i, a continuació, el set:

```
nft add table ip filter
nft add set ip filter enemic { type ipv4_addr\;}
```

On *enemic* és el nom del set i `type` indica el tipus de dada del set, en aquest cas una adreça IPv4.

També es poden afegir elements al set:

```
nft add element ip filter enemic { 192.168.3.4 }
nft add element ip filter enemic { 192.168.1.4, 192.168.1.5 }
```

Aleshores podem posar el set amb nom a la regla:

```
nft add rule ip filter input ip saddr @enemic drop
```

Especificacions dels sets amb nom:

- type: és obligatori i determina el tipus de dada del set. Els tipus de dades suportats són:

  - ipv4_addr: adreça IPv4.
  - ipv6_addr: adreça IPv6.
  - ether_addr: adreça Ethernet.
  - inet_proto: qualsevol protocol d'Internet.
- inet_service: servei d'Internet (per exemple, `read tcp port`).
- mark: tipus de marca.
- ifname: nom de la interfície de xarxa (enp0s3, enp0s1..).
- timeout: determina el temps que l'element és al set. La cadena de caràcters ha de ser del format: "v1dv2hv3mv4s" on v1 és el dia, v2 l'hora, v3 els minuts i v4 els segons. Per exemple podem, crear un set anomenat *ports*, els elements del qual s'eliminaran després de 3 hores i 45 segons:

```
1 nft add set ip filter ports {type inet_service \; timeout 3h45s \;}
```

- flags: els flags poden separar-se amb comes, com es veu a l'exemple del final. Hi ha els següents flags:
  - constant: no es pot canviar el contingut del set, és constant.
  - interval: el set conté intervals.
  - timeout: els elements es poden afegir amb un timeout assignat.

```
1 nft add set ip filter flags_set {type ipv4_addr\; flags constant, interval\;}
```

- gc-interval: és l'interval del recol·lector d'escombreries; només es pot usar si el timeout o els flags del timeout s'han activat. L'interval segueix el mateix format anterior "v1dv2hv3mv4s".
- elements: serveixen per afegir elements al set. L'ordre següent crea un set anomenat *daddrs* amb els elements 192.168.1.1, què hi serà 10 segons, i 192.168.1.2, què hi serà 30 segons:

```
1 nft add set ip filter daddrs {type ipv4_addr \; flags timeout \; elements
    ={192.168.1.1 timeout 10s, 192.168.1.2 timeout 30s} \;}
```

- size: nombre màxim d'elements del set. Per exemple, podem crear un set amb un màxim de 2 elements de la següent forma:

```
1 nft add set ip filter saddrs {type ipv4_addr \; size 2 \;}
```

- policy: determina la política de selecció del set. Els valors disponibles son: `performance` (és el valor per defecte) i `memory`.

Finalment, podem llistar els sets amb nom amb `list`:

```
nft list set ip filter elMeuSet
nft list set ip filter saddrs
```

Una altra característica és la possibilitat de definir els **diccionaris**. La seva estructura és la d'un *set* que, a més, pot tenir veredictes; per això s'anomenen també *mapes amb veredicte*. Un veredicte és una instrucció com les que s'especifiquen dins de les regles. Si s'hi posa més d'un veredicte en el mateix element del diccionari, aquests elements es separen amb comes.

Els mapes amb veredicte són una de les funcionalitats més potents de nftables. Els mapes amb veredicte permeten lligar una acció a un element.

A continuació teniu com a exemple la creació d'un diccionari anònim (o literal) que s'utilitza directament a les regles (igual que succeeix amb els *sets* anònims). Aquest diccionari estableix que, segons el protocol, s'executi una acció o una altra. En aquest cas incrementar diferents comptadors. El primer que es fa, però, és crear les taules i cadenes que ens fan falta, en aquest cas la taula *filter* amb la cadena *input*:

```
nft add table filter
nft add chain ip filter input
nft add rule ip filter udp_chain counter
nft add rule ip filter tcp_chain counter
nft add rule ip filter icmp_chain counter
nft add rule ip filter input ip protocol vmap { tcp : jump tcp_chain, udp :
    jump udp_chain , icmp : jump icmp_chain }
```

El següent codi és el resultat d'executar `nft list table filter` després de les ordres anteriors. Aquest resultat pot posar-se en un fitxer de configuració per fer que les regles siguin permanents:

```
table ip filter {
        chain input {
                type filter hook input priority 0;
                ip protocol vmap { udp : jump udp_chain, tcp : jump tcp_chain,
                     icmp : jump icmp_chain}
        }

        chain tcp_chain {
                counter packets 0 bytes 0
        }

        chain udp_chain {
                counter packets 0 bytes 0
        }

        chain icmp_chain {
                counter packets 0 bytes 0
        }
}
```

Podem declarar diccionaris amb nom de la següent forma:

```
nft add map filter diccionari { type ipv4_addr : verdict\; }
```

Un cop creat, hi podem afegir elements:

```
nft add element filter diccionari { 192.168.0.10 : drop, 192.168.0.11 : accept
    }
```

Tot seguit teniu un altre exemple on, segons la ip de destí, s'executaran unes accions o unes altres; per exemple pels paquets de la ip 192.168.1.1 a la 192.168.1.10, es produeix un salt per executar les accions de la cadena *chain-dmz*:

```
nft add rule ip Firewall Forward ip daddr vmap {\
      192.168.1.1-192.168.1.10 : jump chain-dmz, \
      192.168.2.1-192.168.2.99 : jump chain-ssn1, \
      192.168.2.100-192.168.2.199 : jump chain:ssn2, \
      192.168.3.1-192.168.3.50 : jump chain-desktops \
}
```

El fet que es puguin especificar les interfícies d'entrada i sortida amb `meta`, seguit d'`iifname <Interfície d'entrada>` o `oifname <Interfície de sortida>`, es pot utilitzar per acceptar o denegar el tràfic que tenim en una interfície determinada. En el següent exemple, s'accepta el tràfic de la interfície local de loopback, posant després de la interfície de sortida oifname el nom d'aquesta:

```
nft add rule filter input meta oifname lo accept
```

Els *meta selectors* permeten fer coincidències amb la metainformació dels paquets i, en alguns casos, modificar-la.

Tenim dos tipus de meta selectors: qualificats i no qualificats. Els qualificats obliguen a què usem la paraula reservada *meta* i els no qualificats no.

Entre els qualificats hi trobem *length*, la longitud del paquet, i el protocol. Entre els no qualificats, *mark*, marques dels paquets, *time*, *day* i *hour* (el dia i l'hora).

Teniu informació dels meta selectors a: bit.ly/3aJ9okw

Els protocols que es poden utilitzar són: `udp`, `tcp`, `ip` i `icmp`. Podem posar, després del protocol, el port origen (*sport*) o el port destí (*dport*), el número d'aquest port i l'acció a realitzar: `<protocol> <dport/sport><número de port><acció>`.

Per exemple:

```
tcp dport{dns,http, ntp, https} accept
```

Podem crear el fitxer */etc/nftables.conf* i carregar-lo amb: `sudo nft -f nftables.conf`. Vegeu-ne un exemple:

```
table inet filter {
        chain web {
                ip daddr 83.247.151.178 drop
        }

        chain preruting {
        }

        chain output {
                type filter hook output priority 0; policy accept;
                ip daddr 8.8.8.8 counter packets 0 bytes 0
                ip daddr 83.247.151.178 counter packets 0 bytes 0
```

```
        }

        chain input {
                type filter hook input priority 0; policy accept;
                ip daddr 172.217.168.0/24 drop
        }
}
```

Podem filtrar el tràfic per protocol o comptar els paquets que enviem o rebem dels diferents protocols de xarxa. Podem crear taules per a cada protocol i acció a realitzar, podent crear així la taula ip filter amb les cadenes input i output amb les accions corresponents a realitzar.

A continuació enteniu un exemple:

```
table ip filter{

     chain output{
     ip daddr 192.168.0.3 drop
     ip saddr 127.0.0.6 drop
     ip saddr 127.0.0.2 ip daddr 127.0.0.8 drop
     tcp dport 22 counter packets 0 bytes 0
  }

}
```

1.4.5 Proves de funcionament. Sondeig

Per poder assegurar que el tallafoc realitza les tasques per a les quals ha estat dissenyat s'han de realitzar proves. Hi ha una sèrie d'eines i tècniques que ajuden a realitzar aquestes proves de manera ràpida i eficient.

Nmap

L'`nmap` és una eina molt popular en el món de l'administració de les xarxes. Temuda per molts (injustament) i molt apreciada pels tècnics, aquesta eina escaneja màquines i identifica els serveis assignats als ports.

L'ús d'`nmap` és vist per alguns tècnics com una amenaça. Identifica una part molt sensible de la configuració d'una màquina, la qual cosa fa saltar moltes alarmes. Com a administradors d'un tallafoc i responsables de la seguretat de la xarxa hem de detectar si algú realitza un escaneig a màquines de la nostra xarxa i s'ha d'identificar l'origen de l'escaneig, ja que possiblement s'estigui realitzant aquesta acció amb l'objectiu de trobar forats de seguretat. Aquest és un dels motius pels quals hem de dominar aquesta eina, ja que també és útil per trobar forats de seguretat en la nostra xarxa informàtica. Per no tenir ensurts no s'ha de realitzar un `nmap` en una xarxa que no sigui la pròpia o sobre la qual no tinguem permís, ja que segons la legislació d'alguns països podeu estar realitzant una acció il·legal.

En l'exemple següent es pot veure un escaneig molt simple a una màquina amb l'adreça de xarxa 192.168.7.52:

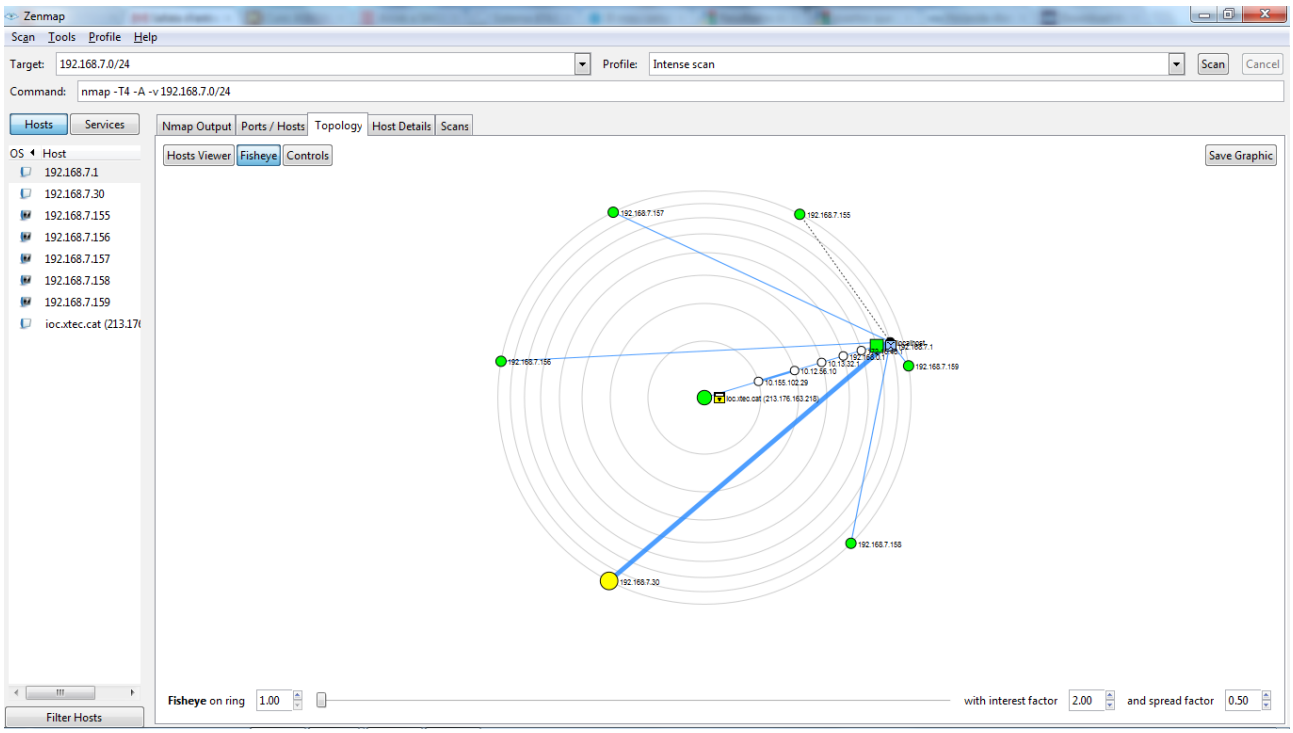
```
Nmap scan report for 192.168.7.52
Host is up (0.00039s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC address: 1C:C1:DE:**:**:** (Unknow)
```

La primera columna indica el número de port i el protocol carregat. La segona indica l'estat del port i la tercera indica el servei activat.

Els ports poden estar oberts (*open*), tancats (*closed*) o filtrats (*filtered*). Un port filtrat pot acceptar o no trànsit depenent les característiques del paquet.

La figura 1.21 mostra l'aspecte de l'eina Zenmap. Aquest programa treballa amb `nmap` per obtenir dades, però ofereix una interfície gràfica molt còmoda per a l'usuari.

FIGURA 1.21. Pantalla de l'aplicació Zenmap



Eines TCP/IP

Existeix una sèrie d'eines bàsiques per resoldre problemes de xarxa relacionats amb TCP/IP i que, alhora, poden resultar útils durant el procés de prova d'un tallafoc. A continuació és descriuen breument:

- `ip`: IP vol dir Internet Protocol. Aquesta ordre és usada per a mostrar o manipular dispositius, l'enrutament i túnels. És similar a l'ordre *ifconfig*,

però té més funcionalitats, ja que, a més de substituir *ifconfig*, substitueix també les ordres *route* i *arp*, aportant també noves funcionalitats. Així, es pot executar: `ip route` per veure l'enrutament dels paquets, `ip monitor` per monitoritzar l'estat dels dispositius i l'encaminament. Podem posar en funcionament interfícies de xarxa amb: `ip link set enp3s0 up`.

- `ifconfig`: actualitza i mostra la configuració de xarxa. La figura 1.22 mostra la sortida d'aquesta ordre. Com es pot observar, el resultat per defecte presenta més informació, a part de l'adreça de xarxa: també l'adreça MAC, l'adreça de difusió (*broadcast*), la màscara de xarxa o la quantitat de trànsit que ha circulat per la xarxa. Des del 2001 ja no té suport i ha estat substituit per l'eina *ip*.

FIGURA 1.22. Exemple d'execució de l'ordre ifconfig

```
jordi@ubuntu:~$ ifconfig
eth11     Link encap:Ethernet  HWaddr 00:23:24:0e:22:85
          inet addr:192.168.20.2  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::223:24ff:fe0e:2285/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33722 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24603 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40301552 (40.3 MB)  TX bytes:4304298 (4.3 MB)
          Interrupt:19 Memory:f0500000-f0520000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)

jordi@ubuntu:~$
```

- `route`: configura i mostra l'estat de la taula d'encaminament d'una màquina. En la figura 1.23 es mostra un cas molt senzill de configuració d'un equip client.

FIGURA 1.23. Exemple d'execució de l'ordre route

```
jordi@ubuntu:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.20.0    *               255.255.255.0   U     1      0        0 eth11
link-local      *               255.255.0.0     U     1000   0        0 eth11
default         192.168.20.1    0.0.0.0         UG    0      0        0 eth11
jordi@ubuntu:~$
```

- `traceroute`: determina la connectivitat amb una màquina remota indicant les màquines que troba pel camí. En màquines amb sistema operatiu Windows l'ordre equivalent és tracert, i el resultat de la seva execució es pot observar en la figura 1.24.

Figura 1.24. Exemple d'execució de l'ordre tracert

```
C:\Users\     >tracert www.google.com

Traza a la dirección www.l.google.com [173.194.69.147]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2    <1 ms    <1 ms    <1 ms  172.16.40.1
  3    <1 ms    <1 ms    <1 ms  192.168.0.1
  4     2 ms     1 ms     1 ms  10.13.32.1
  5     1 ms     1 ms     1 ms  10.12.56.10
  6   236 ms    10 ms     3 ms  10.155.102.29
  7     2 ms     2 ms     2 ms  83.247.145.9
  8     3 ms     2 ms     2 ms  83.247.145.1
  9     3 ms     3 ms     3 ms  213.192.249.158
 10     3 ms     2 ms     2 ms  gencat-0-0-0-11-core3-bap.bt-igs.net [213.192.24
9.157]
 11    15 ms    15 ms    15 ms  xe-0-0-2-core2-espanix.bt-igs.net [212.80.160.97
]
 12    34 ms    15 ms    15 ms  xe-0-0-0-23.core1-espanix.bt-igs.net [212.80.160
.241]
 13    33 ms    15 ms    15 ms  xe-0-0-0-20.core2-espanix.bt-igs.net [212.80.160
.254]
 14    16 ms    16 ms    16 ms  193.149.1.94
 15    16 ms    16 ms    16 ms  216.239.49.196
 16    43 ms    72 ms    36 ms  209.85.240.191
 17    93 ms    80 ms    45 ms  72.14.235.16
 18    50 ms    50 ms    50 ms  209.85.242.187
 19    56 ms    56 ms    56 ms  209.85.240.88
 20    56 ms    56 ms    56 ms  64.233.174.55
 21     *        *        *     Tiempo de espera agotado para esta solicitud.
 22    56 ms    56 ms    56 ms  bk-in-f147.1e100.net [173.194.69.147]

Traza completa.

C:\Users\     >_
```

- `host`: permet realitzar cerques DNS directes i indirectes. En la figura 1.25 es relaciona el domini ioc.xtec.cat amb l'adreça IP 213.176.163.218.

Figura 1.25. Exemple d'execució de l'ordre host

```
jordi@ubuntu:~$ host ioc.xtec.cat
ioc.xtec.cat has address 213.176.163.218
jordi@ubuntu:~$
```

- `dig`: permet realitzar cerques DNS directes i indirectes aportant més informació que l'ordre host. La figura 1.26 mostra el resultat de fer la consulta de dig sobre el domini ioc.xtec.cat i, com es pot veure, el resultat és bastant més complet que el que ofereix host.

Figura 1.26. Exemple d'execució de l'ordre dig

```
jordi@ubuntu:~$ dig ioc.xtec.cat

; <<>> DiG 9.7.3 <<>> ioc.xtec.cat
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 8, ADDITIONAL: 0

;; QUESTION SECTION:
;ioc.xtec.cat.                  IN      A

;; ANSWER SECTION:
ioc.xtec.cat.           523     IN      A       213.176.163.218

;; AUTHORITY SECTION:
cat.                    157764  IN      NS      b.nic.ch.
cat.                    157764  IN      NS      sns-pb.isc.org.
cat.                    157764  IN      NS      cat.pch.net.
cat.                    157764  IN      NS      nsc.nic.de.
cat.                    157764  IN      NS      ns.nic.cat.
cat.                    157764  IN      NS      dns4.ad.
cat.                    157764  IN      NS      anyc1.irondns.net.
cat.                    157764  IN      NS      ns1.nic.es.

;; Query time: 0 msec
;; SERVER: 172.16.40.1#53(172.16.40.1)
;; WHEN: Thu Jun 14 15:17:30 2012
;; MSG SIZE  rcvd: 239

jordi@ubuntu:~$
```

- `tcpdump`: permet veure paquets que arriben a una interfície de xarxa. La sortida d'aquesta ordre és bastant difícil de llegir, tal com es mostra en la figura 1.27.

FIGURA 1.27. Exemple d'execució de l'ordre tcpdump

```
jordi@ubuntu:~$ sudo tcpdump -v
tcpdump: listening on usbmon1, link-type USB_LINUX_MMAPPED (USB with padded Linux header), capture size 65535 bytes
15:22:13.379562 CONTROL SUBMIT to 1:1:0
15:22:13.379564 CONTROL COMPLETE from 1:1:0
15:22:16.127394 INTERRUPT COMPLETE to 1:1:1
```

- IPTraf: permet mesurar el trànsit que circula per una interfície. Treballar amb IPTraf és una opció molt bona a `tcpdump`. Com es pot veure en la figura 1.28, la interfície d'IPTraf presenta les dades de manera clara i entenedora.

FIGURA 1.28. Exemple d'execució de l'ordre IPTraf

IPTraf

Iface	Total	IP	NonIP	BadIP	Activity
lo	188	188	0	0	2,60 kbits/sec
eth11	86939	86939	0	0	60993,20 kbits/sec

1.4.6 Registres d'esdeveniments d'un tallafoc

Treballar amb tallafoc no tindria gaire sentit si no es pogués consultar a posteriori la informació que aquest ha generat. És impossible estar vint-i-quatre hores davant d'un monitor amb la mirada atenta esperant que es produeixi un esdeveniment per actuar. Els tallafocs han de poder emmagatzemar informació rellevant per després poder-la analitzar i prendre les mesures que calgui.

Els diferents tallafocs emmagatzemen els esdeveniments que succeeixen a la xarxa seguint determinades tècniques.

1.4.7 Registre d'esdeveniments amb IPTables

El tallafoc IPTables registra missatges d'esdeveniments amb Syslog. Syslog és un estàndard que s'empra per l'enviament de missatges de registre a les xarxes informàtiques. En una distribució Linux, el nucli captura, mitjançant el dimoni klogd, els esdeveniments atípics que es produeixen i els emmagatzema. El fitxer de configuració syslog.conf, ubicat en el directori */etc*, s'utilitza per indicar el directori de destinació dels missatges de registre generats per IPTables.

Per tal d'emmagatzemar missatges de registre en un directori, s'ha d'afegir al fitxer */etc/syslog.conf* la línia següent:

```
1 kern.=debug/var/log/iptables.log
```

Perquè els canvis tinguin efecte cal reiniciar el dimoni.

1.4.8 Registre d'esdeveniments amb NFTables

Podem activar el registre de missatges amb la següent ordre, que registra tots els paquets de sortida cap al socket NFLOG:

```
1 nft add rule filter output log
```

També podem comptar quants paquets i bytes s'han rebut o s'han enviat a determinades adreces IP posant al fitxer */etc/nftables.conf* les paraules **counter packets 0 bytes 0**, tal i com es pot veure a la figura figura 1.29.

FIGURA 1.29. Comptar paquets

```
table inet filter {
        chain web {
                ip daddr 83.247.151.178 drop
        }

        chain preruting {
        }

        chain output {
                type filter hook output priority 0; policy accept;
                ip daddr 8.8.8.8 counter packets 0 bytes 0
                ip daddr 83.247.151.178 counter packets 0 bytes 0
        }

        chain input {
                type filter hook input priority 0; policy accept;
                ip daddr 172.217.168.0/24 drop
        }
}
```

1.4.9 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 del 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 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.

1.4.10 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 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 i 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, pot tractar-se d'un intent de denegació de servei o bé que s'hi hagi 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 accedir-hi repetidament. Algun d'aquests intents pot generar l'error 404 (*not found*: no trobat), que queda registrat en els *logs* del servidor web. Si els errors 404 es comproven periòdicament, és possible tenir una idea del tipus d'atacs que pateix el servidor.

1.5 Exemples de tallafoc

A Internet es poden trobar molts exemples de tallafocs gratuïts. Alguns d'aquests tallafocs, però, són més representatius i, en alguns casos, són fins i tot utilitzats per explicar diversos aspectes teòrics del món de les xarxes. Així, es podria iniciar l'estudi amb l'antic IPChains, que es pot utilitzar actualment en una segona línia de defensa, tot i que avui en dia és difícil de veure'l instal·lat. A continuació trobaríem l'IPTables, que és l'evolució natural de l'IPChains i, posteriorment, NFTables, l'evolució d'IPChains. A més, hi ha tot un seguit de tallafocs, que no són més que eines que utilitzen IPTables i NFTables, però que ofereixen major facilitat d'ús, fins i tot, en algun cas, amb interfícies gràfiques. També cal estudiar un equip bastió com a exemple curiós de màquina de xarxa amb un extra de seguretat.

1.5.1 IPChains

IPChains és un tallafoc obsolet que només s'utilitza en cassos molt concrets, generalment en la segona línia defensiva i en combinació amb altres tallafocs.

L'última revisió d'aquest programa es va realitzar l'any 2000 i s'incloïa a nuclis Linux anteriors al 2.4. Actualment es pot descarregar d'algunes pàgines d'eines de xarxa.

1.5.2 IPTables

El tallafoc IPTables és més complet que IPChains. És molt més precís, però també és més difícil d'utilitzar. Funciona carregant un mòdul del nucli i executant un guió o script. El guió segueix els passos següents:

1. Es carreguen els mòduls imprescindibles i auxiliars.
2. S'esborren les regles actuals.
3. S'estableixen les polítiques per defecte per acceptar, reenviar o sortida.
4. S'apliquen les regles.

Quan un paquet arriba al tallafoc és processat pel nucli. A partir d'aquí el paquet comença a recórrer etapes al nucli abans de ser enviat a la destinació adient, reenviat cap a un altre equip o bé se li aplica qualsevol altra operació.

Molts tallafocs utilitzen internament IPTables. Es tracta de programes amb una interfície prou entenedora que facilita molt el disseny de directives i la seva aplicació, modificació i manteniment.

1.5.3 NFTables

El tallafoc NFTables és el successor d'IPTables i inclou la gestió amb IPv6. Es va començar a desenvolupar desde zero al 2014 i es va integrar al *kernel* de Linux, a la branca 3.13. Debian es va decantar des del principi per NFTables i, per tant, també Ubuntu. Posteriorment ho va fer Red Hat. Les grans empreses usen actualment NFTables perquè té un rendiment millor. NFTables permet afegir amb una ordre diferents accions en una mateixa regla. Les ordres `ip6tables`, `ebtables` i `arptables`, s'integren totes a NFTables. Incorpora també una capa de compatibilitat amb IPTables per fer la transició més fàcil. NFTables té 3 components bàsics:

- Implementació del kernel
- Biblioteca de comunicació *libnl*
- Frontend per a l'usuari

1.5.4 Equip bastió

Quan un equip de la xarxa, generalment un servidor, esdevé un objectiu potencial d'atacs, requereix una protecció extra. Un equip bastió és una màquina a la qual

En la seva accepció original, un bastió és una fortificació que forma part d'un castell. La seva missió és protegir un espai crític de defensa en el cas de produir-se un atac.

se li afegeix més protecció tot i estar a la xarxa interna. Aquests equips estan especialment configurats per rebre atacs. Un exemple d'equip bastió podria ser un servidor intermediari. Els bastions poden ser *single-homed*, *dual-homed* i *multihomed*.

1.5.5 Uncomplicated Firewall (ufw)

El tallafoc ufw (Uncomplicated Firewall) permet configurar fàcilment les IPTables des de la línia d'ordres. Aquest programa està desenvolupat per Ubuntu en llenguatge Python.

La taula 1.5 mostra resumidament el funcionament d'aquest tallafoc.

TAULA 1.5. Exemples d'accions amb ufw

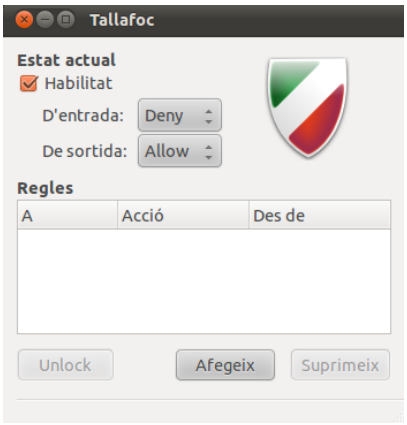
Funció	Ordre
Encendre el tallafoc	`sudo ufw enable`
Apagar el tallafoc	`sudo ufw disable`
Mostrar l'estat del tallafoc	`sudo ufw status`
Mostrar la llista de regles numerades	`sudo ufw status numered`
Bloquejar tot el trànsit d'entrada	`sudo ufw default deny incoming`
Permetre tot el trànsit d'entrada	`sudo ufw default allow incoming`
Bloquejar tot el trànsit de sortida	`sudo ufw default deny outgoing`
Permetre tot el trànsit de sortida	`sudo ufw default allow outgoing`
Bloquejar el port 22	`sudo ufw deny port 22`
Permetre el port 22	`sudo ufw allow port 22`
Bloquejar el port 22 a l'IP 192.168.0.15	`sudo ufw deny from 192.168.0.15 port 22`
Permetre el port 22 a l'IP 192.168.0.15	`sudo ufw allow from 192.168.0.15 port 22`
Bloquejar el port 22 a la xarxa 192.168.0.0	`sudo ufw deny from 192.168.0.0/24 port 22`
Permetre el port 22 a la xarxa 192.168.0.0	`sudo ufw allow from 192.168.0.0/24 port 22`
Bloquejar un rang de ports TCP	`sudo ufw deny 1025:3000/tcp`

1.5.6 Gufw

Gufw és una interfície gràfica desenvolupada per ufw. És una eina molt fàcil d'utilitzar i d'instal·lar. Apareix als repositoris oficials d'Ubuntu.

En la figura 1.30 es mostra la pantalla d'inici del tallafoc, en la qual es pot veure que està habilitat però que encara no contempla cap regla.

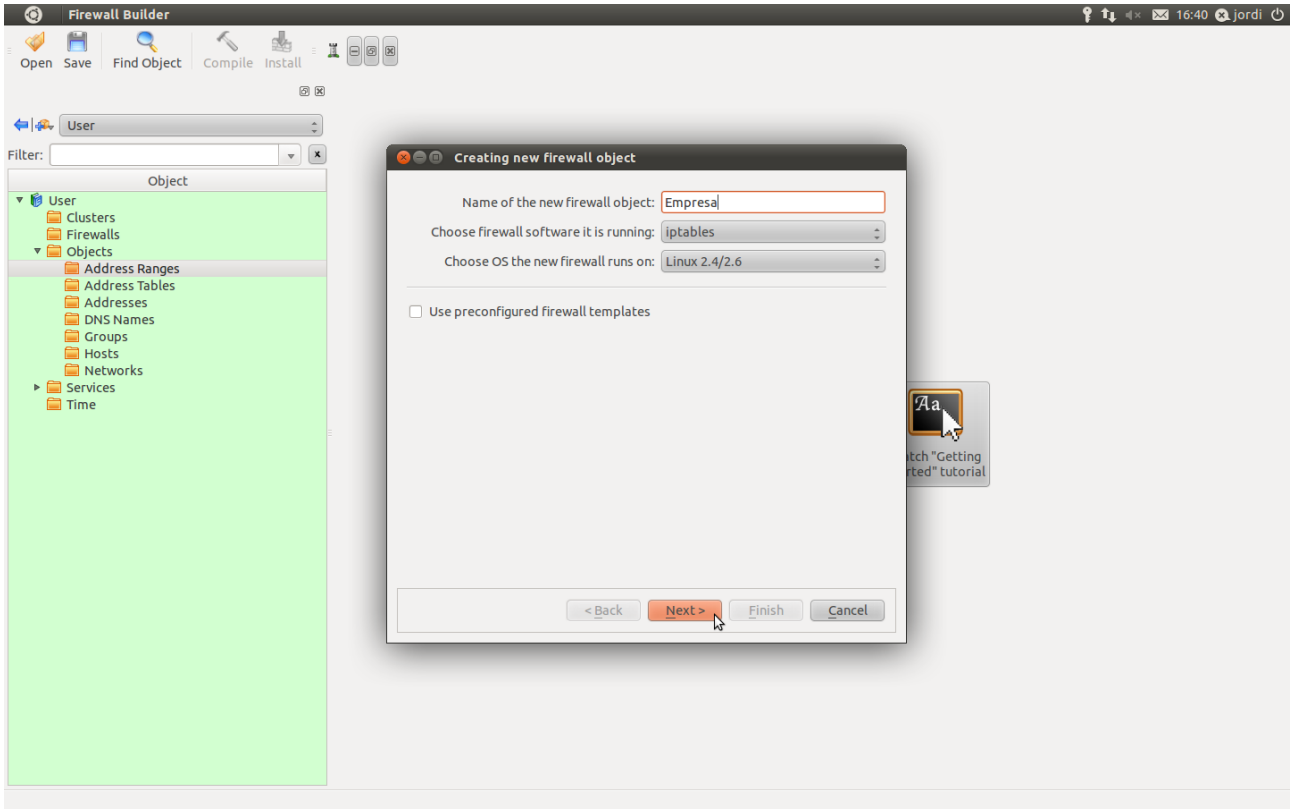
FIGURA 1.30. Pantalla principal de Gufw



1.5.7 Firewall Builder

El tallafoc Firewall Builder és un programa que ofereix una interfície gràfica per gestionar diferents plataformes de tallafocs. En la figura 1.31 es mostra la finestra inicial del procés de creació d'un tallafoc.

FIGURA 1.31. Pantalla de configuració d'un tallafoc amb Firewall Builder



Aquest programa està concebut per controlar diversos tallafocs des d'un únic centre de comandament. El fet que permeti controlar diversos tallafocs i que aquests puguin estar muntats amb IPTables, Cisco ASA and PIX, ipfilter BSD o HP ProCurve ACL el converteixen en un candidat òptim.

1.5.8 Shorewall

Shorewall és una eina que treballa sobre Netfilter i que permet aplicar fàcilment diferents dissenys de regles. Funciona sobre el sistema operatiu de Linux, però permet una gestió a distància utilitzant un navegador web.

Shorewall està considerat un dels tallafocs més potents per a distribucions Linux. Permet gestionar la xarxa utilitzant mecanismes senzills o bé aplicant una major complexitat quan és necessària.

Shorewall es pot descarregar dels repositoris oficials d'Ubuntu. La configuració es basa en treballar sobre quatre fitxers: interfaces, policy, rules i zones. A interfaces es configuren les interfícies del tallafoc. A zones es definiran les zones que s'administraran amb Shorewall i el tipus de zona. A policy s'especifica si s'accepta (ACCEPT) o no (DROP) el trànsit entre zones.

Exemple de fitxer /etc/shorewall/zones

```
#ZONE DISPLAY OPTIONS
fw firewall
net ipv4
loc ipv
dmz ipv4
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Exemple de fitxer /etc/shorewall/interfaces

```
#ZONE INTERFACE BROADCAST OPTIONS GATEWAY
net ppp0 detect
loc enp0s1 detect
dmz enp0s3 detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Exemple de fitxer /etc/shorewall/policy

```
#SOURCE DEST POLICY LOG LIMIT:BURST
loc net ACCEPT
dmz net ACCEPT
fw net ACCEPT
net all DROP info
all all REJECT info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

1.5.9 IPFire

La distribució Linux IPFire va nèixer com un *fork* del tallafoc IPCop i va ser reescrit a partir de la versió 2 (publicada el 2011). IPFire té llicència GNU desde 2007. Des de la seva web es pot descarregar una imatge ISO i fer una instal·lació com si fos un sistema operatiu Linux corrent. Un cop acabada la instal·lació del sistema operatiu, aquest demana fer un reinici per configurar la xarxa i les contrasenyes; una vegada fet això, podem entrar a la consola de configuració accedint a https://ipfire:444.

IPFire pot funcionar com a firewall o com a IDS.

IPFire com a firewall està construït sobre Netfilter, filtrant els paquets de forma molt ràpida i aconseguint rendiments de fins a desenes de Gigabits per segon.

Té una interfície web intuïtiva, que permet crear grups de màquines i de xarxes. Així pot contenir un gran conjunt de regles ordenades. També permet generar informes gràfics.

IPFire necessita, com a mínim, un processador de la família x86 amb 1 GHz, 1GB de RAM i 4GB de disc dur. També necessita 2 adaptadors Ethernet.

Permet filtrar i bloquejar atacs *DoS* (*Denial-of-Service*).

Logotip d'IPFire

Com a IDS, IPFire analitza el tràfic de la xarxa intentant detectar *exploits* i activitats sospitoses. En produir-se una detecció, s'envien les alertes corresponents i es bloqueja l'atacant.

En una configuració típica, IPFire es configura amb **Geen + Red**, que vol dir que tindrem 2 xarxes.

Normalment, hi ha dues xarxes: la xarxa **Green**, pels ordinadors de la xarxa interna, i la xarxa **Red**, pels altres ordinadors, connectats a través d'Internet.

Com a molt són possibles 4 xarxes, anomenades: **Green**, **Blue**, **Orange** i **Red**:

- La xarxa **Red** serà una WAN, és a dir, una xarxa externa conectada a Internet i al Proveidor d'Internet (ISP) corresponent.
- La xarxa **Green** serà la nostra xarxa interna o LAN privada.
- La xarxa **Orange** serà la Zona Desmilitaritzada, DMZ, on es podrà accedir a un servidor desprotegit o a una xarxa desprotegida des d'Internet.
- La xarxa **Blue** serà una xarxa Wireless WLAN, és a dir, una xarxa *wireless* separada per a aquest tipus de clients.

Per a instal·lar IPFire en una màquina virtual, podem crear al VirtualBox 2 interfícies de xarxa -és el mínim necessari- i escollir-hi el teclat *es*. Amb 2 interfícies de xarxa, podem configurar un sistema **Green+Red**; per fer-ho hem d'escollir **Red** com a *tipus de configuració* i, després, assignar els controladors i les targetes a les interfícies **Green** i **Red**.

Tot seguit, hem d'assignar les adreces IP a **Green**, que sol correspondre al host 1 d'una adreça IP privada (per exemple, 10.0.0.1), i **Red**, que serà especial ja que dependrà del nostre ISP. Sol ser una adreça IP pública (podria ser, per exemple, 193.100.10.8). Per acabar, només hem de configurar el DNS i la porta d'enllaç. Com a DNS primari podem posar l'adreça IP 8.8.8.8, que correspon al servidor DNS de Google, i, com a porta d'enllaç, la que tinguem a la xarxa. Seguint l'exemple anterior, un valor posible seria 10.0.0.50.

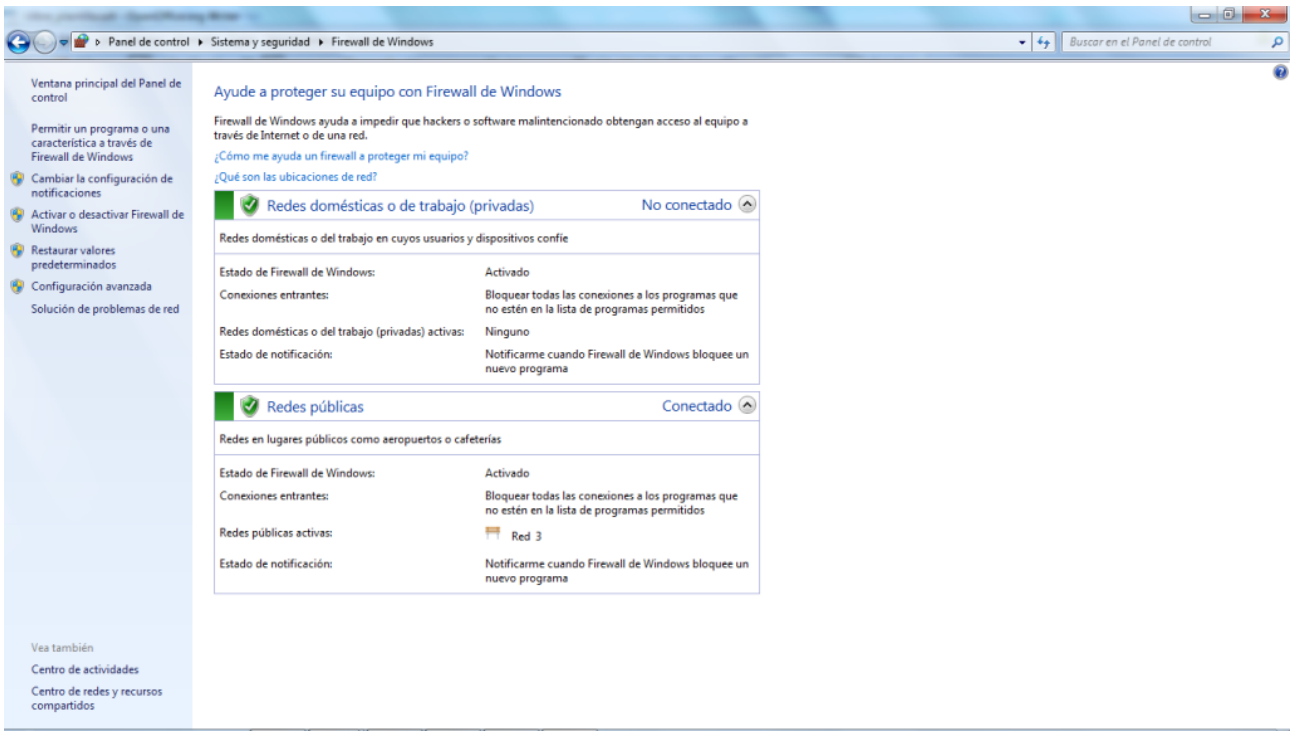
Amb `iptables -L` podem veure les cadenes que hi ha; entre aquestes trobarem GEOIPBLOCK, BADTCP, WIRELESSINPUT i TOR_INPUT.

1.5.10 Tallafoc de Microsoft Windows

El tallafoc de Microsoft Windows és un clar exemple de tallafoc per a xarxes domèstiques. No es requereixen grans coneixements per administrar-lo i és un programa ja instal·lat en el sistema operatiu. En molts casos aquest programa està funcionant a l'equip de l'usuari i aquest ho desconeix totalment.

La figura 1.32 mostra la pantalla de configuració del tallafoc. Es pot apreciar que no disposa de paràmetres tècnics ni requereix de gaires coneixements per activar-lo o desactivar-lo i per fer-ne una configuració bàsica.

FIGURA 1.32. Pantalla de configuració del tallafoc de Microsoft Windows



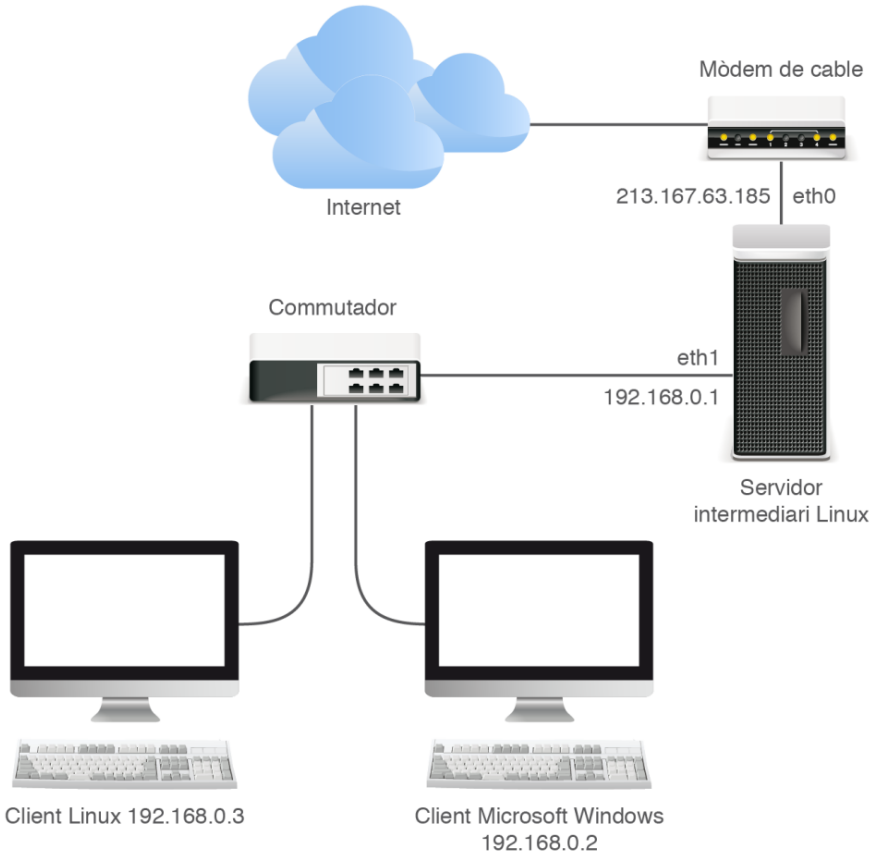
2. Servidors intermediaris

Una xarxa informàtica pot arribar a assolir un nivell de complexitat que faci que la seva gestió i manteniment es converteixi en un problema. Quan s'arriba a aquesta situació, la persona responsable de la xarxa ha de buscar solucions, ja que si no ho redreça pot esdevenir un caos organitzatiu. La utilització de màquines amb funcions específiques de centralització de gestions, capaces d'assumir determinades funcions abans encarregades a equips de xarxa sobrecarregats, és una solució molt interessant.

Un **servidor intermediari** és un programa o un equip capaç d'assumir les funcions d'un altre equip.

La figura 2.1 mostra un servidor intermediari en una xarxa petita. No és necessari treballar amb una gran estructura o una xarxa molt complexa per utilitzar un servidor intermediari. De servidors intermediaris n'hi ha diversos tipus.

Figura 2.1. Servidor intermediari en una xarxa petita



Les funcions més habituals d'un servidor intermediari són controlar l'accés a

serveis o a recursos, proporcionar memòria cau per a determinats serveis, registrar esdeveniments de xarxa i un llarg etcètera.

2.1 Característiques i tipus de servidors intermediaris

Els servidors intermediaris es caracteritzen per interceptar les connexions de xarxa que un client emet cap a un servidor de destinació.

El servidor intermediari més conegut és el servidor intermediari de web. Aquest equip té com a missió interceptar totes les peticions dels clients que sol·liciten pàgines web. Per què s'utilitza un servidor intermediari per consultar un web? En principi, això sembla que no tingui sentit, ja que l'accés es ralentitza, però el servidor intermediari web ofereix seguretat i rendiment, i permet ocultar identificacions, entre altres coses.

A part del servidors intermediaris web existeixen els servidors intermediaris ARP, els servidors intermediaris FTP i els servidors de patró de disseny (presents en entorns de programació).

Els servidors intermediaris es poden classificar depenent de qui desitgi implementar la política a aplicar: servidors intermediaris locals o servidors intermediaris externs.

En un **servidor intermediari local** implementa la política el mateix equip que realitza la petició.

Parlar d'un servidor intermediari local vol dir que el mateix client pugui establir regles de filtratge, control de trànsit o gestió d'accessos des de la màquina amb què treballa i realitza peticions de serveis.

En un **servidor intermediari extern** implementa la política un equip diferent al que realitza la petició.

Habitualment, els servidors intermediaris externs s'utilitzen per gestionar memòries cau, trànsit de xarxa o compartició de serveis i recursos. Els avantatges més destacats que ofereix la utilització de servidors intermediaris externs són la possibilitat de limitar l'accés als usuaris, forçant-los a passar pel servidor, restringir drets d'usuaris, estalviar recursos, millorar la velocitat de resposta dels serveis, filtrar el trànsit prohibit o modificar informació segons les necessitats. Però també presenta una sèrie d'inconvenients, ja que pot tenir un excés de càrrega que ralentitzi les connexions, pot generar situacions d'intromissió o es pot lliurar informació no actualitzada.

2.2 Funcions principals dels servidors intermediaris

Són diverses les funcions dels servidors intermediaris. La gestió de peticions, la gestió de la velocitat de resposta, el filtratge de continguts, l'emmascarament d'identitat o la gestió de continguts a demanda són possiblement els casos més utilitzats.

2.2.1 Gestió de peticions

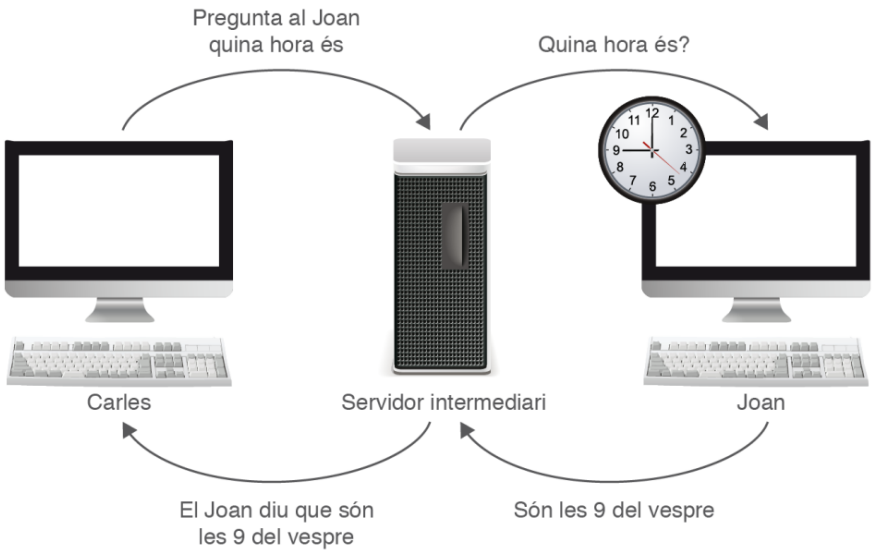
Gestionar les peticions a un determinat servei o recurs és sens dubte una de les funcionalitats estrella dels servidors intermediaris. Aquesta acció permet reduir dràsticament el trànsit que es genera en una xarxa quan els recursos o serveis són limitats i s'han de compartir.

Optimitzar els recursos

En determinades ocasions un lloc web és consultat per molts equips en una franja de temps petita. Si no se'n fa la gestió oportuna, això pot provocar la pèrdua de l'accés a Internet. Imagineu un nombre elevat d'equips sol·licitant consultar el mateix web: arribarà un moment en què l'accés a Internet no podrà oferir una qualitat de servei correcta. Solució: instal·lar un servidor intermediari que mantingui en la memòria les parts més sol·licitades del web que s'està consultant. Ara els equips de xarxa consultaran el web a la velocitat de la xarxa interna sense haver de sortir a Internet i provocar el col·lapse de la línia d'accés a l'exterior.

Com es pot observar en la figura 2.2, l'equip del client demana al servidor intermediari que demani l'hora a una altra màquina. La màquina que informa de l'hora es comunica amb el servidor intermediari, el qual envia les dades a l'equip client.

Figura 2.2. Servidor intermediari gestor de peticions



Com que la memòria dels servidors intermediaris que gestionen peticions no és infinita, requereixen l'ús d'algorismes que s'encarreguen d'anar renovant les entrades.

Quan fa temps que un lloc web no és sol·licitat s'allibera la memòria que s'utilitzava per emmagatzemar les seves dades, i així queda disponible per a noves consultes.

2.2.2 Gestió de la velocitat de resposta

És habitual estar constantment enviant i rebent dades d'Internet, però potser no té gaire sentit anar moltes vegades a buscar una mateixa informació a l'exterior. Una manera eficient de treballar és descarregar els continguts d'Internet una vegada i distribuir-los a la velocitat de la xarxa interna. La velocitat és un dels factors que surt guanyant en aquest cas.

Aprofitar la xarxa local

Amb periodicitat semestral apareixen distribucions millorades del sistema operatiu Ubuntu. Per actualitzar les màquines no es permet que accedeixin totes a Internet, sinó que l'actualització es baixa a una màquina local de la xarxa i la resta d'equips hi accedeixen a la velocitat de la xarxa interna. La gestió de la velocitat de resposta és sens dubte un dels punts forts dels servidors intermediaris.

2.2.3 Filtratge

Els servidors intermediaris permeten realitzar el filtratge de continguts, com per exemple determinats tipus de fitxers. És força comú que les xarxes corporatives no permetin el trànsit de correu que contingui fitxers adjunts o que determinats perfils d'usuari no accedeixin a continguts externs a la intranet.

Un mètode per tal d'evitar introduir virus a la xarxa d'una empresa és no permetre l'entrada de correus que continguin fitxers adjunts.

2.2.4 Emmascarar la identitat

En ocasions pot resultar útil amagar a un servidor la identitat d'una màquina que sol·licita un servei. El servidor que ofereix un recurs o un servei detecta que un servidor intermediari està realitzant una petició i no reconeix quina és la màquina que realment fa la sol·licitud.

2.2.5 Continguts a demanda

Determinats servidors intermediaris s'utilitzen per modificar la presentació de la informació. Depenent del dispositiu (tauleta, PDA, telèfon intel·ligent, PC...) o del navegador utilitzat hi ha continguts que requereixen una modificació per poder ser visualitzats correctament.

La importància de la imatge

Si es consulta el web de segons quins diaris des de diferents plataformes es pot comprovar que el format de la pàgina s'adapta per oferir la màxima llegibilitat en cadascuna d'elles.

2.3 Configuració i utilització de servidors intermediaris

Parlar de servidor intermediari en general no té gaire sentit. Els servidors intermediaris són dispositius o programes que realitzen unes funcions determinades segons els seus objectius, que poden ser molts i variats. Això fa que la seva configuració i utilització variïn.

2.3.1 Tipus de servidors intermediaris

Actualment el mercat ofereix tot de servidors intermediaris específics per complir determinades funcionalitats. La identificació d'aquestes funcions permet crear etiquetes com ara servidor intermediari de web, servidor intermediari *proxy*, servidor intermediari transparent, servidor intermediari SOCKS, servidor intermediari invers, servidor intermediari obert i servidor intermediari d'emmascarament.

Servidor intermediari de web

A vegades es necessita disposar d'un mecanisme per concentrar l'accés a una intranet o a Internet des d'una xarxa informàtica i, alhora, quan el trànsit és elevat i hi ha moltes peticions a continguts cal evitar la baixada de la velocitat d'accés.

Els **servidors intermediaris de web** possibiliten l'accés al web i ofereixen memòria cau per millorar la velocitat d'accés a continguts.

El funcionament d'aquest servidors és molt senzill i alhora molt productiu. Quan un usuari vol realitzar una consulta al web, primer passa pel servidor intermediari. Si la informació que busca s'ha consultat amb anterioritat, en comptes d'anar a la web original, el servidor web intermediari mostra els continguts emmagatzemats en la seva memòria. En resum, no cal sortir al web per accedir a uns continguts que un altre usuari ha consultat recentment. La velocitat de resposta del servidor intermediari web és molt més alta que la que possibilita el servidor públic.

L'ús de servidors intermediaris web, però, presenta un inconvenient: pot passar que una informació emmagatzemada en la memòria del servidor intermediari canviï en el servidor web original, la qual cosa farà que les dades que lliuri el servidor intermediari no es corresponguin amb la informació real que es vol consultar.

Servidor intermediari proxy

Les xarxes en les quals conviuen molts equips o en les quals cal filtrar tots els requeriments a un servei requereixen la utilització d'un servidor intermediari *proxy* per millorar l'eficàcia de funcionament de la xarxa.

Un **servidor intermediari *proxy*** s'interposa entre els usuaris i l'accés a un servei. Generalment es facilita l'accés al servei mitjançant una aplicació web.

No s'ha de confondre un servidor intermediari *proxy* amb un servidor intermediari web, ja que el segon ofereix l'accés a un recurs determinat: el web. En canvi, el servidor intermediari *proxy* està obert a qualsevol tipus de recurs o servei.

Servidor intermediari transparent

Quan es parla d'utilitzar recursos transparents ens referim a fer ús d'equips sense que l'usuari hagi de realitzar cap modificació en la seva configuració. Utilitzar equips no transparents implica que en un moment o un altre, l'usuari, que tindrà més o menys coneixements, haurà de realitzar algun tipus d'acció en el seu equip. Això genera dos grans problemes: el primer és que un usuari inexpert no pugui accedir al recurs o serveis, i el segon, que els usuaris experts i no autoritzats obtinguin informació sobre la configuració i detecten vulnerabilitats.

Un **servidor intermediari transparent** ofereix accés a recursos i serveis sense que l'usuari hagi de fer cap canvi de configuració.

Un exemple de l'ús de servidors intermediaris transparents és el que fan les empreses proveïdores d'Internet: quan contracten un servei d'accés a Internet l'únic que cal fer és connectar l'equip d'accés, generalment un encaminador preconfigurat, i deixar tots les opcions de l'equip en automàtic.

Servidor intermediari SOCKS

En ocasions el nivell de seguretat de les comunicacions entre ordinadors ha de ser molt alt. Per aconseguir-ho, una opció és permetre l'accés a un servidor extern únicament a un equip determinat.

Un **servidor intermediari SOCKS** és l'únic equip que té accés a un servidor extern. Qualsevol usuari que desitgi accedir a aquest servidor extern ha d'establir prèviament connexió amb el servidor intermediari SOCKS.

L´ús de servidors intermediaris SOCKS està molt vinculat a aplicacions que ofereixen connexions segures, com per exemple *PuTTY*. El servidor intermediari SOCKS utilitza un protocol de la capa 5 que s'anomena SOCKS. Quan s'estableix la comunicació entre l'equip de l'usuari i el servidor intermediari SOCKS, el client demana tot el que li cal al servidor intermediari, que s'encarrega de fer les peticions a l'exterior.

Servidor intermediari invers

Si la raó de ser dels servidors intermediaris és estar al mig del camí de l'accés d'un equip intern a una xarxa externa, a vegades cal fer el mateix, però a la inversa.

Un **servidor intermediari invers** intercepta el trànsit de l'exterior que va cap a un servidor intern.

Interceptar el trànsit d'entrada a la xarxa n'augmenta la seguretat: el servidor intermediari invers ofereix una capa més a l'estratègia de seguretat implantada. Una altra raó per al seu ús, també lligada amb la seguretat, és que si es necessita xifrar la comunicació de l'exterior cap a un equip de l'interior de la xarxa, per exemple amb SSH, el servidor intermediari invers s'encarregarà de permetre la sessió SSH. Un servidor d'aquest tipus també podria repartir la càrrega cap a diferents equips interns, o fer de servidor cau per a la xarxa interna.

Servidor intermediari obert

L'usuari habitual de serveis com Internet coneix conceptes com *llista negra*. Estar en una llista negra implica que se'ns negui l'accés a diversos continguts o s'interceptin correus electrònics lligats a un determinat domini. Quan s'investiga per què s'ha afegit el nostre domini en una llista negra la resposta més comú és que enviem correu brossa o que els nostres equips s'utilitzen com a plataforma de salt. Si no és així, acostuma a ser degut a una gestió deficient d'un servidor intermediari obert.

Un **servidor intermediari obert** accepta les peticions d'equips que no tenen per què formar part de la seva xarxa.

Quan un equip que no forma part de la xarxa es connecta al servidor intermediari obert i fa qualsevol petició, a ulls externs la petició l'ha realitzat el servidor, per tant, sigui el que sigui el que estigui fent l'usuari, es vincularà al servidor intermediari obert i, en conseqüència, a l'administrador del servidor.

Servidor intermediari d'emmascarament

El funcionament habitual d'una xarxa informàtica és que els equips que en formen part de la xarxa local tinguin una adreça privada i accedeixin a l'exterior de la LAN amb una única IP pública. Això és possible gràcies a un pas previ: l'emmascarament.

Un **servidor intermediari d'emmascarament** s'encarrega de permetre als equips d'una xarxa interior l'accés a l'exterior utilitzant una adreça pública.

La utilització d'un servidor intermediari d'emmascarament afegeix seguretat a la

xarxa, ja que els equips de la xarxa interna no queden exposats a atacs perpetrats des de l'exterior.

2.3.2 Exemples de servidors intermediaris

Al mercat es poden trobar diversos exemples molt interessants de servidors intermediaris. Cada vegada més la seva instal·lació està esdevenint una pràctica habitual a causa de la facilitat d'administració i la gran quantitat de possibilitats que ofereixen.

Servidors intermediaris com ara Squid, Ziproxy o Polipo són casos prou coneguts que cada vegada més són presents a les xarxes informàtiques.

Squid

Logotip del programa Squid

Un dels servidors intermediaris més populars en entorns Unix és Squid. Aquest programari implementa un servidor intermediari i un domini per a memòria cau de llocs web.

Squid disposa de la majoria de funcionalitats pròpies dels servidors intermediaris:

- Permet l'accés web a màquines privades que no estan connectades directament a Internet.
- Registra el trànsit web que surt de la xarxa local.
- Controla l'accés web utilitzant regles.
- Funciona com a memòria cau de pàgines web.
- Controla el contingut web consultat.
- Controla les descàrregues que es realitzen.
- Implementa una memòria cau per a les connexions fallides.
- Emmagatzema en la memòria cau les peticions DNS.
- És compatible amb el protocol ICP.
- Registra totes les peticions realitzades.

Squid s'ha d'instal·lar en una màquina que se situarà entre les màquines dels usuaris i una altra xarxa (per exemple Internet). Squid farà de frontera entre xarxes, separant-les i permetent accelerar l'accés a llocs web o restringint l'accés a continguts.

Squid permet centralitzar el trànsit de la xarxa local cap a una altra xarxa.

Només la màquina que té instal·lat Squid ha de disposar d'accés a la xarxa d'Internet.

Un detall molt important a tenir en compte és que la màquina que tingui instal·lat Squid ha de tenir dues interfícies de xarxa per tal de poder exercir de frontera. Una interfície s'utilitza per tenir accés a la xarxa local i l'altra per proporcionar accés a Internet.

No hem de confondre Squid amb un servidor web. Squid emmagatzema les dades que sol·liciten els clients i així les pot oferir a altres peticions a gran velocitat, però no ofereix pàgines web per sí mateix. Squid només permet accedir a les pàgines originals si detecta que s'hi han produït modificacions.

Existeixen programes que ajuden a configurar i a operar amb squid, com per exemple Gadmin-Squid.

Ziproxy

El servidor intermediari Ziproxy permet reduir la mida d'imatges JPG i comprimir fitxers HTML. Aquestes accions optimitzen la navegació i accés a dades. A més, aquest servidor intermediari optimitza la càrrega d'HTML, JavaScript i CSS.

No necessita programari client i dóna resultats en qualsevol navegador i sistema operatiu.

Polipo

Polipo és un servidor intermediari de memòria cau per a navegació. Es tracta d'un programa molt lleuger que no presenta cap complicació en la instal·lació ni en la configuració.

Polipo està als repositoris oficials d'Ubuntu i es configura mitjançant el fitxer /etc/polipo/config. El canvi de configuració no s'aplicarà fins que no es reinicii el programa.

2.3.3 Instal·lació de servidors intermediaris

La instal·lació física dels servidors intermediaris és bàsica per aconseguir la màxima eficiència de la xarxa.

Un **servidor intermediari** s'ha de situar entre la màquina de l'usuari i la xarxa externa, generalment Internet.

Només d'aquesta manera es pot centralitzar el trànsit de la xarxa local cap a

l'exterior. Totes les peticions cap a l'exterior dels equips de la xarxa local hauran de passar per el servidor intermediari.

Instal·lació d'Squid

La instal·lació d'Squid es pot fer des dels repositoris oficials d'Ubuntu amb la línia:

```
1 sudo apt-get install squid
```

Els directoris amb els quals s'ha de treballar són:

- /usr/bin/: directori executable
- /var/run/: directori amb el PID del procés
- /var/log/squid/: directori de registres
- /var/spool/squid/: directori de memòria cau
- /etc/squid/: fitxers de configuració
- /usr/lib/squid/: complements
- /usr/share/doc/squid/: documentació

Després d'instal·lar Squid caldrà canviar-ne la configuració per poder treure-li rendiment. El fitxer de configuració d'Squid és squid.conf. Els paràmetres més importants a considerar són:

- http_port: indica el port que s'utilitzarà per escoltar el servidor. Per defecte aquest valor és 3128.
- cache_mem: defineix la memòria RAM que s'utilitzarà per emmagatzemar les dades que més se sol·licitin.
- cache_swap_low: indica el nivell d'espai mínim que s'ha de mantenir en l'àrea d'intercanvi.
- cache_swap_high: indica el nivell d'espai màxim que s'ha de mantenir en l'àrea d'intercanvi.
- maximum_object_size: indica la mida màxima que poden tenir els objectes que s'emmagatzemen en la memòria cau.
- hierarchy_stoplist: indica els caràcters que s'utilitzaran com a filtre. Si els caràcters es detecten en una adreça web es carrega directament el contingut des de la memòria cau.
- visible_hostname: indica el nom de l'equip.
- cache_dir: estableix la mida que es reservarà en el disc per a la memòria cau.

- access_log: indica el directori en què s'emmagatzemaran els accessos a Squid.
- cache_log: estableix la ruta en què s'emmagatzemaran els missatges de *log* d'Squid.

2.3.4 Configuració de filtres

Els filtres que es configuren en els servidors intermediaris utilitzen majoritàriament llistes de control d'accés, conegudes com a ACL.

Les llistes ACL realitzen una acció sobre els paquets que tinguin determinades característiques. Una ACL s'ha d'identificar amb un nom o un número i cada regla especifica una condició i una acció. Les accions que es poden executar són permetre o denegar tots els paquets que acompleixin una condició.

```
1 acl nom_o_numero acció condició
```

Si un paquet compleix la condició se li aplicarà l'acció. Les accions són només permetre o negar, i les condicions depenen del tipus d'ACL. Les ACL més senzilles, anomenades *estàndard*, especifiquen valors per comparar amb l'adreça IP d'origen del paquet, mentre que en les ACL anomenades *extenses* les condicions permeten especificar valors per comparar IP d'origen, IP de destinació, protocols de capa 4, ports, indicadors de TCP...

Configuració de filtres amb Squid

Hi ha disponibles diversos elements per treballar amb ACL. És imprescindible fer una petita descripció de cadascun d'ells per tal d'aplicar les regles amb la lògica amb la qual han estat dissenyades:

- `src`: especifica una o diverses adreces de xarxa o un segment de la xarxa amb la seva màscara corresponent.

  Una regla anomenada "xarxa_servidors" que té assignada la subxarxa 192.168.10.0/24 seria:

```
1 acl xarxa_servidors src 192.168.10.0/24
```

  Per indicar un conjunt d'adreces de xarxa s'utilitzaria també l'ordre src:

```
1 acl equips_publics src 192.168.10.5 192.168.10.7 192.168.10.27
```

  I fins i tot es poden indicar les adreces des d'un fitxer:

```
1 acl produccio src "/etc/squid/"p_produccio
```

  Per a una sola adreça IP:

```
acl administrador src 192.168.1.10/255.255.255.255
```

O bé:

```
acl administrador src 192.168.1.10/32
```

Per definir una subxarxa:

```
acl xarxa_inf src 192.168.1.0/255.255.255.0
```

Per definir una llista d'adreces:

```
acl programadors src 192.168.1.11 192.168.1.12 192.168.1.13
```

La llista d'adreces de xarxa pot estar escrita en un fitxer i ser carregada:

```
acl programadors src "/etc/squid/programadors."acl
```

Per crear una llista basada en un rang d'adreçes IP:

```
acl programadors src 192.168.1.11-192.168.1.13
```

"tothom": s'utilitza per filtrar tots els equips d'una xarxa.

```
acl tothom src 0.0.0.0/0.0.0.0
```

La mateixa màquina d'origen: la nostra màquina serà l'origen de les connexions.

```
acl localhost src 127.0.0.1/255.255.255.255
```

El tipus MIME d'un fitxer és una descripció del fitxer. Generalment s'utilitzen a la banda dels servidors perquè el gestor esculli la millor manera de mostrar l'element.

- A més de treballar amb adreces IP es poden crear regles d'accés basades en ports, dominis, adreces web i tipus MIME:

```
acl ports_segurs port 8080 23 443 1025-65535
```

- `dts`: s'utilitza per indicar l'adreça de destinació en format IP i màscara o el nom de la destinació. Per exemple es podria declarar una regla que fes referència a adreces de xarxa de la nostra subxarxa:

  acl ips_departament dst 192.168.3.5 192.168.3.6 192.168.3.7

  O fins i tot de servidors de correu habituals:

```
acl correus dst www.gmail.com www.hotmail.com www.webmail.com
```

  La mateixa màquina com a destinació.

```
acl localhost_destinacio dst 127.0.0.0/255.255.255.255
```

- `srcdomain`: serveix per donar accés a dominis determinats. Aquesta regla no funcionarà si no es disposa d'un DNS local. El cas següent indicaria els noms d'equip que pertanyen a la xarxa:

```
acl equips srcdomain servidorweb.lamevaxarxa.com servidorcorreu.
    lamevaxarxa.com repositori.lamevaxarxa.com
```

- `dstdomain`: estableix els permisos sobre els dominis web de destinació. Per exemple, es podria utilitzar per etiquetar els dominis prohibits:

```
acl dominis_prohibits dstdomain .messenger.com live.com jocs.com
```

- `srcdom_regex`: és la responsable d'avaluar text d'entrada a la xarxa. Si, per exemple, volem analitzar les paraules "examen" que circulin per la nostra xarxa farem:

```
acl xarxa_local srcdom_regex -i examen\..*
```

- `dstdom_regex`: s'encarrega d'avaluar text de sortida de la xarxa. Si per exemple volem analitzar totes les paraules de sortida que continguin "google" s'aplicarà:

```
acl consulta_google dstdom_regex -i google\..*
```

- `time`: marca el temps límit de connexió dins d'una setmana. S'utilitza un paràmetre per indicar cada dia de la setmana segons la taula 2.1. I les hores s'utilitzen seguint el format de vint-i-quatre hores. Si, per exemple, es vol habilitar una regla per als dissabtes i diumenges de vuit del vespre a onze de la nit:

```
acl caps_setmana_nit time AS 20:00-23:00
```

Taula 2.1. Paràmetre que indica el dia de la setmana amb Squid

Dia de la setmana	Paràmetre
Dilluns	M
Dimarts	T
Dimecres	W
Dijous	H
Divendres	F
Dissabte	A
Diumenge	S

- `url_regex`: permet especificar text que aparegui en adreces web i interceptar la informació. El més habitual és emmagatzemar en un fitxer les paraules a les quals volem aplicar el filtre:

```
acl webs_prohibits url_regex "/etc/squid/webs/prohibits."txt
```

- `urlpath_regex`: s'utilitza per poder administrar el trànsit de dades utilitzant l'extensió dels fitxers. És habitual utilitzar un fitxer per emmagatzemar les extensions a considerar:

```
acl pelis urlpath_regex "etc/squid/filtres/peelis."txt
```

- `req_mime`: amb aquest tipus de regla es comprova el tipus de petició MIME realitzada per un client. Per filtrar trànsit del programa Messenger de Microsoft:

```
acl messenger req_mime type application/x-msn-messenger
```

- `macaddress`: permet realitzar l'administració utilitzant les adreces MAC dels equips. Per exemple, per controlar els equips de direcció utilitzant les seves adreces MAC:

```
acl mac_direccio arp 1C:75:08:AC:**:** 1C:75:08:AD:**:** 1C:75:08:AD
    :**:**
```

- `password`: pot controlar l'accés a Internet utilitzant un nom d'usuari i una contrasenya.

Utilització d'usuari i contrasenya per accedir a un servei

L'exemple següent mostra pas a pas el procediment a seguir per establir autenticació per accedir a un servei:

1. Crear un fitxer que contingui les claus d'accés:

   ```
   vi claus
   ```

2. Donar permís d'escriptura i lectura:

   ```
   chmod 600 claus
   ```

3. Canviar el propietari:

   ```
   chown squid.squid claus
   ```

4. Crear l'usuari i la contrasenya per accedir a Internet:

   ```
   htpasswd claus clients
   ```

5. Modificar el paràmetre "auth_param":

   ```
   auth_param basic program
   /usr/lib/squid/ncsa_auth /etc/squid/claus
   ```

6. Habilitar la regla:

   ```
   acl password proxy_auth REQUIRED
   ```

- `http_access`: el control d'accés es realitza amb `http_access`. Per permetre l'accés als equips vinculats a la regla "estudiants" escriurem:

```
http_access allow estudiants
```

I per no permetre l'accés als equips vinculats a la regla "visitants" afegirem:

```
http_access deny visitants
```

Permetre o negar l'accés a una o més ACL: amb el paràmetre `allow` es permet l'ACL i amb `deny` es denega. En l'exemple següent se'ns permet l'accés encara que no siguem programadors:

```
http_access allow ! Programadors
```

2.3.5 Configuració de l'emmagatzematge en memòria cau d'un servidor intermediari

Un dels problemes més habituals dels servidors intermediaris és la gestió de l'emmagatzematge en memòria cau. En alguns servidors, com per exemple Polipo, gestionar deficientment la memòria pot provocar deixar sense memòria la màquina que allotja el servidor. Aquest problema es reprodueix en la resta de servidors i Squid no n'és l'excepció. Utilitzarem Squid com a exemple de dos processos: esborrar la memòria cau i evitar el servidor intermediari per realitzar determinades consultes.

Esborrar la memòria cau d'Squid

Una de les tasques que s'han de realitzar dins els procediments de manteniment d'un servidor intermediari Squid és netejar la seva memòria cau. Tot i que es tracta d'una acció molt senzilla i que a priori pugui semblar una tasca secundària, no és aquest el cas. Una mala gestió de la memòria cau pot inhabilitar el servidor.

Abans de fer cap acció vinculada a la memòria cau cal parar el dimoni d'Squid:

```
1 sudo service squid stop
```

Per comprovar que efectivament Squid està aturat:

```
1 sudo service squid status
```

Per eliminar el contingut emmagatzemat a la memòria cau d'Squid es pot utilitzar la línia:

```
1 sudo rm –rf /var/spool/squid/*
```

Sovint, la informació emmagatzemada a la memòria cau d'Squid pot aportar dades que ajuden a interpretar problemes de la xarxa. Una bona opció per no perdre aquesta informació és fer-ne una còpia abans d'eliminar-la:

```
1 sudo mkdir /var/spool/squid/copia/
2 sudo mv /var/spool/squid/ /var/spool/squid/copia/
```

I ara només cal reiniciar el dimoni:

```
1 sudo squid start
```

Exemple de com no utilitzar la memòria cau amb Squid

El servidor intermediari Squid és una bona solució per millorar l'accés a Internet, però en determinades ocasions pot ser un problema.

Error en la visualització de dades

Suposem que estem esperant la publicació de la nota d'un examen. Cada cinc minuts consultem el web on s'ha de publicar la nota i aquesta no apareix. Se'ns ocorre trucar a un amic i aquest ens comunica que les notes s'han publicat fa un parell d'hores. Amb neguit tornem a consultar la pàgina web i res de res. Hi haurà algun problema amb la meva nota? No! El que passa és que des de la xarxa on estic fent la consulta hi ha un servidor Squid que no m'està mostrant l'última versió del web. El que no paro de consultar és una pàgina descarregada en local que no reflecteix els canvis!

El servidor intermediari Squid permet indicar dominis que no s'emmagatzemaran en memòria cau:

```
sudo vi /etc/squid/dominis_no_cache
```

Aquests dominis s'inclouran en un fitxer de text:

```
ioc.xtec.cat
gmail.com
hotmail.com
```

Una solució molt enginyosa que ofereix Squid és que permet indicar equips que no utilitzin la memòria cau del servidor intermediari. Aquesta acció es realitza mitjançant l'adreça MAC dels equips:

```
acl equip_sense_cau arp 1C-75-08-AC-**-**
```

I aquesta línia s'afegeix al fitxer de configuració

```
/etc/squid/squid.conf
```

Perquè aquest procediment tingui efecte caldrà reiniciar el dimoni amb:

```
sudo squid restart
```

Exemple de fitxer squid.conf

A continuació es mostra part del contingut del fitxer squid.conf, en el qual s'utilitzen alguns dels conceptes bàsics d'aquest programa:

Una opció molt interessant és donar un nom propi a Squid perquè aquest sigui més reconeixedor a la xarxa:

```
visible_hostname servidor_intermediari
```

A continuació es defineixen les diferents xarxes a tractar amb ACL:

```
acl xarxa_local src 192.168.0.0/24
```

També es marca l'horari de treball:

```
acl jornada_laboral time M T W H F 8:30-22:00
```

Per decissió administrativa s'ha decidit restringir una màquina de la xarxa:

```
acl maquina_restringida src 192.168.0.15
```

Per fer efectiva la restricció en la màquina anterior:

```
http_access deny maquina_restringida
```

I per permetre l'accés a la xarxa local durant les hores de feina:

```
http_access allow xarxa_local jornada_laboral
```

A causa del mal ús que es fa de la xarxa es decideix que no es pugui accedir a determinats continguts. S'editarà el fitxer webs_prohibits amb:

```
#fitxer: /usr/local/etc/webs_prohibits
www.webprohibit1.com
www.webprohibit2.com
www.webprohibitN.com
```

També es pot indicar en un fitxer quins són els llocs web permesos, i titular-lo, perexemple, webs_permesos:

```
#fitxer: /usr/local/etc/webs_permesos
ioc.xtec.cat
```

I ara només caldrà especificar les corresponents ACL en el fitxer de configuració d'Squid:

```
acl WebsPermesos dstdomain "/usr/local/etc/"webs_permesos
acl WebsProhibits dstdomain "/usr/local/etc/"webs_prohibits
```

També es podria combinar amb http_access la xarxa local, l'horari d'oficina i els llocs web permesos:

```
http_access allow xarxa_local jornada_laboral WebsPermesos
```

2.3.6 Mètodes d'autenticació d'un servidor intermediari

En funció del servidor intermediari que s'utilitzi es disposarà d'un ventall més o menys gran de possibilitats per treballar amb modes d'autenticació. Per entendre els modes d'autenticació bàsics caldrà comprendre dos conceptes molt importants: el tipus de desafiament (*type of challenge)* i les credencials substitutes (*surrogate credentials*).

El **tipus de desafiament** indica el tipus de desafiament que es trobarà un client.

En el món de la informàtica el tipus de desafiament consisteix a plantejar una pregunta a l'usuari, que ha de respondre adequadament per poder continuar. Es tracta d'un protocol d'actuació molt utilitzat des de fa molt de temps.

El *tipus de desafiament* més simple és demanar confirmar una contrasenya.

Les **credencials substitutes** consisteixen a utilitzar unes determinades credencials fictícies en comptes d'utilitzar les reals.

Els modes d'autenticació més habituals són:

- **Auto**: el mode d'autenticació *auto* o *default* se selecciona en funció del que el client sol·liciti. Depèn del tipus de connexió i la configuració d'autenticació dels equips.
- **Proxy-IP**: el servidor intermediari utilitza un *type of challenge* de manera explícita i la IP de l'equip client com a credencials substitutes.
- **Origin**: el servidor intermediari treballa com si es tractés d'un servidor de comunicacions en temps real. Quan s'autentica la connexió es pot utilitzar com a credencial substituta.
- **Origin-IP**: el servidor intermediari treballa com si es tractés d'un servidor de comunicacions en temps real i, a més, pot generar i presentar al client desafiaments.
- **Origin-Cookie**: el servidor intermediari actua com un Origin-IP, però és capaç de generar una galeta (*cookie*) com a credencial substituta. És més segur que Origin-IP. S'ha de destacar que aquesta configuració permet treballar en servidor invers. Cal tenir en compte que només HTTP i HTTPS admeten galetes.
- **Origin-cookie-redirect**: en aquest cas es redirigeix el client cap a una adreça virtual on es realitzarà el procés d'autenticació. Les galetes s'utilitzaran com a credencials substitutes.
- **SGOS 3.0**: fent ús de regles predefinides al sistema, permet establir comunicacions segures.
- **From-IP**: realitza un cerca de les credencials d'usuari. Quan caduca una credencial, busca la correspondència amb l'usuari i fa una cerca de noves credencials.
- **From-Cookie**: es realitza una recerca de credencials vinculades a un usuari. Les galetes es relacionen amb un servidor intermediari i l'usuari adquireix un perfil específic per a cada domini.
- **From-Cookie-Redirect**: en aquest cas s'envia la sol·licitud de l'usuari a una adreça virtual. L'usuari haurà de superar un *type of challenge* quan les credencials expirin.
- **From-IP_Redirect**: aquest mode treballa gairebé igual que el From-IP, excepte que en aquest cas l'usuari és enviat a una adreça virtual abans de ser presentat.

2.3.7 Instal·lació i configuració de clients de servidors intermediaris

La utilització de servidors intermediaris comporta un pas previ: configurar els equips dels usuaris perquè utilitzin el servidor intermediari. En determinats casos, si la màquina del client està configurada per adquirir configuracions automàticament, no caldrà fer-hi cap canvi, però en d'altres és necessari configurar els navegadors.

Els navegadors més utilitzats són Internet Explorer, Firefox i Chrome. Per tant, caldrà estudiar com es configuren manualment els servidors intermediaris en aquests programes.

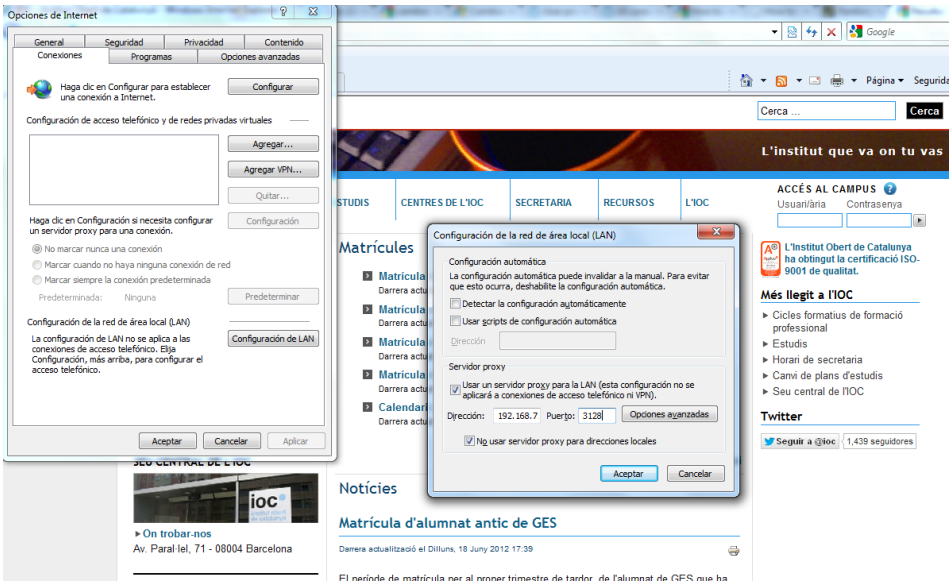
Configurar el servidor intermediari amb Internet Explorer

Més de la meitat dels usuaris domèstics utilitzen Microsoft Internet Explorer per navegar per Internet. La configuració del servidor intermediari és habitual quan l'usuari s'ha de connectar a Internet utilitzant una xarxa corporativa, i es dóna el cas que en general Internet Explorer detecta automàticament la configuració del servidor intermediari.

Si Internet Explorer no detecta la configuració caldrà seguir els passos següents:

1. Obrir el Microsoft Internet Explorer.
2. Prémer *Eines*.
3. Fer clic a *Opcions d'Internet*.
4. Activar la fitxa *Connexions*.
5. Anar a *Configuració de LAN*.
6. Al quadre *Adreça* indicar l'adreça del servidor intermediari.
7. Al quadre *Port* indicar el port escaient.
8. Fer clic a *Acceptar* per guardar els canvis.

FIGURA 2.3. Configuració del servidor intermediari a Internet Explorer de Microsoft Windows



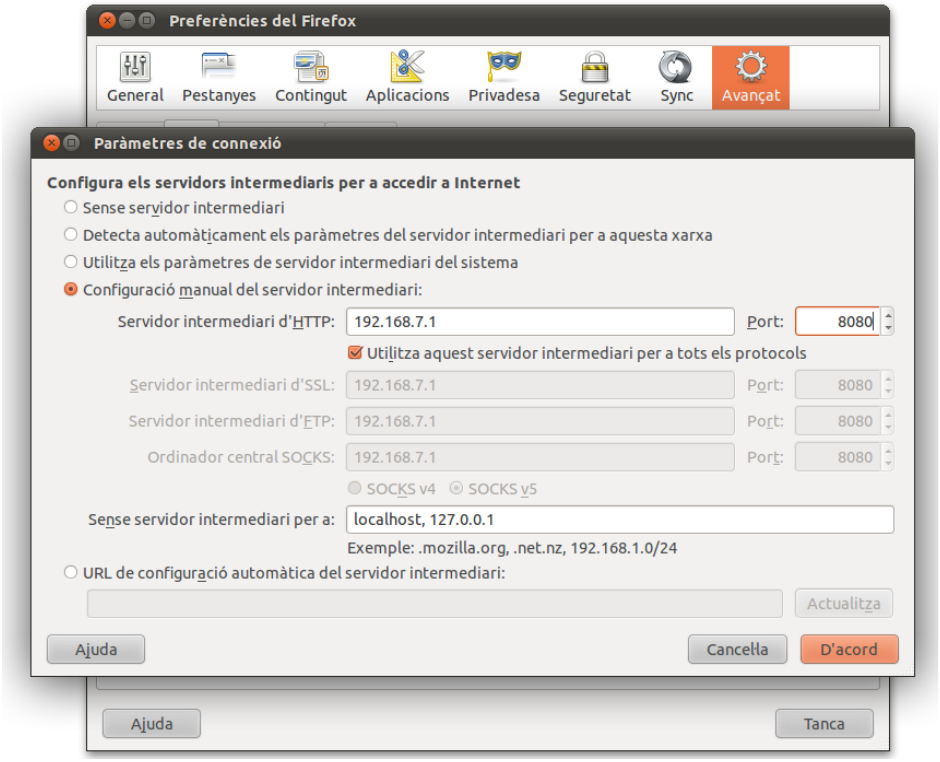
La interfície de configuració que utilitza Internet Explorer de Microsoft Windows és molt intuïtiva, tal com mostra la figura 2.3. En moltes ocasions la caixa *Detectar la configuració automàticament* estarà marcada i no caldrà fer cap canvi en la configuració.

Configurar el servidor intermediari amb Firefox

Els passos a seguir per configurar el servidor intermediari en Firefox són els següents:

1. Obrir el navegador Firefox.
2. Fer clic a *Edita*.
3. Prémer *Preferències*.
4. Activar la pestanya *Avançat*.
5. Activar la pestanya *Xarxa*.
6. Fer clic a *Paràmetres*.
7. Marcar *Configuració manual del servidor intermediari*.
8. Indicar l'adreça i port del servidor intermediari.
9. Si fos el cas, deixar marcat el quadre *Utilitza aquest servidor intermediari per a aquesta xarxa*.
10. Fer clic al botó *D'acord*.
11. Tancar el quadre de menús.

FIGURA 2.4. Configuració del servidor intermediari a Firefox



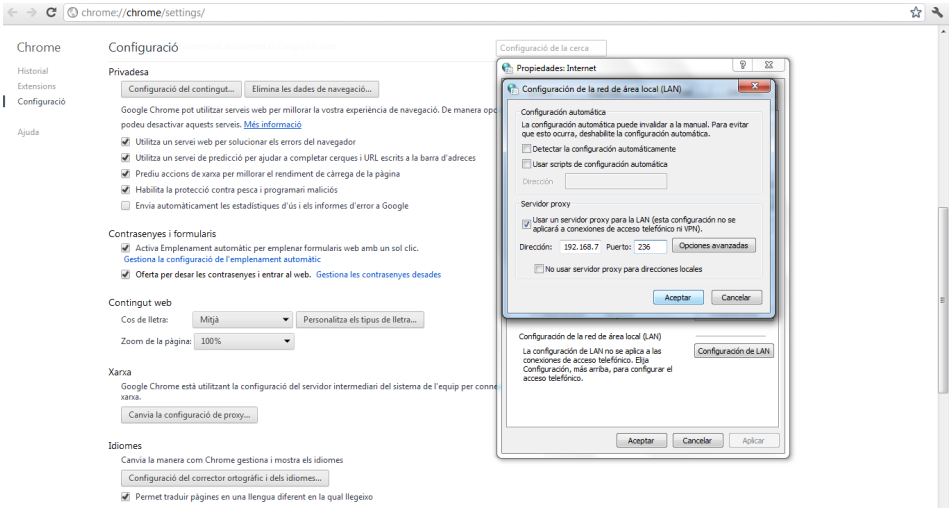
Com es pot observar en la figura 2.4, en aquest cas els paràmetres de connexió permeten configurar una màquina com a servidor intermediari genèric i evitar que determinades consultes passin pel servidor intermediari.

Configurar el servidor intermediari amb Chrome

El navegador Google Chrome és el tercer en percentatge d'ús a nivell mundial. La configuració del servidor intermediari es realitza seguint els passos següents:

1. Obrir el navegador Chrome.
2. Fer clic a la clau que apareix a la cantonada superior dreta: *Personalitza i controla Google Chrome*.
3. Prémer *Configuració*.
4. Anar a la part baixa de la finestra i fer clic a M*ostra la configuració avançada*.
5. Dins de *Xarxa*, ferclic a *Canvia la configuració de proxy...*
6. Anar a *Configuració de LAN*.
7. Indicar l'adreça del servidor intermediari i el port que utilitzi.

FIGURA 2.5. Configuració del servidor intermediari a Chrome



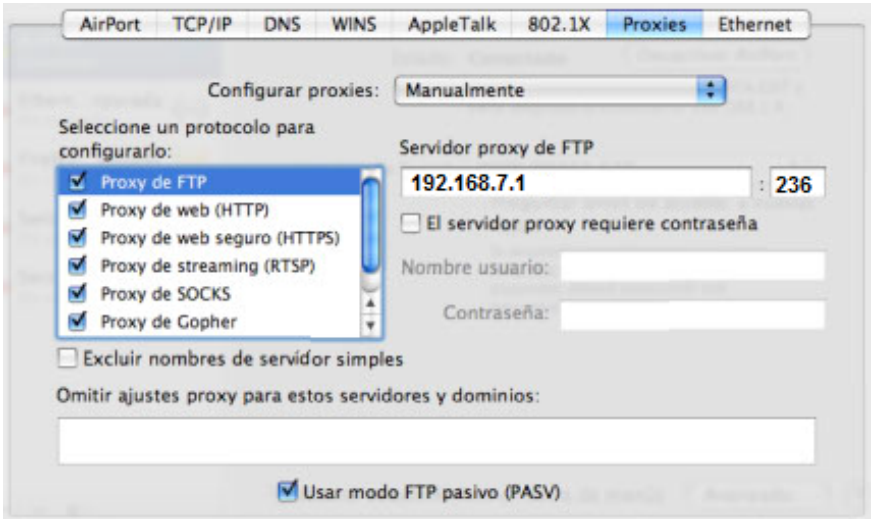
En el cas de Google Chrome cal destacar que, tal com es mostra en la figura 2.5, el navegador utilitza en última instància les finestres d'interacció amb l'usuari del sistema operatiu instal·lat. La imatge ha estat capturada en un sistema operatiu Microsoft Windows.

Configurar servidor intermediari amb Safari

El navegador d'Apple també ofereix la possibilitat de configurar un servidor intermediari. Els passos a seguir són:

1. Seleccioneu el menú *Safari*.
2. Anar a *Preferències*.
3. Activar la pestanya *Avançat*.
4. A *Proxies* fer clic a *Canviar preferències*.
5. A *Configurar Proxies* seleccionar *Configurar manualment*.
6. Activar el quadre de protocol que es necessiti.
7. Indicar l'adreça IP del servidor intermediari i el port que s'utilitzi.
8. Prémer *OK* per guardar la configuració.

FIGURA 2.6. Configuració del servidor intermediari a Safari



El navegador Safari ofereix la possibilitat, igual que Firefox, de configurar diversos servidors intermediaris relacionant-los a diferents protocols. En la figura 2.6 s'assigna al servidor intermediari d'FTP un port diferent de l'usual.

2.3.8 Interpretació i utilització de documentació tècnica

Per considerar que un sistema està operatiu primer cal que passi pels entorns de proves, preproducció i producció. A més, cal generar documentació per poder fer el procés repetible, registrar els procediments associats al servei i establir un sistema de monitoratge perquè les fallades del servei siguin detectades.

Instal·lació i posada en marxa d'un sistema

Des del punt de vista de la seguretat, un sistema ha 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.

> Cal evitar que un entorn de proves estigui exposat a atacs externs per mitjà de la publicació de serveis.

1. **Entorn de proves**. Primer de tot, cal disposar d'un entorn adequat per poder fer les primeres proves de funcionament del sistema. Convé que aquest entorn estigui el més aïllat possible, ja que en aquesta fase no es pot esperar que els serveis estiguin configurats correctament ni que els usuaris hagin de fer servir contrasenyes fortes.

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, cal que el sistema tingui els serveis definitius, configurats correctament, publicats, però amb l'accés limitat. Un cop el sistema està validat, 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.

Documentació del sistema

Per tal d'instal·lar el sistema correctament, cal consultar la documentació del producte. Acostuma a estar en anglès.

L'anglès s'ha convertit en la llengua més utilitzada per a la documentació tècnica.

És habitual 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 del sistema per accedir-hi.

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 programa de font pública que pot funcionar com a sistema gestor del coneixement.

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 balancejos 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 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.

Monitoratge del sistema

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.

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 el més aviat possible.

És important monitorar els serveis per assegurar que es troben dins dels paràmetres del nivell de servei establert (també conegut com a SLA o *Service Level Agreement*).

Disponibilitat del sistema

La disponibilitat del sistema es compta com 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 habitual disposar d'un programa que supervisi els dimonis que hi pugui haver, ja sigui en un clúster o només en un node.

Daemontools és un programa de font pública que reinicia automàticament els dimonis quan s'aturen.

Aquest tipus de supervisió dels dimonis redueix considerablement el temps de caiguda dels serveis, ja que, en alguns casos, el problema se soluciona quan, simplement, el dimoni es torna a posar en funcionament.

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 això passi.

Monit és un programa de font pública dedicat a la gestió de processos i sistemes de fitxers que permet fer tasques de manteniment de manera automàtica: permet configurar monitors reactius.

Realització d'informes d'incidències de seguretat

Quan hi ha un incident de seguretat, cal notificar l'incident als responsables dels sistemes involucrats i procedir amb cautela.

És bastant habitual entrar als equips involucrats i començar a remenar-los sense saber exactament què s'hi busca. D'aquesta manera, es poden destruir pistes que podrien ajudar a entendre què ha passat. Per tant, el primer que s'ha de fer és conservar la calma i seguir les recomanacions 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'han d'intentar reduir els danys. Pot ser que calgui bloquejar l'accés a l'equip o al 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.

L'informe sobre l'incident ha d'incloure els punts següents:

1. Descripció
2. Resum
3. Anàlisi

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 el més aviat possible i de manera ininterrompuda. Per exemple, si la base de dades principal de l'entitat queda fora de línia, caldrà una dedicació total per resoldre-ho.
  - **Moderada**: implica un problema que només ha degradat el servei o n'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 programa, cal aplicar els pedaços adients durant els dies següents.

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 sense coneixements d'informàtica hauria de ser capaç d'entendre què ha passat i quines mesures s'han pres per evitar que l'incident es repeteixi.

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: procediment i metodologia, documentació i annexos.

1) Procediment i metodologia. És important definir com s'ha actuat envers l'incident per 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 les eines necessàries compilades estàticament (sense llibreries del sistema que hagin pogut ser manipulades). Aquests fitxers s'han de transmetre al sistema de 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 el SHA1.

L'MD5 i el SHA1 són dos algorismes que generen un número de longitud fixa, que permet detectar si un fitxer ha estat modificat després de la seva creació.

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.

A continuació, cal obtenir una còpia de totes les dades que puguin aportar alguna pista, com les dades i les metadades en disc. Convé obtenir aquesta informació mitjançant una imatge completa del disc.

Seguidament, es poden investigar els processos del sistema. Així, 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.

2) 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.

Existeixen una sèrie d'ítems que han d'estar sempre presents a la base de dades d'incidències:

- **Incidències detectades**. Finalment, cal destacar la incidència o conjunt d'incidències detectades. Quan s'investiga un incident determinat, no és estrany detectar altres punts d'accés al sistema.
- **Pla d'acció**. Un cop s'ha entès el problema, convé prendre mesures per evitar que es repeteixi en el 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, cal verificar tota la configuració del servei implicat, ja que s'hi podrien detectar altres problemes de configuració.
- **Un error sense pedaç disponible**. Si el problema detectat és un error (*bug*) 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.

- **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. El lliurament 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.

3) 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 el pugui veure.

Un **guió** (*script* en anglès) és una eina present en la majoria de distribucions Linux que permet enregistrar una sessió de consola.

Alta disponibilitat

Alba Batlle Linares

Índex

Introducció **5**

Resultats d'aprenentatge **7**

1 Alta disponibilitat **9**
1.1 L'alta disponibilitat en els sistemes informàtics . . . 9
1.2 Com mesurar l'alta disponibilitat . . . 12
1.3 Solucions d'alta disponibilitat . . . 14
1.3.1 Redundància en el maquinari . . . 14
1.3.2 Redundància de servidors . . . 16
1.3.3 Subministrament elèctric . . . 17
1.3.4 Sistemes d'emmagatzematge redundant . . . 18
1.3.5 Centres de processament secundaris . . . 22
1.3.6 Xarxes i sistemes d'emmagatzematge en xarxa . . . 23
1.3.7 Solucions d'alta disponibilitat en bases de dades . . . 26
1.3.8 Redundància en les comunicacions . . . 27
1.3.9 Repartiment de càrrega . . . 29
1.3.10 Clúster de servidors . . . 29
1.3.11 Plans de contingència . . . 31

2 Virtualització **33**
2.1 Objectius de la virtualització . . . 33
2.2 Virtualització de servidors . . . 35
2.2.1 Virtualització nativa . . . 35
2.2.2 Virtualització allotjada . . . 36
2.2.3 Paravirtualització . . . 37
2.3 Virtualització d'escriptoris . . . 38
2.4 Virtualització d'aplicacions . . . 40
2.5 Eines per a la virtualització . . . 41
2.5.1 Sistemes propietaris . . . 41
2.5.2 Sistemes lliures . . . 42
2.5.3 Maquinari específic per virtualitzar . . . 44
2.6 Configuració i utilització de les màquines virtuals . . . 44
2.7 Migració en calent . . . 45
2.8 Virtualització i alta disponibilitat . . . 46
2.9 Informàtica en núvol . . . 47
2.10 Contenidors . . . 51
2.10.1 Linux Containers . . . 52
2.10.2 Contenidors: Docker . . . 53
2.10.3 Creació i desplegament d'un contenidor amb Docker . . . 54

Introducció

En ple segle XXI hi ha un fet que és clar: la vida no és possible sense la informàtica. Amb el pas dels anys, la informàtica ha anat evolucionant des dels seus orígens en els camps de la investigació i la recerca per anar ficant-se cada cop més en les nostres vides, fins al punt que actualment gairebé totes les accions quotidianes estan relacionades d'alguna manera amb un procés informàtic. D'aquesta manera la informàtica ha deixat de ser una eina tecnològica per desenvolupar unes tasques concretes i s'ha convertit en una necessitat vital. Podem trobar centenars d'exemples al respecte: el món empresarial, on els sistemes d'informació són la clau sobre la qual es construeixen les empreses; les xarxes socials, que ocupen cada dia més hores en el temps d'oci de les persones...

Històricament, la informàtica es centrava a donar resposta a aquestes necessitats, construint solucions tècniques als diferents requeriments que anaven sorgint en la societat. Avui en dia això no és suficient, la dependència dels sistemes informàtics és total. Imaginem-nos que, per exemple, fem una transferència bancària d'un gran import i en aquell moment el sistema informàtic del banc deixa de funcionar. Què passa si s'han perdut les dades de la transacció? On han anat a parar els diners? Les conseqüències de la fallada del servei poden ser fatals. Això ha provocat que s'hagin de buscar solucions destinades a assegurar la continuïtat dels serveis. Així ha aparegut aquesta nova disciplina anomenada *alta disponibilitat*, que s'ocupa d'assegurar que els serveis imprescindibles sempre estiguin operatius, estudiant les causes de les possibles interrupcions i prenent les mesures adequades per evitar-les.

Al llarg del mòdul s'han donat a conèixer mètodes i tècniques de seguretat informàtica per tal d'evitar qualsevol atac als sistemes, garantint tres dels quatre principis bàsics de la seguretat: confidencialitat, fiabilitat i integritat. No obstant, no podem considerar que un sistema informàtic sigui del tot segur si no es pot garantir també la disponibilitat, tema que tractarem en aquesta última unitat formativa.

En l'apartat "Alta disponibilitat" estudiarem en què consisteix, com es mesura i quan es considera que un servei ofereix alta disponibilitat. Aprendrem el concepte de temps d'inactivitat i identificarem les principals causes que poden induir una fallada en els sistemes. A més, analitzarem detalladament les diferents solucions que permeten obtenir un servei continu de manera segura. El motiu pel qual un servei deixa de funcionar pot ser molt variat i imprevisible: un desastre natural com un llamp, terratrèmol o inundació a la seu d'un empresa on s'allotgen els servidors, un error humà en la manipulació dels equips, un mal manteniment, una fallada esporàdica d'un component... Per tant, cal buscar solucions específiques que donin resposta a riscos específics presents en els diferents nivells d'un sistema informàtic. Així, estudiarem les tècniques que s'apliquen per evitar les fallades de maquinari, els errors de programari, les interrupcions al subministrament

elèctric, les condicions climàtiques i una llarga llista de més amenaces que poden afectar al servei. Conceptes com *redundància*, *recuperació* o *independència* seran recurrents en les diferents solucions implementades.

En l'apartat "Virtualització" ens centrarem especialment en una solució específica d'alta disponibilitat: la virtualització. Així veurem de quina manera aquesta tècnica proporciona fiabilitat als sistemes, a més de portar altres avantatges com l'eficiència d'ús dels servidors i el conseqüent estalvi econòmic. Veurem les diferents variants de virtualització segons l'arquitectura implantada i els avantatges i inconvenients de les diferents opcions. També veurem una alternativa a la virtualització actualment en auge i que és més eficient, però té algunes limitacions: la tecnologia dels contenidors.

Al final d'aquesta unitat serem capaços de reconèixer si una solució és adequada o no per a un servei, avaluant no només la capacitat d'executar les funcionalitats necessàries sinó tenint en compte els seus requeriments de continuïtat en el servei i veient les diferents tècniques d'alta disponibilitat aplicades.

Resultats d'aprenentatge

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

1. Implanta solucions d'alta disponibilitat emprant tècniques de virtualització i configurant els entorns de prova.
    - Analitza supòsits i situacions en les quals es fa necessari implementar solucions d'alta disponibilitat.
    - Identifica solucions de maquinari per assegurar la continuïtat en el funcionament d'un sistema.
    - Avalua les possibilitats de la virtualització de sistemes per implementar solucions d'alta disponibilitat.
    - Implanta un servidor redundant que garanteixi la continuïtat de serveis en casos de caiguda del servidor principal.
    - Implanta un sistema de balanç de càrrega a l'entrada de la xarxa interna.
    - Implanta sistemes d'emmagatzematge redundant sobre servidors i dispositius específics.
    - Avalua la utilitat dels sistemes de clústers per augmentar la fiabilitat i productivitat del sistema.
    - Analitza solucions de futur per a un sistema amb demanda creixent.
    - Esquematitza i documenta solucions per a diferents supòsits amb necessitats d'alta disponibilitat.

1. Alta disponibilitat

Quan parlem de seguretat informàtica, estem parlant en definitiva de fiabilitat, confidencialitat, integritat i disponibilitat. Només si aconseguim complir totes aquestes condicions podrem dir que el nostre sistema és segur.

- **Fiabilitat**: funcionament correcte dels sistemes, realitzant les tasques tal com han estat previstes.
- **Confidencialitat**: garantir que l'accés a les dades del sistema està restringit únicament a les persones autoritzades.
- **Integritat**: assegurar que les dades del sistema no han estat manipulades per persones no autoritzades i que per tant no s'han vist alterades.
- **Disponibilitat**: capacitat del sistema per ser accessible i operatiu el màxim de temps possible.

Tan important és garantir una bona seguretat dels sistemes informàtics tot evitant l'entrada de persones alienes i assegurant la qualitat de les dades que s'hi emmagatzemen com que el sistema estigui disponible el màxim de temps possible. No serveix de res tenir un sistema 100% infal·lible si finalment no pot realitzar les tasques per a les quals s'ha creat i no està disponible a l'usuari.

Per tal d'assegurar la qualitat i la disponibilitat de les dades, fa uns anys que ha sorgit un nou concepte a l'hora de dissenyar els sistemes informàtics.

Els sistemes d'**alta disponibilitat** són sistemes informàtics que han estat dissenyats seguint un conjunt de normes i tècniques per tal que el sistema pugui estar disponible sempre o, si més no, el màxim de temps possible.

Aplicacions de l'alta disponibilitat

En els sistemes informàtics no només és important conèixer l'índex de disponibilitat. També hi ha altres tipus de serveis en els quals és interessant conèixer els temps d'inactivitat. El Metro de Barcelona, per exemple, genera estadístiques mensuals sobre el temps de funcionament del seu servei.

Aconseguir que els sistemes informàtics estiguin disponibles sempre és gairebé utòpic, ja que són molts els riscos que s'han de tenir en compte. No obstant això, les empreses preparen els seus sistemes per tal que estiguin disponibles el màxim temps possible.

1.1 L'alta disponibilitat en els sistemes informàtics

Les empreses són cada cop més dependents dels seus sistemes informàtics i, per tant, una aturada en els servidors els pot suposar elevades pèrdues tant econòmiques com materials. Fins i tot en casos extrems podria suposar la pèrdua de vides humanes. És per aquest motiu que cal dissenyar adequadament els

sistemes informàtics de manera que es trobin disponibles en qualsevol moment i que puguin oferir els seus serveis als usuaris de forma continuada.

Per tal que els sistemes informàtics tingui una elevada disponibilitat caldrà implantar solucions de programari i de maquinari. Cal tenir present que la majoria de solucions d'alta disponibilitat comporten uns costos força elevats.

En el procés de disseny cal determinar les necessitats d'alta disponibilitat que tindrà el nostre sistema i fins a quin nivell és necessari implantar aquest tipus de solucions, ja que a vegades per millorar la disponibilitat unes poques hores s'han de fer grans inversions econòmiques. Per exemple, no té associats els mateixos riscos l'aturada dels sistemes d'una torre de control, una entitat bancària o una botiga virtual que la del sistema comptable d'una perruqueria, un taller mecànic o una botiga de queviures.

En funció del tipus de negoci, no cal que els sistemes estiguin disponibles les vint-quatre hores del dia i, per tant, es poden programar aturades per realitzar tasques de manteniment. I en cas que es produeixi una aturada inesperada, sovint no impediran l'activitat econòmica que es desenvolupa.

Fa uns anys, l'alta disponibilitat estava únicament orientada a donar solució als sistemes informàtics de grans empreses. Tanmateix, en els últims anys s'han desenvolupat solucions menys costoses, fet que ha permès la implantació de solucions d'aquest tipus en empreses petites i mitjanes.

Determinades tasques de manteniment que realitzen els administradors (com actualitzacions, canvis de configuració o algunes còpies de seguretat) provoquen que el sistema deixin d'estar operatiu durant uns minuts. Aquest tipus d'aturades és el que s'anomenen *aturades planificades*, ja que els administradors les planifiquen per realitzar en moments que puguin tenir poc impacte en el funcionament de l'empresa. Estan controlades i es coneix per endavant la durada que tindran. Aquest tipus d'accions que generen un temps d'inactivitat s'acostumen a fer per les nits o en cap de setmana per tal d'afectar el mínim nombre d'usuaris, i sempre es notifiquen per endavant.

El **temps d'inactivitat** és el període de temps en què el nostre sistema no està operatiu i, per tant, no pot respondre a les peticions que realitzin els usuaris. En funció de les causes podem diferenciar dos tipus de temps d'inactivitat: **planificat** o **no planificat**.

D'altra banda, es troben els temps d'inactivitat no planificats, els quals poden ser causats per factors diversos. Per tal de poder identificar els possibles causants cal fer una avaluació de riscos. A continuació s'identifiquen alguns dels possibles riscos que caldrà tenir en compte:

- **Fallades de maquinari**: el sistema deixarà d'estar operatiu si es produeix una aturada en algun dels dispositius bàsics del servidor com són la font d'alimentació, el disc dur o bé la memòria.

- **Talls i fluctuacions del subministrament elèctric**: els sistemes informàtics són molt sensibles als canvis en el subministrament elèctric, que poden ser produïts per una fallada en les fonts d'alimentació locals, fluctuacions de tensió (tant pujades com caigudes de tensió) i per acabar, talls totals en el subministrament elèctric.

- **Pèrdua o bloqueig de la informació**: la informació del sistema pot ser inaccessible ja sigui per un atac o bé per una mala gestió dels usuaris.

- **Fallada en la infraestructura de comunicacions**: avui en dia la majoria de sistemes informàtics estan formats per la unió de diferents dispositius en una xarxa comuna. Un tall en la infraestructura de comunicacions suposarà la fallada del sistema complet, tant si es tracta de comunicacions locals com de comunicacions entre centres.

- **Saturació en els servidors de processament de dades**: sovint, el bloqueig del servidor per un volum de dades superior al que és capaç de gestionar pot suposar una caiguda del sistema.

Un cop s'han identificat els possibles riscos, cal dissenyar i implantar solucions d'alta disponibilitat per tal que si algun d'aquests riscos s'acabés manifestant no representés una fallada del funcionament del sistema informàtic.

Per dur a terme un projecte d'implantació d'alta disponibilitat caldrà que seguim les fases de projecte següents:

1. **Coneixement del sistema i identificació de riscos**: primer de tot cal conèixer en detall l'arquitectura del sistema on treballarem. Cal analitzar tots els components, per insignificants que puguin semblar, per poder identificar els dispositius més crítics i que, per tant, tindran un impacte més gran en cas de fallada.

2. **Establiment dels objectius a assolir**: s'han de definir juntament amb l'usuari quins han de ser els nivells de servei a assolir.

3. **Disseny i planificació**: un cop s'han establert els objectius, es buscaran les possibles solucions per donar resposta aquesta demanda. S'analitzaran una a una i s'escollirà la que més s'adeqüi a les nostres necessitats. Finalment, es realitzarà el disseny del nou sistema i es crearà la planificació del projecte.

4. **Implantació**: a partir del disseny realitzat i en base a la planificació elaborada, es procedirà a la implantació de la solució acordada. Cal ser curosos a l'hora d'implantar un sistema d'aquest tipus, de manera que l'usuari no noti canvis en la qualitat del servei.

5. **Mesura**: validar que la solució implantada assoleix els objectius establerts. En el cas que es produeixi alguna desviació es prendran les mesures correctives per tal de poder aconseguir la fita marcada.

6. **Control**: monitorar i controlar el sistema implantat per tal d'assegurar-nos que està treballant dins dels paràmetres establerts. Al llarg dels anys

els sistemes es van actualitzant i van afegint nous dispositius. Cal també controlar que aquestes variacions del disseny inicial no influeixen de manera negativa en el funcionament del sistema.

1.2 Com mesurar l'alta disponibilitat

Per tal de controlar els temps de disponibilitat dels sistemes informàtics s'ha creat una mètrica de càlcul. Aquesta mètrica es vàlida per a tots els sistemes informàtics. Primer de tot cal establir quina hauria de ser la disponibilitat del nostre sistema. És el que s'anomena SLA (*Service Level Agreement*) **acord del nivell de servei**, que en una empresa normal podria rondar entre 8x5 o un 10x5, depenent dels horaris dels treballadors, que garanteix que els sistemes estaran operatius els cinc dies laborables de la setmana dins de l'horari de treball. Hi ha altres tipus de sistemes, però, que necessiten d'una disponibilitat superior, com poden ser les entitats bancàries les quals han de tenir una acord de servei de 24x365, és a dir que es trobin operatius tots els dies de l'any les vint-i-quatre hores del dia. Aquests acords de servei d'alta disponibilitat també poden anomenar-se 24/7, com el seu nom indica els sistemes es trobaran operatius les vint-i-quatre hores del dia tots els dies de la setmana.

SLA

Els SLA (*Service Level Agreement*) o acords del nivell de servei s'acostumen a utilitzar per establir un contracte entre un proveïdor de servei i un client. En aquest contracte s'estableixen els nivells mínims de qualitat en base a diferents aspectes: temps de resposta, disponibilitat horària, personal assignat... Bàsicament, es realitzen contractes d'aquest tipus amb empreses de telecomunicacions i serveis externalitzats.

Un cop s'han determinat les hores de servei de cada sistema podem passar a calcular el total d'hores anuals que el sistema suposadament hauria d'estar operatiu. En el cas de sistemes d'alta disponibilitat, 24 x 365 = 8.760 hores/any. Si coneixem el total de temps d'inactivitat del sistema al llarg de l'any podem calcular el percentatge de disponibilitat aplicant la fórmula matemàticasegüent:

% disponibilitat = ((X – Y) / X) · 100
On X representa el nombre d'hores que el sistema hauria d'estar operatiu en referència a l'acord de nivell de servei de l'empresa i Y representa les hores d'inactivitat del sistema.

És interessant conèixer alguns dels càlculs més habituals d'índex de disponibilitat i temps d'inactivitat.

Exemple de càlcul de l'índex de disponibilitat

El cap d'informàtica d'un hospital ens ha demanat que calculem l'índex de disponibilitat del servidor on es troben emmagatzemats els expedients mèdics de tots els pacients. L'hospital disposa de servei d'urgències, que està obert les vint-i-quatre hores del dia tots els dies de l'any. Perquè els metges del servei puguin consultar els expedients mèdics s'han implantat algunes mesures d'alta disponibilitat, no obstant això, al llarg de l'any el servidor ha tingut un temps d'inactivitat acumulat de 53 minuts i 14 segons. El cap ens comenta que un índex de disponibilitat inferior a un 99,99% seria insuficient per al servidor de l'hospital.

Primer de tot hem d'identificar quin ha de ser el nombre d'hores que el servei hauria d'estar operatiu. En aquest cas hauríem d'aconseguir que el servidor estigués operatiu vint-i-quatre hores durant 365 dies de l'any per tant un total de 24 x 365 = 8.760 hores. Atès que el temps d'inactivitat està indicat en minuts i segons cal passar el temps d'inactivitat tot a hores per poder aplicar la fórmula. 53 min / 60 = 0,88 hores i 14 segons / 3.600 = 0,0038

hores. Per tant, els 53 minuts i 14 segons equivalen a 0,89 hores. Finalment, calculem l'índex de disponibilitat: ((8.760 – 0,89) / 8.760) · 100 = **99,98%**. Podem determinar que les solucions d'alta disponibilitat implantades no són suficients, ja que l'índex de disponibilitat obtingut és inferior a l'esperat.

Exemple de càlcul del temps d'inactivitat

En una gestoria on els treballadors fan un horari laboral de nou del matí a sis de la tarda, el servidor on s'emmagatzemen les dades de comptabilitat té un índex de disponibilitat del 99%. Quin temps d'inactivitat màxim ha acumulat el servidor al llarg de l'any per arribar a aquest índex d'inactivitat?

En aquest tipus d'exercicis, primer de tot s'ha de determinar el nombre d'hores que hauria d'haver estat operatiu el servidor. Com que no es tracta d'un sistema d'alta disponibilitat, el servidor de comptabilitat només hauria d'haver estat operatiu els dies laborables entre les 9 i les 18 h. Atès que en un any hi ha 240 dies laborables i la jornada laboral de la gestoria és de nou hores diàries, al llarg d'un any el sistema hauria d'haver estat operatiu un total de 240 x 9 = 2.160 hores. En aquest cas, a partir de l'índex de disponibilitat s'ha d'esbrinar el temps d'inactivitat. 99% = ((2.160 – t. inactivitat)) / 2.160. S'aïlla de la fórmula el temps d'inactivitat i s'obté un temps de 21,6 hores.

Exemple de relació entre l'índex de disponibilitat i el temps d'inactivitat

En una empresa d'allotjament web disposen actualment d'un índex d'inactivitat del 99%. Han rebut una oferta força interessant econòmicament d'una agència de viatges que opera per Internet. No obstant això, per acabar utilitzant els seus serveis exigeixen un índex de disponibilitat no inferior al 99,99%. Com s'hauria de reduir el temps d'inactivitat per tal que l'agència de viatges accepti allotjar el seu web en el servidor d'aquesta empresa?

En aquest cas, en tractar-se d'una empresa d'allotjament web, els seus servidors han d'estar operatius 24 hores x 365 dies = 8.760 hores/any. Si l'índex de disponibilitat és del 99%, substituint a la fórmula 99% = ((8.760 – t. inactivitat)) / 8.760 s'obté que el màxim temps d'inactivitat actual és de 87,6 hores. Si es millorés l'índex d'inactivitat al 99,99% = ((8.760 – t. inactivitat)) / 8.760 s'obtindria un temps d'inactivitat màxim de 0,876 hores. Per tant, s'haurien d'implantar millores d'alta disponibilitat per reduir el temps d'inactivitat en 87,6 – 0,876 = 86,724 hores.

A la taula 1.1 podeu veure un quadre resum de la relació entre l'índex de disponibilitat i el temps d'inactivitat per any, mes i dia d'un sistema d'alta disponibilitat.

Taula 1.1. Relació entre percentatge de disponibilitat i temps d'inactivitat per any, mes i dia d'un sistema 24x365

Disponibilitat	Temps inactiu/any	Temps inactiu/mes	Temps inactiu/dia
90%	36,5 d	73 h	2,4 h
95%	18,3 d	36,5 h	1,2 h
98%	7,3 d	14,6 h	28,8 min
99%	3,65 d	7,3 h	14,6 min
99,9%	8,8 h	43,8 min	1,46 min
99,99%	52,6 min	4,4 min	8,8 s
99,999%	5,3 min	26,3 s	0,9 s
99,9999%	31,5 s	2,6 s	0,08 s

Com es pot apreciar en la taula 1.1, per cada increment de disponibilitat, el temps d'inactivitat es redueix de manera significativa. D'altra banda, cal analitzar els costos associats que comporta una millora d'aquest tipus, ja que passar d'una

disponibilitat del 99% a una del 99,99% pot suposar duplicar el pressupost. Fins i tot se sol dir que per cada 9 que millorem en disponibilitat hauríem d'afegir un 0 en el pressupost.

Per aquest motiu és important establir una relació entre les millores econòmiques que ens suposarà augmentar la disponibilitat del nostre sistema i els costos que això comporta. A més, no totes les empreses necessiten tenir una disponibilitat del 99,999%. Només ho necessiten entitats bancàries, sistema de pagament amb targeta de crèdit de grans magatzems, botigues virtuals o torres de control, entre d'altres.

Tanmateix, és important que els administradors sàpiguen interpretar aquests resultats i que per analitzar la disponibilitat i fiabilitat dels seus sistemes no es basin únicament en aquests indicadors, ja que de vegades poden no ser del tot representatius. Per exemple ens podríem trobar amb un sistema amb una disponibilitat del 99,99%, que, tot i estar operatiu, presenta problemes de rendiment i no ofereix un bon servei als seus usuaris. Per tant, cal valorar també el tipus de servei que s'està oferint, no només els temps d'activitat dels dispositius. És per aquest motiu que cal també monitorar els serveis que ofereixen les nostres màquines.

1.3 Solucions d'alta disponibilitat

Un cop s'han identificat els possibles riscos als quals pot estar sotmès un sistema informàtic s'han d'implantar les solucions adients per evitar o mitigar el seu impacte. Les empreses que necessitin garantir una major disponibilitat dels seus serveis hauran d'incrementar les inversions en aquest àmbit per tal de cobrir totes les possibles circumstàncies.

Podem trobar solucions de tot tipus, des de redundància en els dispositius de maquinari a redundància en les comunicacions, passant per centres de processament de dades secundaris i plans de contingència.

1.3.1 Redundància en el maquinari

Un dels riscos que en cas de manifestar-se pot comportar uns majors temps d'inactivitat són les fallades en el maquinari. Si no han estat previstes, aquest tipus de fallades poden deixar el sistema totalment inoperatiu durant hores i fins i tot dies. Tots els elements del maquinari poden deixar de funcionar en un moment determinat, no obstant això, cal identificar quins són més crítics per a la continuïtat del funcionament del nostre sistema. Aquests són, bàsicament, les fonts d'alimentació, els discos durs i la memòria.

Per poder dimensionar adequadament la solució que més ens convé, cal conèixer les dades de fiabilitat dels diferents components que formen un servidor. Normalment, els fabricants d'equips electrònics aporten entre altres dades tècniques l'anomenat MTBF (de l'anglès *mean time between failures*), que és el temps mitjà entre fallades expressat en hores. Es tracta d'una dada estadística obtinguda a partir de proves de laboratori i dels resultats obtinguts de l'experiència amb els components electrònics més elementals, com poden ser els xips, els busos, les resistències... L'MTBF correspon exactament a la probabilitat inversa de fallada d'un sistema. Cal tenir present que varia segons els tipus de dispositius, el fabricants i les gammes de productes. A continuació s'indiquen alguns exemples d'MTBF:

- Disc dur: 10.000-20.000 hores
- Mòdem: 20.000-30.000 hores
- Ordinador personal: 1.000-5.000 hores
- Impressora: 2.000-4.000 hores

Normalment els valors de MTBF no són constants en el temps, sinó que es poden dividir en tres etapes ben diferenciades:

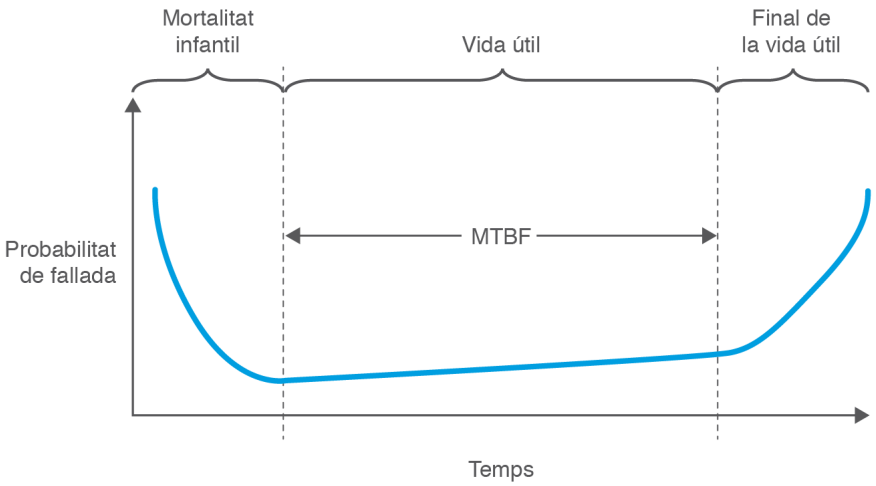
1. **Mortalitat infantil**: es considera que el primer any de vida d'un dispositiu és el període en què poden aparèixer més fallades. El motiu és clar: si hi ha hagut errors en la fabricació, males condiciones en l'emmagatzematge, defectes en els materials emprats per al muntatge o un tractament deficient en les manipulacions, és a l'inici del seu ús on aquests es manifestaran i causaran un mal funcionament.

2. **Vida útil**: passat un any sense fallades, es considera que un dispositiu entra en la seva vida útil i la probabilitat que falli passa a ser l'MTBF indicat pel fabricant, sempre i quan el dispositiu treballi en les condicions necessàries de temperatura, humitat, vibracions... recomanades pel fabricant.

3. **Final de la vida útil**: finalment, passat uns anys es considera que els components s'han degradat degut a l'ús, a la temperatura... i la probabilitat que fallin augmenta considerablement.

En a la figura 1.1 es mostra la fiabilitat d'un dispositiu en el temps, amb les tres etapes diferenciades.

FIGURA 1.1. Evolució de la probabilitat de fallada en el temps



Així, a l'hora de dissenyar els plans per aconseguir una alta disponibilitat en els dispositius de maquinari cal analitzar degudament les dades que aporta el fabricant. En funció d'aquesta anàlisi es pot determinar quines parts del sistema és necessari redundar, que és la principal solució per assegurar l'alta disponibilitat, ja que permet reduir la probabilitat de fallada per dos o, el que és el mateix, duplicar el valor de l'MTBF.

Exemple de càlcul del MTBF

Tenim un servidor que segons el fabricant té una probabilitat de fallada de 1×10^{-4}. Per tant, el seu MTBF és: 1 / Probabilitat de fallada = 10.000 hores de vida útil. Aquest valor indica que estadísticament el servidor fallarà cada 416 dies.

L'empresa considera que aquest valor és massa baix i que necessita una disponibilitat més elevada. Per això decideix redundar el dispositiu completament i que dos servidors treballin en paral·lel. D'aquesta manera, la fallada del sistema global només es produirà quan fallin els dos servidors a la vegada.

Per tant, P (sistema) = P (fallada servidor 1) · P (fallada servidor 2) = 10^{-8}.

L'MTBF serà de 100.000.000 hores: la disponibilitat global del sistema ha augmentat de manera significativa.

1.3.2 Redundància de servidors

Atès que en un servidor hi ha diversos components que poden deixar de funcionar i, en conseqüència, impedir al sistema oferir un nivell de servei adequat, s'acostuma a duplicar el servidor sencer. D'aquesta manera, sigui quin sigui el component que ha deixat de funcionar podem garantir un nivell de servei semblant al que s'ofereix en el servidor principal.

Es pot classificar la redundància de servidors en funció de la capacitat de resposta en cas de fallada:

- **Redundància en calent**: es tracta de dos servidors idèntics sincronitzats que treballen en paral·lel, però dels quals només un respon a les peticions del sistema. Disposen d'un programari de supervisió mútua. En cas que el servidor que està responent en aquell moment entri en fallada, el servidor en espera prendrà el relleu en un temps suficient perquè el servei no es vegi afectat, habitualment de l'ordre de pocs mil·lisegons.
- **Redundància intermèdia**: es tracta de dos servidors, un de principal que respon a les peticions del sistema i un de secundari que no està sincronitzat en temps real. El servidor secundari s'actualitza cada cert període de temps prèviament establert, per exemple un cop al dia o un cop per setmana. En cas de fallada es produeix una aturada en el servei, perquè el servidor secundari s'ha d'actualitzar amb les dades del sistema principal. Aquest tipus d'aturades poden durant entre pocs minuts i algunes hores.
- **Redundància freda**: es tracta de dos servidors, un de principal que respon a les peticions del sistema i un de secundari amb característiques semblants, però que no està operatiu. En cas de fallada s'hauria d'iniciar el servidor secundari, instal·lar el programari actualitzat i fer un bolcat de les dades. L'activació d'un sistema d'aquest tipus acostuma a requerir algunes hores i fins i tot algun dia.

1.3.3 Subministrament elèctric

Tan important és preveure arquitectures i solucions d'alta disponibilitat del maquinari com dels sistemes de subministrament elèctric. Sense una bona infraestructura que permeti l'alimentació ininterrompuda dels nostres sistemes és impossible assegurar una alta disponibilitat global.

Els talls en el subministrament elèctric poden produir-se per motius diversos. A continuació s'enumeren algunes de les fallades elèctriques que poden originar problemes en el funcionament d'un sistema informàtic:

- Talls en el subministrament elèctric de la companyia proveïdora de servei.
- Fallades elèctriques dins de la instal·lació de l'empresa a causa de curtcircuits, derivacions…
- Avaria d'un dispositiu elèctric com el transformador, la font d'alimentació…

Per tenir un sistema robust i obtenir el nivell de protecció adequat contra aquestes amenaces es poden utilitzar les solucions següents:

- **Redundància en el subministrament**: es recomana la contractació de dues línies de subministrament elèctric a dos proveïdors de serveis diferents. En el cas que això no sigui possible es recomana disposar de dues connexions

provinents de dues estacions transformadores diferents, d'aquesta manera la caiguda d'una part de la xarxa elèctrica no afectarà el funcionament de la empresa.

- **Arquitectura elèctrica redundada**: dins de l'arquitectura elèctrica de l'empresa es connectaran dues línies d'alimentació per a cada equip crític. Aquestes línies hauran de ser independents, amb protecció diferencial i magnetotèrmica independent. D'aquesta manera, si un dispositiu falla i fa disparar la protecció de capçalera, els altres dispositius no es veuran afectats. Per exemple, en dos servidors redundants s'hauria de disposar de dues línies independents per a cadascun d'ells.

- **Sistema d'alimentació ininterrompuda (SAI)**: aquest dispositiu serveix per estabilitzar la tensió d'entrada, evitar pics i microtalls. A més, aquests sistemes ofereixen protecció contra talls en els subministrament elèctric oferint a partir de bateries l'autonomia necessària per continuar amb l'activitat de l'empresa o per a l'apagament controlat dels sistemes. En casos en què es necessiti un nivell de disponibilitat molt elevat, es col·loquen dos SAI en paral·lel (no deixa de ser un dispositiu que també pot fallar).

- **Redundància de dispositius**: per acabar, també es poden produir fallades en les fonts d'alimentació dels mateixos equips. És per aquest motiu que molts fabricants ja ofereixen servidors amb dues fonts d'alimentació. Tanmateix, redundar totes les fonts d'alimentació de tots els servidors crítics pot suposar un cost massa elevat per a segons quina empresa. Com a alternativa existeixen els clústers d'alimentació (n+1). Aquests clústers estan formats per n fonts d'alimentació connectades en paral·lel que disposen de la potència necessària per a tota la instal·lació més una font addicional per si alguna fallés.

1.3.4 Sistemes d'emmagatzematge redundant

Per garantir el bon funcionament d'un sistema informàtic és important que la informació estigui sempre disponible o bé que en cas de fallada es pugui recuperar quan es necessiti sense que els usuaris se n'assabentin.

Tot i que els discos tenen cada vegada una capacitat més gran i són més fiables, continuen sent un dels principals punts dèbils dels sistemes informàtics. La tecnologia RAID (*Redundant Array of Independent Disks* o conjunt redundant de discos independents) ens permet assolir alts graus de fiabilitat en l'emmagatzematge de la informació.

Un **RAID** és un sistema d'emmagatzematge d'informació que permet combinar dos o més discos d'igual capacitat perquè siguin tractats pel sistema com una única unitat lògica. La informació es divideix i es replica, de manera que s'ofereixen diferents nivells de tolerància a fallades.

Els esquemes RAID poden ser gestionats per:

- **Maquinari**: en aquest cas es necessita una controladora RAID específica que permet alleugerir la càrrega del processador. Aplicant una solució de maquinari obtindrem una tolerància més alta a fallades i millorarem el rendiment de lectura i escriptura als discos. No obstant això, en afegir la controladora RAID també estem afegint un possible nou punt de fallada.
- **Programari**: el mateix sistema operatiu és l'encarregat de gestionar els discos i, per tant, el rendiment del sistema es veu afectat, ja que part del processador ha d'estar dedicat a aquesta gestió.

Com s'ha indicat, les arquitectures RAID gestionades per maquinari ofereixen un millor rendiment. A més, aquest tipus de solucions acostumen a admetre substitucions en calent (*hot swapping*), és a dir, permeten que els discos puguin ser substituïts sense necessitat d'aturar el sistema.

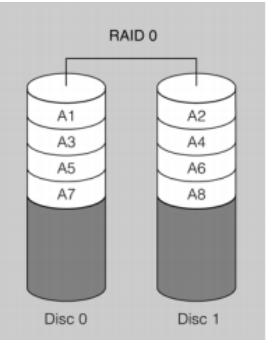
A continuació es detallen els esquemes RAID més comuns.

RAID 0

El RAID 0, també anomenat *stripping*, distribueix equitativament la informació entre els diferents discos durs, de manera que la capacitat de la unitat lògica és la suma de les capacitats dels discos que la formen. De tots els esquemes RAID, aquest és l'únic que no proporciona tolerància a fallades: si un dels discos del RAID falla es perden totes les dades.

Com podem veure en la figura 1.2, les dades es divideixen en petits blocs que es van emmagatzemant de forma alternada entre els diferents discos que formen el RAID. Aquesta manera d'emmagatzemar la informació permet que les lectures i escriptures en el disc puguin ser simultànies, la qual cosa augmenta la velocitat de transferència.

Figura 1.2. Distribució de la informació en un sistema RAID 0



Aquest esquema s'acostuma a utilitzar per millorar el rendiment en entorns on les dades no són crítiques, ja que una fallada en un dels disc suposaria la pèrdua total de la informació.

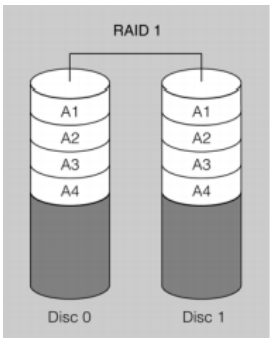
RAID 1

El RAID 1, també anomenat *mirror*, està format per la unió de dos o més disc durs. La capacitat de la unitat lògica correspon a la capacitat del disc més petit. En aquest esquema totes les dades es dupliquen en cadascun dels discos, d'aquesta manera si algun falla es poden recuperar totes les dades sempre que quedi un disc operatiu (figura 1.3).

El RAID 1 ens proporciona un bon nivell de tolerància a fallades, però empitjora l'eficiència pel que fa a l'emmagatzematge disponible, ja que es necessita el doble d'espai per emmagatzemar una informació determinada. La velocitat de lectura i escriptura és semblant a la que podem aconseguir en un sol disc.

Aquest tipus de solucions és recomanable per a empreses petites que volen aconseguir seguretat en l'emmagatzematge de dades sense fer una gran inversió.

FIGURA 1.3. Distribució de la informació en un sistema RAID 1



RAID 5

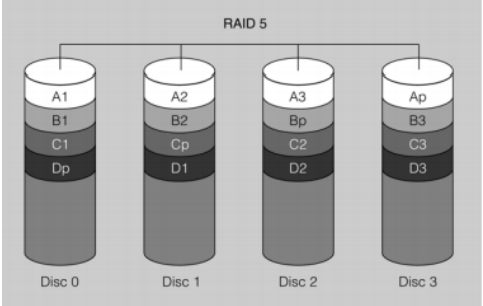
El RAID 5, també conegut com a *stripping amb paritat*, necessita un mínim de tres discos per poder-se implantar. La capacitat d'emmagatzematge de la unitat lògica correspon a la suma de les capacitats de tots els seus discos menys un.

Codis de paritat

Serveixen per detectar i corregir errors en les transmissions de dades. S'incorpora un conjunt de bits calculats a partir d'un algorisme al final del missatge original per tal que el receptor pugui verificar que les dades són correctes.

Tal com s'observa en la figura 1.4, la informació es divideix en petits blocs que es van emmagatzemant alternativament entre els diferents discos. S'introdueixen codis de paritat distribuïts entre els diferents discos per tal de garantir la recuperació de les dades. En el cas de que un dels discos falli es podrà recuperar la informació a partir de les dades emmagatzemades en la resta de discos i els codis de paritat.

FIGURA 1.4. Distribució de la informació en un sistema RAID 5



El RAID 5 ha aconseguit una gran popularitat, perquè ofereix redundància de dades a un cost baix.

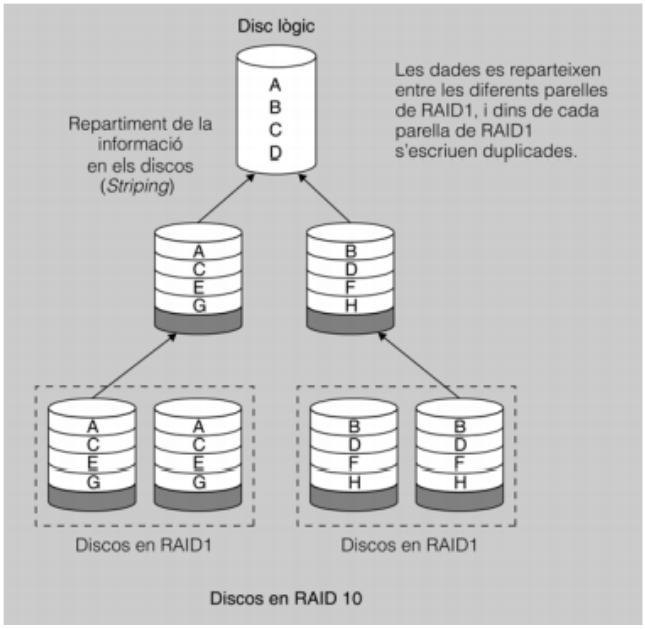
RAID 1+0

Algunes targetes controladores RAID permeten niar diferents esquemes RAID, de manera que ens podem beneficiar dels avantatges que ofereix cadascun. El RAID 1+0 és una combinació d'aquest tipus. Consisteix, concretament, a unir discos amb un RAID 1 com si es tractessin de discos físics en un RAID 0. D'aquesta manera, aconseguim la velocitat en els accessos que ens ofereix el RAID 0 en permetre accessos simultanis i la redundància que ens ofereixen els esquemes RAID 1.

Aquesta combinació es podria també realitzar a la inversa creant un RAID 0+1, però no és recomanable fer-ho, ja que en cas de fallada s'haurien de recuperar més discos.

Com es pot observar en la figura 1.5, per implementar una solució d'aquest tipus són necessaris quatre discos com a mínim, fet que incrementa notablement el cost de la solució.

Figura 1.5. Distribució de la informació en un sistema RAID 1+0



1.3.5 Centres de processament secundaris

Un centre de processament de dades (CPD) secundari està especialment dissenyat per entrar en funcionament quan per qualsevol contingència el centre principal deixa d'estar operatiu. Els costos d'adquisició i manteniment d'un CPD secundari són molt elevats. És per aquest motiu que només són recomanables per a empreses molt grans que requereixin d'una disponibilitat total.

Les característiques tècniques del CPD secundari han de ser les mateixes o molt semblants a les del CPD principal, ja que en cas que entri en funcionament haurà de poder oferir el mateix nivell de servei. A més, caldrà que compleixi amb les mateixes mesures de seguretat tant pel que fa a seguretat física com a la lògica per garantir la integritat de les dades. Es recomana ubicar el servidor secundari a uns 30 o 50 quilòmetres de distància del principal per evitar que els dos CPD es puguin veure compromesos en un mateix desastre natural. A l'hora de triar la ubicació, cal tenir present que quanta més distància hi hagi entre els dos CPD més retard hi haurà en les transmissions de dades i que, per tant, es pot produir un petit decalatge.

Les actualitzacions de dades entre els dos CPD poden ser de dos tipus:

- **Síncrones**: el CPD secundari rep en temps real els canvis que es produeixen en el CPD principal i manté en tot moment una còpia exacta de les dades. En el cas que es produeixi una emergència i entri en funcionament, podrà fer-se càrrec del servei amb la garantia de disposar de totes les dades actualitzades.
- **Asíncrones**: les actualitzacions no es fan en temps real sinó per lots. Per exemple, es poden fer còpies diàries per la nit al CPD principal i restaurar-les al CPD secundari el matí següent. En el cas que el centre secundari entri en funcionament s'ha de tenir present el possible decalatge temporal i actuar amb conseqüència.

En definitiva, sempre és més fiable un centre de processament de dades secundari amb actualitzacions síncrones que un amb actualitzacions asíncrones, perquè en cas de caiguda podrà disposar de tota la informació, mentre que en el que fa actualitzacions asíncrones podem tenir una pèrdua irrecuperable d'informació. D'altra banda, la implementació d'un sistema síncron és molt més cara que la d'un asíncron, ja que s'han d'establir canals de comunicació entre el centre principal i el secundari amb prou capacitat per enviar un gran volum de dades a temps real. A més, aquests costos es disparen com més gran sigui la distància entre els dos centres.

Els CPD secundaris amb actualitzacions asíncrones poden ser una bona solució per a empreses grans que no requereixin una disponibilitat total. Són més econòmics i no necessiten una infraestructura de telecomunicacions tan costosa.

Un altre aspecte a tenir en compte és com es realitzarà entre els dos centres la commutació de serveis. Aquest fet dependrà molt del tipus de servei que es vulgui

traslladar. Pel que fa als sistemes síncrons, la commutació de serveis acostuma a ser senzilla i ràpida, semblant a commutar equips redundants dins d'un mateix CPD. Pel que fa als centres asíncrons, acostuma a ser més complicada i menys automatitzada. Sovint es necessita fer una posada a punt del CPD i realitzar una restauració de les dades, fet que pot provocar temps d'ineficiència en el sistema.

1.3.6 Xarxes i sistemes d'emmagatzematge en xarxa

Les empreses generen un volum de dades cada cop més gran i fer una gestió eficient d'aquesta informació és cada cop més complicat. A més, els usuaris necessiten que les dades es trobin disponibles en tot moment des de diferents plataformes i dispositius. Amb aquest objectiu s'han desenvolupat dues solucions d'emmagatzematge en xarxa: el NAS (sistema d'emmagatzematge en xarxa) i el SAN (xarxa d'emmagatzematge).

Sistema d'emmagatzematge en xarxa (NAS)

Els sistemes d'emmagatzematge en xarxa o NAS (en anglès *Network-Attached Storage*) estan compostos per dispositius d'emmagatzematge que es connecten directament a la xarxa corporativa i permeten compartir les dades amb tots els usuaris de l'empresa (figura 1.6).

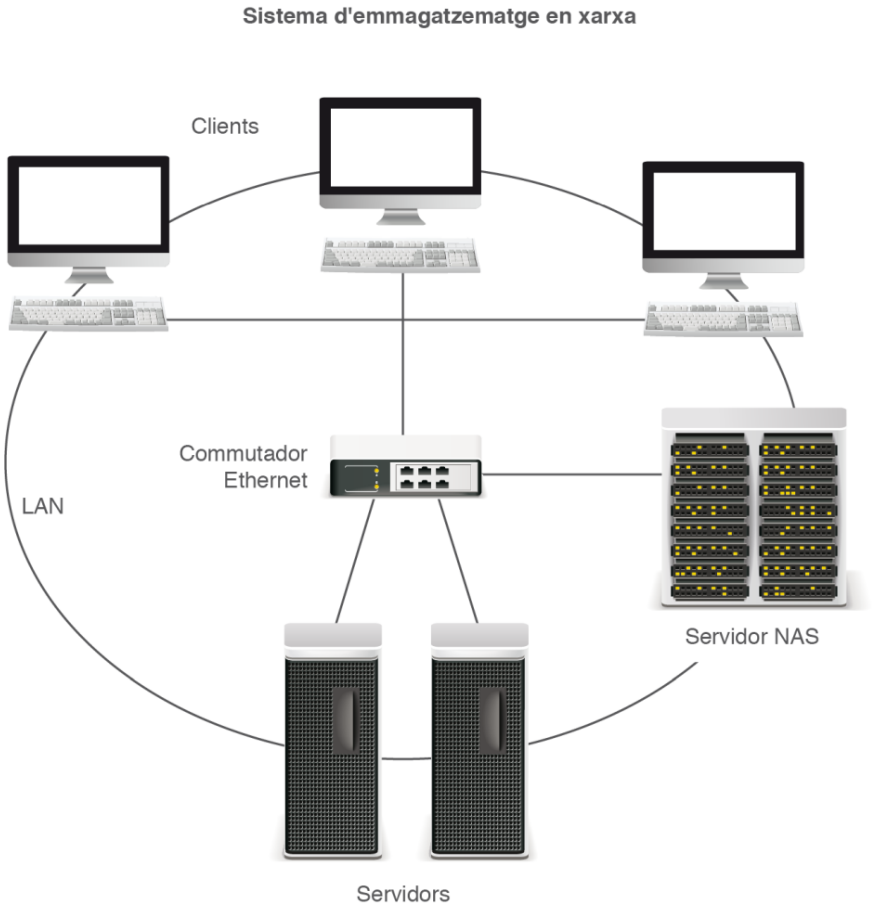
Els servidors NAS disposen d'un maquinari específic per traduir els diferents sistemes de fitxers, des del qual els usuaris poden accedir als dispositius d'emmagatzematge. Internament, els dispositius d'emmagatzematge tenen implantats esquemes RAID, la qual cosa els proporciona un bon rendiment i una alta tolerància a fallades. Podem afirmar que les dades estan protegides, ja que estan centralitzades en el sistema NAS, que té una estructura d'alta disponibilitat.

Per accedir a la informació emmagatzemada en un sistema NAS, s'han de fer servir les funcions del sistema de fitxers del mateix sistema operatiu. Així, les lectures de dades es realitzen a nivell de fitxers i no a nivell de blocs, com es fa habitualment en un sistema d'emmagatzematge local. Això fa que les consultes en el sistema NAS siguin més lentes que en un sistema d'emmagatzematge natiu, fet que pot provocar retards en sistemes que treballin a temps real, tot i que pot ser una molt bona solució per a empreses que no requereixin un temps de resposta tan ràpid.

Els sistemes NAS són fàcils d'instal·lar i d'administrar. A més, en els últims anys han baixat molt de preu i avui en dia són assequibles per a qualsevol empresa i fins i tot per a usuaris particulars.

Els protocols que utilitzen aquests sistemes són el CIFS, l'NFS i l'SMB. Fins i tot podem trobar distribucions de programari lliure que ofereixen serveis NAS, com FreeNas, NASLite i Openfiler, entre d'altres.

FIGURA 1.6. Arquitectura d'un sistema d'emmagatzematge en xarxa

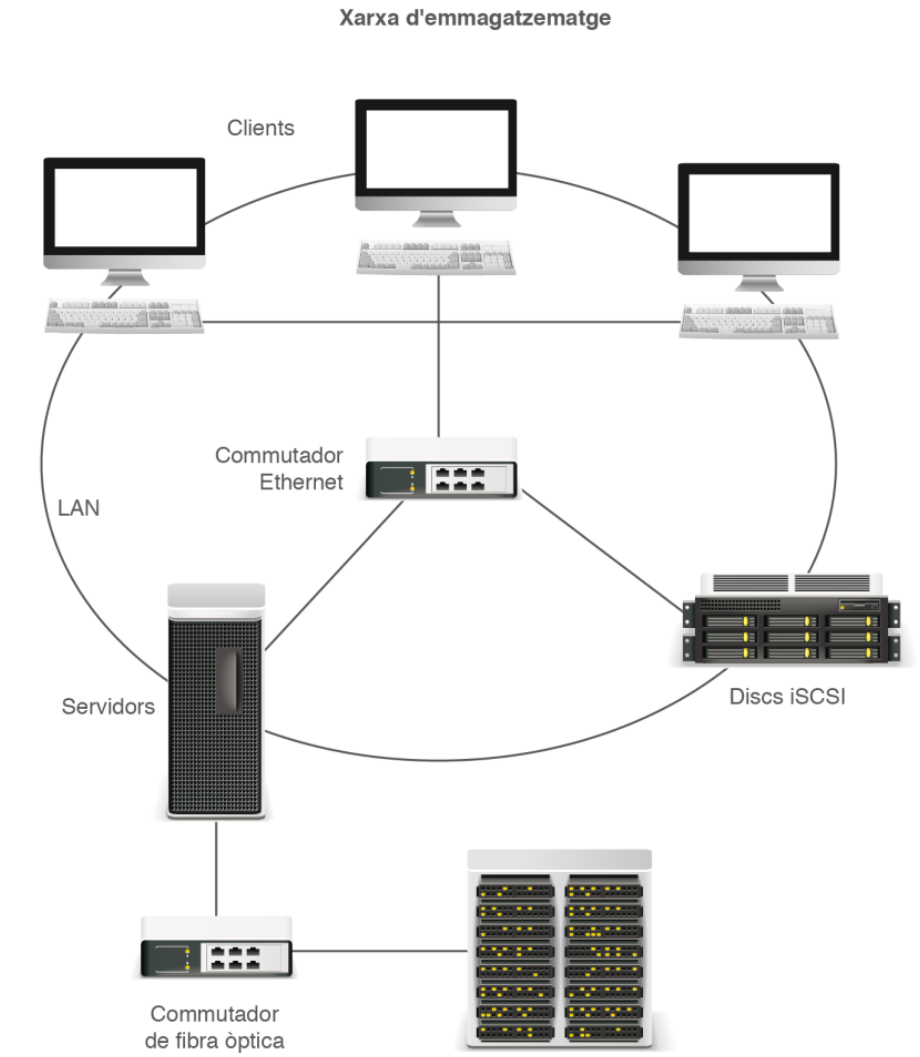


Xarxa d'emmagatzematge (SAN)

En les xarxes d'emmagatzematge o SAN (en anglès, *Storage Area Network*), els dispositius d'emmagatzematge estan connectats directament a una xarxa d'alta velocitat i els usuaris els poden gestionar des del seu sistema operatiu com si hi estiguessin connectats de forma local (figura 1.7).

Els dispositius d'emmagatzematge i els servidors estan connectats a la xarxa mitjançant fibra òptica o iSCSI, que garanteixen rapidesa i fiabilitat en les seves connexions. La fibra òptica proporciona més velocitat. Això no obstant, les targetes i els commutadors de fibra òptica són molt cars. És per aquest motiu que avui en dia la majoria de xarxes SAN utilitzen el protocol iSCSI, ja que les peticions SCSI s'envien pel protocol TCP/IP, sense necessitat d'instal·lar fibra òptica. No són tan ràpides, però permeten reduir costos.

Figura 1.7. Arquitectura d'una xarxa d'emmagatzematge



De tota manera, aquest tipus d'infraestructures són molt costoses i, per tant, només són assequibles per a empreses molt grans.

A diferència dels sistemes NAS, les xarxes SAN no estan orientades a fitxers, sinó a blocs, igual que els sistemes d'emmagatzematge local. D'aquesta manera, els accessos són molt més ràpids, la qual cosa en fa una bona solució per a sistemes a temps real.

Un dels avantatges de les xarxes SAN és que en tenir una connectivitat més alta, els servidors i els dispositius d'emmagatzematge poden estar-hi connectats més d'una vegada i, per tant, creen d'aquesta manera canals redundants, fet que n'augmenta la tolerància davant de fallades.

1.3.7 Solucions d'alta disponibilitat en bases de dades

Avui en dia les empreses treballen amb volums de dades molt grans i la tendència ens indica que en el futur encara s'emmagatzemaran més dades. Ara mateix, les empreses ja no mantenen únicament un llistat dels clients, sinó que acostumen a emmagatzemar altra informació rellevant com: els seus hàbits, aficions, llistat de compres realitzades... Amb tota aquesta informació es poden crear perfils de compres genèrics i individuals, d'aquesta manera l'empresa pot avançar-se a les tendències del mercat i realitzar campanyes publicitàries personalitzades.

Per facilitar les tasques de gestió i administració de les dades, aquesta informació es troba emmagatzemada en bases de dades que disposen de les eines necessàries per poder-ne fer una gestió eficient.

En els últims anys s'ha incrementat en el món empresarial l'ús del programari de gestió ERP (*Enterprise Resource Planning*), que ha fomentat la creació de grans bases de dades on se centralitza tota la informació de l'empresa. Aquest tipus de bases de dades acostuma a estar força exposat a fallades, ja que gestiona un volum de peticions molt elevat i això pot causar errors o caigudes del sistema. Per a moltes empreses, especialment les que tenen negocis molt dependents dels sistemes d'informació, com els bancs, una caiguda de la base de dades pot suposar pèrdues econòmiques importants. Per això les hem d'identificar com un dels punts més crítics del sistema.

La millor manera de reduir el nombre d'errors i fallades en una base de dades és disposar d'un bon disseny inicial que permeti una escalabilitat posterior. També cal que les aplicacions que treballen amb la base de dades realitzin només les peticions indispensables per obtenir la informació que necessiten.

En qualsevol cas, un bon disseny no garanteix que no tinguem cap tipus de fallada o caiguda del sistema. Per això cal que protegim les bases de dades amb sistemes d'alta disponibilitat. El sistema més habitual és disposar de la base de dades de producció, anomenada també *principal* o *primària*, i una base de dades secundària rèplica exacta de la primària. La base de dades replicada entrarà en funcionament quan es produeixi una fallada en la base de dades de producció o quan es realitzi alguna actualització. Per tal de millorar-ne la disponibilitat és recomanable que les dues bases de dades es trobin ubicades físicament en servidors diferents; així augmentarem la disponibilitat en cas d'una caiguda del servidor.

La còpia d'informació entre les dues bases de dades es pot fer de forma síncrona o asíncrona:

- **Síncrona**: en cada transacció que suposa una modificació de la base de dades es copien de manera automàtica tots els canvis a la base de dades secundària i no es dóna la transacció per acabada fins que no s'ha realitzat la modificació en ambdues bases de dades. Aquest mètode empitjora lleugerament el rendiment de la base de dades, ja que les transaccions són més llargues.

- **Asíncrona**: en aquest cas es potencia més el rendiment de la base de dades que la qualitat de les dades en cas de fallada. Es dóna per vàlida la transacció un cop s'han guardat els canvis a producció i es retarda lleugerament la còpia de dades al servidor secundari. Això pot generar petites diferències amb la base de dades original en el cas que s'hagi de restaurar.

Com que els sistemes síncrons tenen la informació actualitzada permeten fer una commutació automàtica de les bases de dades sense riscos. D'aquesta manera, si es produís una caiguda o errada en la base de dades principal, els sistemes de la empresa podrien funcionar amb normalitat amb la base de dades secundaria, sense que els seus usuaris se n'assabentessin.

D'altra banda, quan es produeix una fallada en la base de dades principal d'un sistema asíncron s'ha de forçar la commutació, fet que pot generar pèrdues de dades, ja que la base de dades secundària pot no trobar-se del tot actualitzada en el moment del canvi.

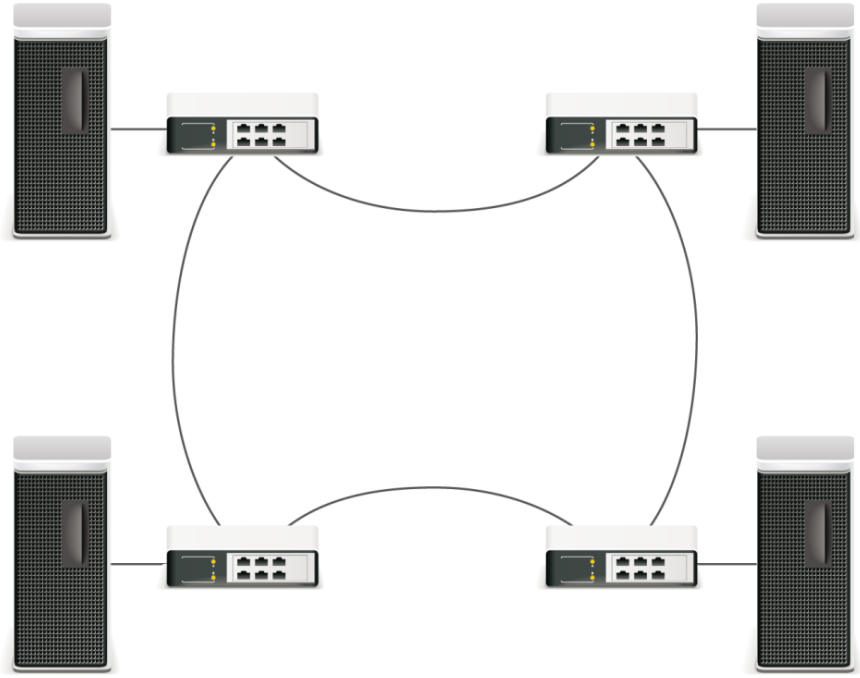
Els principals proveïdors de bases de dades ja ofereixen solucions asíncrones i de commutació automàtica de les dades. És el cas de Data Guard d'Oracle i l'AlwaysOn d'SQL Servers.

1.3.8 Redundància en les comunicacions

Les comunicacions no són menys importants que les bases de dades. No serveix de res tenir un servidor amb una disponibilitat del 100% si els clients no s'hi poden connectar. Per garantir aquesta connectivitat entre servidors i clients, la majoria de servidors disposen de dues targetes de xarxa. Així els serveis no es veuen afectats en cas de fallada. Tanmateix, el servidor pot treballar amb es dues targetes de xarxa com si fossin una de sola, sumant les seves capacitats i millorant el seu rendiment.

Tant si les comunicacions són internes com externes hi intervenen molts dispositius de xarxa (encaminadors, commutadors, concentradors...). La caiguda de qualsevol d'aquests dispositius pot suposar la caiguda del servei. És important redundar la majoria d'aquests dispositius en les xarxes internes de l'empresa perquè una caiguda no afecti a les comunicacions i, en definitiva, al servei ofert. A part dels dispositius de la xarxa també és important replicar els canals de connexió entre els principals dispositius per tal d'evitar que un tall en el canal provoqui la caiguda del sistema. Per això s'acostuma a construir les xarxes amb una arquitectura d'anell, de manera que la caiguda d'un canal entre dos nodes, per exemple per un tall accidental en una fibra òptica, no afecti a les comunicacions del sistema i tots els dispositius puguin seguir estant connectats entre sí i treballar amb total normalitat (figura 1.8).

FIGURA 1.8. Estructura d'una connexió en anell



Una xarxa en anell, però, pot originar alguns problemes en la selecció de rutes per part dels protocols i crear situacions de bucles infinits dins de la xarxa, en els quals els paquets es vagin enviant entre els dispositius de xarxa sense arribar mai a la seva destinació. Per això cal utilitzar protocols que permetin la resolució d'aquests problemes, com fa el protocol Ethernet amb la seva funcionalitat *Spanning Tree* (STP). Aquesta funcionalitat detecta automàticament en una xarxa quan s'ha creat un anell de redundància entre els dispositius, desactiva un dels enllaços entre els nodes de comunicació de manera automàtica i evita així la formació de bucles. Davant d'una fallada en un enllaç, l'STP activa l'enllaç que havia desactivat virtualment per evitar l'aparició de bucles i desactiva l'enllaç que ha caigut realment.

La majoria d'empreses disposen avui d'una xarxa d'oficines connectades entre elles per compartir recursos i dades. Tot i disposar d'una xarxa de comunicacions interna d'alta disponibilitat, aquestes comunicacions entre centres requereixen l'ús de xarxes de telecomunicacions públiques, com per exemple Internet. Així, doncs, els proveïdors de serveis passen a ser un dels punts més crítics del sistema. Una caiguda del proveïdor de servei d'Internet suposa unes pèrdues econòmiques significatives per a la empresa. No només es perden les comunicacions entre les diferents seus, sinó que també deixen d'estar disponibles altres serveis imprescindibles per al bon funcionament de la companyia com el correu electrònic, el web, es perden comunicacions amb els clients... a més que es pot generar la desconfiança de clients potencials.

Per garantir un bon accés a Internet i evitar tots aquests problemes, les empreses opten per contractar dues línies de comunicacions amb diferents proveïdors. Encara es millorarà més la disponibilitat si es contracta l'accés a Internet a dos

proveïdors que ofereixin una tecnologia diferent, per exemple fibra òptica i ADSL. Tanmateix, aquesta opció no sempre és viable.

Disposar de més d'un proveïdor d'accés a Internet ajuda a garantir la disponibilitat de les comunicacions en cas de caiguda del servei i, a més, permet realitzar un repartiment de càrrega entre les dues línies i millorar la seva capacitat.

1.3.9 Repartiment de càrrega

Tot i que el repartiment de càrrega no és una solució d'alta disponibilitat, serveix com a mesura preventiva, ja que permet gestionar el trànsit de la xarxa entre els diferents dispositius de manera que no es puguin saturar les interfícies i provocar una caiguda de les comunicacions. En el cas que una de les interfícies de xarxa caigués, es podrien mantenir les comunicacions a partir de les altres interfícies operatives. Per contra, el rendiment de la xarxa es veuria afectat.

1.3.10 Clúster de servidors

Un dels factors que més impacte pot tenir en el funcionament d'un sistema són les fallades del maquinari. Una caiguda del servidor principal pot tenir uns efectes devastadors i per això es recomana redundar aquest tipus de màquines. No obstant això, no s'ha d'oblidar que és una solució costosa i que no totes les empreses poden permetre-se-la.

Tanmateix, la redundància de servidors no és la única opció. Hi ha altres solucions més econòmiques i més ràpides per continuar amb l'activitat de negoci. Una de les solucions que més implanta a les empreses són els clústers de servidors d'alta disponibilitat.

Per facilitar la tasca de transferència de serveis i dades entre servidors en cas de fallada s'han desenvolupat noves arquitectures de servidors, els clústers.

> Un **clúster** és un conjunt d'unitats funcionals amb característiques similars interconnectades per mitjà d'una xarxa d'alta velocitat i configurades perquè actuïn coordinadament, com una sola unitat.

Els clústers es poden classificar segons la seva finalitat en:

- Clústers d'alt rendiment
- Clústers d'alta disponibilitat

Un **clúster d'alt rendiment** es basa en el processament en paral·lel, que consisteix a unir els diferents nodes en una xarxa i que parts d'un mateix programa s'executin

de forma paral·lela en els diferents processadors connectats. D'aquesta manera s'aconsegueixen sumar les capacitats de càlcul dels nodes que el componen. Sovint, aquestes formacions poden disposar d'un gran nombre d'ordinadors connectats per a la creació de supercomputadors. Aquest tipus d'arquitectura s'acostuma a utilitzar per a la resolució de problemes científics que requereixin processar un gran volum de dades. És el cas dels estudis sobre el genoma humà o el canvi climàtic.

Encara que la finalitat dels clústers d'alt rendiment no és l'alta disponibilitat, també acostumen a incorporar solucions d'aquest tipus, ja que no es podrà assolir un alt rendiment si no s'assegura una alta disponibilitat del sistema. Per això un clúster d'alt rendiment sempre oferirà millors prestacions que un únic ordinador amb igual capacitat de càlcul. A Catalunya, el supercomputador MareNostrum funciona amb aquesta tecnologia.

Supercomputador MareNostrum

A Catalunya tenim el supercomputador MareNostrum, basat en una tecnologia de clúster d'alt rendiment. Va ser creat l'any 2004 i encara avui és un dels superordinadors més potents de tot Europa. Està format per la unió de 10.280 processadors de 64 bits, una memòria de 20 terabytes, 280 terabytes de disc, que li proporcionen una capacitat de procés de 62 teraflops. El Barcelona Supercomputing Center (BSC) és l'organisme encarregat de la seva gestió i de seleccionar els projectes científics que en poden fer ús. S'hi desenvolupen tot tipus de projectes, com per exemple investigacions sobre el genoma humà o l'estructura de les proteïnes. Està ubicat en una antiga capella a les instal·lacions del campus de la UPC a Barcelona.

En un **clúster d'alta disponibilitat**, els diferents nodes que componen el clúster es troben monitorats en tot moment, de manera que si es produeix una fallada en el maquinari o programari d'algun dels nodes, es podran restaurar de forma automàtica els serveis caiguts en un altre servidor. Quan el node caigut torna a estar operatiu es restauren els seus serveis inicials i tot continua funcionant com ho feia abans de la caiguda. D'aquesta manera, la caiguda d'un dels servidors no afecta al funcionament global del sistema.

Els clústers d'alta disponibilitat no només són útils davant d'aturades no planificades, sinó que també són una bona solució per realitzar tasques de manteniment sense deixar d'oferir servei. A diferència dels clústers d'alt rendiment, no acostumen a disposar d'un gran nombre de nodes connectats; sovint es tracta únicament de la unió de dos nodes.

Existeixen diferents configuracions de clústers d'alta disponibilitat, tot i que les més comunes són l'actiu-actiu i l'actiu-passiu.

- **Configuració actiu-actiu**: tots els nodes estan operatius i poden executar els mateixos recursos de forma simultània. En el cas que es produís una fallada en un dels nodes, la resta de nodes del clúster podrien oferir els mateixos serveis, però augmentaria la càrrega dels altres nodes i la qualitat del servei es podria veure afectada. Aquesta configuració permet aprofitar molt millor els recursos del clúster, ja que tots els nodes poden treballar de forma simultània. La implantació d'un solució d'aquest tipus és bastant més complexe que una configuració actiu-passiu.

- **Configuració actiu-passiu**: el node actiu està operatiu i és l'encarregat d'oferir el servei als usuaris, mentre que el node passiu està aturat i només entra en funcionament quan el node actiu pateix una fallada. Aquest tipus de configuració és menys eficient que l'actiu-actiu, ja que en un moment determinat només s'aprofiten els recursos d'un dels dos nodes.

1.3.11 Plans de contingència

Siguin quines siguin les mesures que s'hagin aplicat per garantir l'alta disponibilitat en un sistema, sempre es poden produir fallades que no estiguessin contemplades o que no hagin pogut ser resoltes per les solucions implantades. En aquests casos només ens quedarà posar en funcionament el pla de contingència.

> El **pla de contingència** recull el conjunt de procediments alternatius que permetrien a l'empresa continuar treballant de manera normal en el cas que alguna de les seves funcionalitats es veiés afectada per un accident intern o extern.

A l'hora d'elaborar un pla de contingències, primer de tot cal realitzar una anàlisi de riscos. Aquesta anàlisi consisteix a identificar les causes i conseqüències de les amenaces que pot patir el nostre sistema. Per facilitar la feina, habitualment es dibuixen unes taules en les quals s'identifica per a cada una de les possibles amenaces la probabilitat que es produeixi i l'impacte que tindria en la continuïtat del negoci.

Un cop identificades totes les possibles amenaces es començaran a definir les solucions o processos per evitar que es produeixin o per mitigar-ne l'impacte. Es comença descrivint els processos d'aquelles amenaces que tenen una probabilitat i impacte alt, i s'acaba per les que són molt poc probables i tindrien un impacte molt baix.

Per a cadascuna de les amenaces identificades es descriuen diferents solucions. Algunes seran preventives, d'altres d'actuació i d'altres de recuperació.

- **Solucions preventives**: descriuen les accions que s'han de realitzar per evitar que es materialitzi aquesta amenaça.
- **Solucions d'actuació**: consisteixen en la descripció de les accions que s'han de realitzar un cop s'ha manifestat l'amenaça per tal de mitigar-ne l'impacte.
- **Solucions de recuperació**: són les accions que s'han de realitzar per recuperar el funcionament del sistema.

En un pla de contingència hi trobarem les solucions d'actuació per a tots els riscos identificats. En canvi, no sempre trobarem solucions preventives i de recuperació. Els procediments d'actuació han de contenir la informació següent: les accions a realitzar, la metodologia i el protocol a seguir, els materials necessaris, les persones implicades, les seves funcions i la persona responsable.

Els plans de contingència han ser revisats periòdicament, perquè no quedin obsolets i representin en tot moment la realitat de l'empresa. A part d'aquestes revisions periòdiques, cada cop que es posa en funcionament el pla se'n fa una valoració posterior per identificar possibles millores.

Pla de recuperació en cas de desastre

Un pla de recuperació en cas de desastre (en anglès, *Disaster Recovery Plan*) és un pla de contingència basat en els sistemes d'informació d'una empresa. En aquest pla s'identifiquen les amenaces que poden afectar al programari o maquinari del sistema, que poden causar una pèrdua de dades, en definitiva. Les empreses són cada cop més dependents de les tecnologies de la informació i per això si assegurem aquesta part de la companyia s'evitaran molts problemes derivats.

Aquest pla protegiria els sistemes d'informació contra desastres naturals com incendis i inundacions, actes vandàlics, talls en el subministrament elèctric, aturades del sistema i baixes de personal, entre altres situacions.

Es calcula que un 50% de les grans empreses estan protegides amb plans d'aquest tipus, mentre que en les petites i mitjanes empreses encara és una assignatura pendent, ja que només al voltant d'un 20% tenen plans de recuperació en cas de desastre. Algunes empreses destinen grans quantitats de diners a mantenir aquest tipus de plans. Tot i que poden tenir costos molt elevats, és preferible fer aquest tipus d'inversions que no que es produeixi una pèrdua de dades. Això suposaria pèrdues econòmiques importants per a la empresa i podria causar danys d'imatge irreparables.

Pla de continuïtat del negoci

Els plans de continuïtat de negoci (en anglès, *Business Continuity Plan*) són els plans de contingència que vetllen per la continuïtat de les funcions crítiques del negoci en cas de que es produeixi una interrupció no programada. En aquests tipus de plans, a part de disposar d'un pla de recuperació dels sistemes d'informació en cas de desastre, es detallen els procediments necessaris per poder continuar l'activitat. Per tant, es tracta de plans molt més complexos i que requereixen la implicació de tota la organització.

Perquè aquests plans siguin efectius cal generar una cultura de continuïtat de negoci i campanyes de sensibilització als treballadors, ja que és important que tot el personal participi en la elaboració del pla i sàpiga on trobar-lo quan faci falta.

En el seu procés d'elaboració és important que s'identifiquin les funcions crítiques del negoci i que s'elaborin plans preventius, d'actuació i recuperació per a cadascuna d'aquestes funcions, per tal de poder garantir un servei mínim en cas de contingència. Sovint no és fàcil identificar els processos més crítics o que poden tenir un major impacte de cara els clients. Per poder visualitzar tots aquests aspectes i poder prioritzar els diferents processos s'acostuma a realitzar una anàlisi d'impacte (en anglès, *Business Impact Analysis*). En aquestes anàlisis s'identifica per a cada funció l'impacte econòmic i d'imatge, temps de recuperació i els recursos requerits per continuar amb el seu funcionament. En base a aquestes anàlisis es prioritzen els processos i s'elaboren els procediments d'actuació.

2. Virtualització

Sovint, les empreses instal·len un servidor per cada servei a oferir. Aquesta és la opció més fàcil i segura, i garanteix una bona qualitat de servei. Podem trobar empreses que disposen d'un servidor específic per a l'allotjament web, que està en espera la gran part del dia i té un temps d'ús del 5-10%. I el mateix passa amb el servidor de correu, el de la base de dades...

Des de fa uns anys moltes empreses han utilitzat solucions de virtualització per millorar el rendiment del seu maquinari, a banda d'altres avantatges d'aquesta tecnologia, com per exemple l'alta disponibilitat.

La **virtualització** consisteix a crear amb un programa específic una capa d'abstracció sobre una màquina física perquè els seus recursos puguin ser compartits i utilitzats per múltiples usuaris. Es poden virtualitzar servidors, sistemes d'emmagatzematge, connexions de xarxa, estacions de treball, aplicacions i sistemes operatius.

Inicis de la virtualització

En els últims anys s'ha potenciat molt la virtualització a les empreses a causa dels nombrosos avantatges que ofereix. No obstant això, no es tracta de cap tecnologia nova, ja que en els anys 60 ja s'utilitzaven solucions d'aquest tipus. En aquell moment les empreses disposaven d'un únic supercomputador i virtualitzaven el sistema per tal que cada treballador pogués treballar amb una part d'aquest com si es tractés d'un ordinador independent.

No obstant això, l'ús principal de la virtualització és la creació de múltiples ordinadors o servidors completament independents, coneguts com a *màquines virtuals*, en un sol ordinador físic. Tot i que les màquines treballen de forma independent, comparteixen els mateixos recursos de maquinari (processador, memòria, disc dur i interfícies de xarxa). Això és possible gràcies a l'**hipervisor**, també anomenat **monitor de les màquines virtuals** o VMM (de l'anglès *Virtual Machine Monitor*), que és el programa que arbitra i gestiona dinàmicament aquests recursos entre totes les màquines virtuals.

2.1 Objectius de la virtualització

Enumerem a continuació alguns dels principals avantatges i objectius de les empreses que utilitzen la virtualització:

- **Millorar els índexs d'utilització del maquinari**: avui podem trobar molts servidors que tenen índexs d'utilització del 10 o el 15%. Això suposa una inutilització dels sistemes i, per tant, una pèrdua de diners en la inversió realitzada. Aplicant tècniques de virtualització podem oferir més d'un servei en una mateixa màquina física. D'aquesta manera aconseguirem índexs d'utilització d'un 70 o 90% i aconseguim fer més eficients les inversions realitzades.

- **Problemes d'espai en els centres de processament de dades**: en els últims anys ha augmentat molt el volum de dades digitals que han de tractar les empreses, ja que molts processos que abans eren manuals i es feien en paper ara estan digitalitzats. Altrament, també han augmentat els serveis de què disposen: servidors de pàgines web, intranets, correu electrònic... i, sovint, les sales de servidors havien estat dimensionades per a una altra realitat. Unificant processos gràcies la virtualització es poden pal·liar aquests problemes d'espai i evitar haver de fer reformes o crear nous CPD, ja que són molt costosos.

- **Reduir costos en el subministrament elèctric**: cada cop les empreses destinen més diners al subministrament elèctric a causa de l'increment de les tarifes i sobretot de l'increment del nombre d'aparells electrònics. Amb la virtualització es pot reduir el nombre de servidors físics i, per tant, la despesa en energia, contribuint a la conservació del medi ambient, moviment que en anglès s'anomena *green IT*.

- **Reduir costos d'operació**: els ordinadors no són autònoms del tot, necessiten ser monitorats, actualitzats, reparats i revisats pel personal tècnic de l'empresa. La virtualització ajuda a reduir els costos en aquestes operacions.

- **Afegir flexibilitat i escalabilitat**: les empreses canvien i ho fan molt ràpid. D'altra banda, els sistemes d'informació sovint són rígids i és difícil adaptar-los a les noves necessitats de l'empresa. Amb la virtualització, aquests canvis son molt més ràpids i els problemes d'escalabilitat desapareixen.

- **Pla de recuperació en cas de desastre**: una de les millors solucions en cas de desastre és disposar d'un centre de processament de dades secundari que pugui entrar en funcionament quan es produeixi una caiguda en el servei. No obstant això, aquesta solució és molt costosa i poc eficient, ja que si no es produeix cap caiguda el centre secundari estarà infrautilitzat. Algunes empreses sense tants recursos veuen en la virtualització una solució, ja que permet restaurar, crear o transferir màquines virtuals i continuar amb l'activitat de negoci en pocs minuts.

- **Compatibilitat d'aplicacions**: sovint, quan es realitzen actualitzacions en els sistemes, algunes aplicacions una mica antigues poden deixar de funcionar, ja que no estan pensades per treballar amb un sistema operatiu tan modern. Això pot suposar un problema en el funcionament de l'empresa ja que sovint es tracta d'aplicacions pròpies que van costar molts diners i que encara funcionen correctament. Amb la virtualització podem simular màquines més antigues per tal que aquestes aplicacions puguin continuar executant-se.

- **Entorn de proves**: abans de donar per vàlid un programa, els desenvolupadors necessiten executar-lo en un entorn el més semblant possible al servidor de producció. Per contra, s'ha de tenir present que en tractar-se d'un programa en fase de desenvolupament pot ser que encara no estigui prou depurat i que pugui produir algun problema en el funcionament del sistema. Per aquest motiu les proves es realitzen en un entorn controlat. La

virtualització permet proveir un entorn de proves econòmic, que es pot restaurar de forma ràpida en cas de fallada sense interrompre el funcionament del sistema productiu.

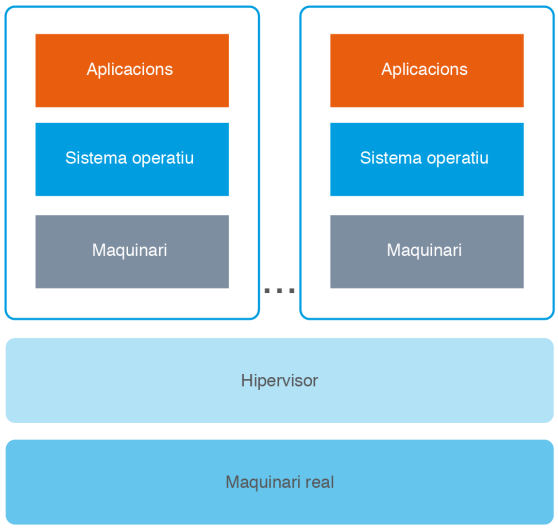
2.2 Virtualització de servidors

La virtualització de servidors consisteix en la creació de màquines virtuals amb el seu propi sistema operatiu que funcionen com si es tractessin de servidors totalment independents. D'aquesta manera, en un únic servidor físic es poden allotjar diferents servidors virtuals, els quals poden funcionar amb diferents sistemes operatius. Dins de la virtualització de servidors podem trobar diferents tècniques: la virtualització nativa, la virtualització allotjada i la paravirtualització.

2.2.1 Virtualització nativa

L'hipervisor s'executa directament en el maquinari físic per controlar l'assignació de recursos i memòria entre les diferents màquines virtuals, a més de proporcionar una interfície per a l'administració a alt nivell i eines per monitorar. Tal com s'observa en la figura 2.1, les màquines virtuals s'executen de manera simultània en un nivell superior.

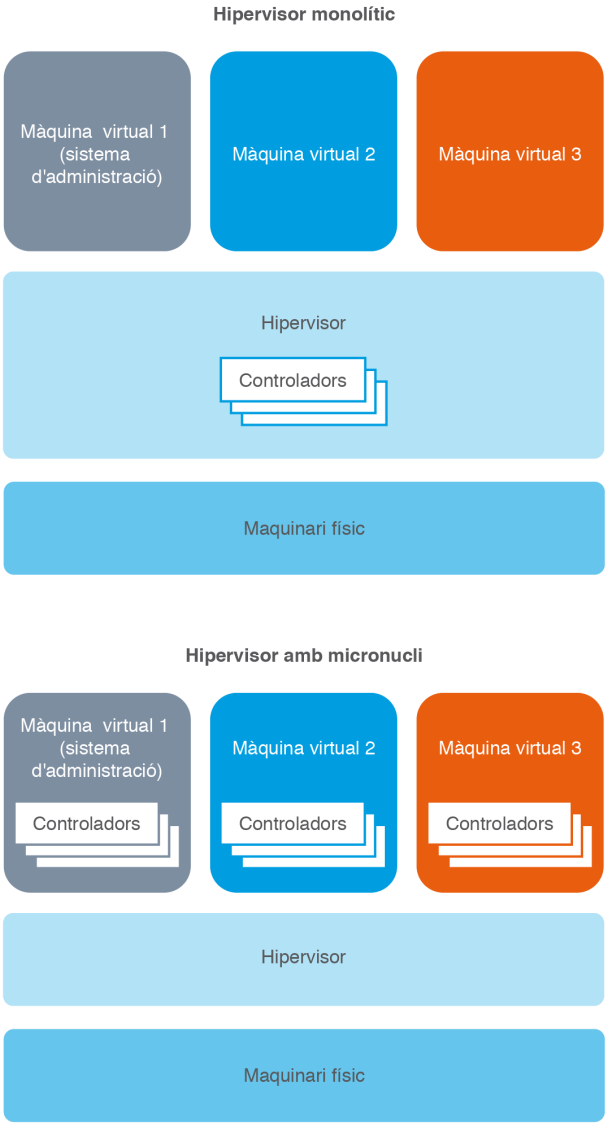
Figura 2.1. Estructura d'un sistema de virtualització natiu



L'hipervisor s'executa en l'anell 0 de la CPU i, per tant, els sistemes operatius de les màquines virtuals hauran d'estar modificats i utilitzar anells superiors. Això complica la virtualització nativa, ja que la majoria del sistemes operatius estan dissenyats perquè s'ubiquin en l'anell 0, perquè hi ha algunes tasques que només es poden realitzar en aquest nivell, com per exemple l'execució d'instruccions amb privilegis a la CPU o l'accés directe a la memòria.

D'altra banda, depenent de l'arquitectura, l'hipervisor pot disposar o no dels controladors necessaris per a la gestió dels recursos de maquinari o bé pot ser el mateix sistema operatiu de la màquina virtual el que els té prèviament instal·lats. En la figura 2.2 podem observar aquestes dues situacions.

FIGURA 2.2. Arquitectura dels hipervisors



Com que l'hipervisor té accés directe al maquinari, sempre oferirà un millor rendiment que la virtualització allotjada, ja que utilitza menys recursos.

Alguns exemples de virtualització nativa són VMware ESXi, VMware ESX, Xen, Citrix XenServer i Microsoft Hyper-V Server.

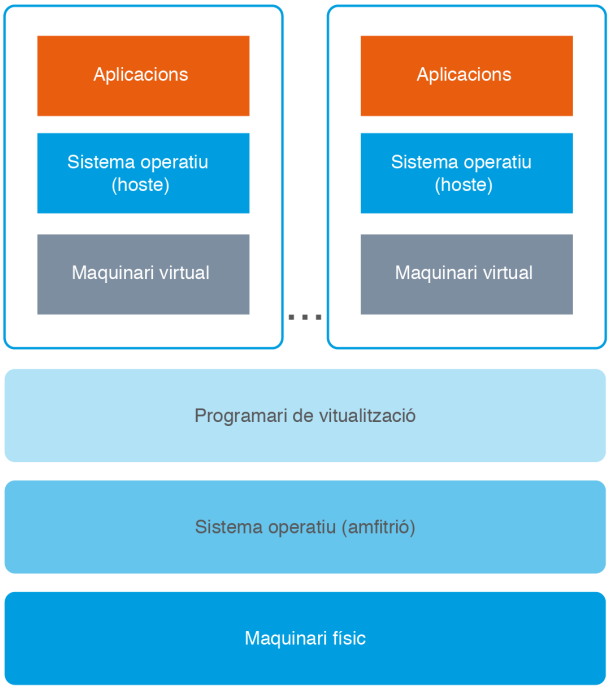
2.2.2 Virtualització allotjada

En la virtualització allotjada, l'hipervisor s'executa sobre un sistema operatiu convencional per després virtualitzar diferents sistemes operatius. En aquesta

arquitectura, l'hipervisor proporciona a cada màquina virtual tots els recursos de la màquina física, incloent una BIOS virtual i una memòria virtual. Aquesta situació fa que el sistema allotjat tingui la sensació que s'està executant directament en la màquina física en lloc d'en una màquina virtual dins d'una aplicació.

En la figura 2.3 podem observar l'estructura d'un sistema de virtualització allotjada.

Figura 2.3. Estructura d'un sistema de virtualització allotjada



La virtualització se situa en una capa més allunyada del programari que en la virtualització nativa, fet que afecta al rendiment de l'hipervisor.

Alguns exemples de virtualització allotjada són VirtualBox, VMware Workstation, VMware Server, VMware Player, QEMU, Microsoft Virtual PC i Microsoft Virtual Server.

2.2.3 Paravirtualització

En la paravirtualització, l'hipervisor està allotjat sobre el maquinari de la màquina física, és a dir que es tracta d'un sistema de virtualització nativa. Tal com es fa en la virtualització nativa, les màquines virtuals es creen sobre l'hipervisor, que és específic i més simple que els de virtualització nativa, ja que en la paravirtualització les màquines virtuals disposen de privilegis que els permeten accedir directament a alguns recursos de la màquina física.

Que les màquines virtuals puguin accedir directament a alguns recursos del sistema té com a objectiu millorar el temps d'execució, ja que algunes tasques

són molt més difícils d'executar si es realitzen des d'un entorn virtualitzat que si es realitzen directament en la màquina nativa. Els sistemes operatius utilitzats en les màquines virtuals d'un sistema de paravirtualització han de ser creats específicament per a aquesta utilitzat.

Per exemple, Xen ofereix una solució d'aquest tipus en la qual el rendiment de les màquines virtuals només es veu afectat entre un 2 i un 8% respecte del que obtindrien si estiguessin funcionant directament en la màquina física. Aquest projecte s'anomena XenWindowsGplPv.

2.3 Virtualització d'escriptoris

Els servidors no són els únics dispositius que es poden beneficiar dels avantatges de la virtualització en una empresa. També es poden virtualitzar els escriptoris, els sistemes d'emmagatzematge, aplicacions i xarxes.

La majoria d'empreses i organitzacions disposen de multitud de dispositius. En moltes companyies gairebé cada treballador disposa d'un ordinador, a part d'altres dispositius d'accés al sistema com ordinadors portàtils o dispositius mòbils. La gestió d'aquest volum de dispositius genera una càrrega de feina molt gran per al personal informàtic de l'empresa, ja que ha de realitzar tasques de manteniment, còpies de seguretat de les dades i actualitzar el sistemes operatius, els antivirus, les aplicacions o els pedaços de seguretat de cadascun d'aquests dispositius. No fer-ho podria causar grans problemes de seguretat. Per solucionar aquests problemes, les empreses comencen a implantar solucions de virtualització d'escriptoris.

La **virtualització d'escriptoris** trenca amb la concepció que l'escriptori són tots els programes i les dades ubicats en una màquina física, i el defineix com el conjunt d'aplicacions i dades amb què un usuari treballa, independentment del dispositiu amb què hi accedeixi.

Quan els usuaris treballen en un escriptori virtual, tots els programes i dades estan emmagatzemats en un servidor compartit on s'emmagatzemen i executen de manera centralitzada. Això permet als usuaris accedir als seus escriptoris des de qualsevol dispositiu, com un ordinador, un portàtil, un telèfon intel·ligent o un client lleuger. Sovint s'acostuma a utilitzar aquesta última opció, ja que els clients lleugers són més econòmics i fiables que els ordinadors convencionals, perquè en no disposar de discos d'emmagatzematge local redueixen la probabilitat de fallar.

En aquest tipus de virtualització és necessària una bona connexió entre el servidor i els clients. Si aquesta connexió és deficient, pot provocar problemes en el rendiment del sistema. S'ha desenvolupat una variant de virtualització d'escriptoris anomenada *Check In Check Out* en què els clients descarreguen a l'inici de la sessió el seu sistema i hi treballen en local sense necessitat de connectar-se constantment al servidor. Al final de la sessió tornen a fer un bolcat de l'escriptori al servidor principal, cosa que deixar el dispositiu utilitzat completament net.

S'acostuma a utilitzar aquesta variant en connexions poc fiables, com per exemple connexions d'usuaris que treballen des de casa o que estan de viatge.

En les primeres solucions de virtualització d'escriptoris es creava en el servidor una imatge de disc per a cada usuari de l'empresa. Això suposava un gran volum de dades emmagatzemades en el disc del servidor, la qual cosa podia provocar problemes d'espai. En canvi, avui en dia s'emmagatzema una única imatge que es pot clonar per a cada usuari i només s'emmagatzemen de manera separada les configuracions personals. Quan un usuari acaba la sessió, totes les dades i modificacions de configuració es tornen a emmagatzemar en el servidor i no queda cap informació en el dispositiu.

La virtualització d'escriptoris ofereix molts avantatges a les empreses:

- **Augment de la seguretat**: els usuaris executen un escriptori virtual ubicat en el centre de processament de dades. D'aquesta manera, els usuaris finals no poden ni instal·lar ni modificar el programari del seu escriptori. Són els administradors els encarregats de definir un perfil per a cada tipus de treballador i d'assignar-los únicament aquelles aplicacions que necessiten. Així, els administradors poden gestionar de manera centralitzada els escriptoris en comptes de fer-ho físicament, assegurant que els usuaris no puguin modificar res del sistema operatiu i que a més es realitzen totes les actualitzacions de seguretat i d'antivirus.
- **Seguretat de les dades**: les dades estan centralitzades en el servidor de l'empresa, la qual cosa impedeix als usuaris treballar amb fitxers ubicats en el seu disc local. Això facilita la realització de còpies de seguretat i garanteix que tota la informació compleix la normativa de seguretat de l'empresa. A més, evita que es puguin produir fuites o malversacions de dades confidencials. Amb la virtualització d'escriptoris és més difícil poder extreure documents de la empresa i, en cas de pèrdua o robatori d'un ordinador portàtil, no s'haurà de patir pel seu contingut, ja que no contindrà cap informació compromesa.
- **Reducció de costos**: la virtualització d'escriptoris permet reduir costos de manteniment per part del personal d'informàtica, ja que es podran mantenir tots els ordinadors de la empresa de manera centralitzada, sense necessitat de desplaçar-se físicament. D'altra banda, també permet reduir costos en maquinari. Com que les aplicacions s'executen en el servidor. no es necessiten estacions de treball d'última tecnologia. Sovint, amb un client lleuger (més barat que un ordinador convencional) connectat al servidor n'hi haurà prou. A més, la vida útil d'aquest tipus de dispositius és del voltant d'uns sis anys, mentre que la d'un ordinador normal és de tres.
- **Respecte al medi ambient**: en centralitzar tots els càlculs en el servidor, el consum elèctric dels clients lleugers és molt inferior que si s'executessin les aplicacions de forma distribuïda. És calcula que pot suposar un estalvi energètic d'entre el 50 i el 90%.
- **Continuïtat de negoci**: la virtualització d'escriptoris és una solució senzilla i eficient a implantar en un pla de recuperació en cas de desastre.

Les empreses que disposen d'aquesta tecnologia podran continuar la seva activitat des de qualsevol dispositiu que tingui connexió amb el servidor.

- R**educció del temps d'inactivitat**: en cas de fallada del maquinari o el programari, en pocs minuts es pot restaurar l'escriptori i continuar treballant amb el que s'estava fent en el mateix dispositiu o des d'un altre, la qual cosa redueix de manera significativa el temps d'inactivitat dels usuaris finals.

- **Millora de la productivitat**: en tractar-se d'escriptoris restringits, els treballadors no poden instal·lar programari no permès. D'aquesta manera es pot garantir que els usuaris només tenen accés a les aplicacions autoritzades per la empresa i que, per tant, dediquen tot el seu temps a la feina, sense distraccions que puguin reduir la seva productivitat.

- **Escalabilitat**: la virtualització d'escriptoris facilita gestionar el creixement d'una empresa i, en definitiva, l'escalabilitat dels seus sistemes. Quan un nou treballador entra a l'empresa, en pocs minuts pot disposar d'un escriptori amb totes les aplicacions necessàries.

Tot i el gran ventall d'avantatges que ofereix la virtualització d'escriptoris, encara són poques les empreses que han optat per implantar solucions d'aquest tipus. En canvi la majoria d'empreses s'han beneficiat dels avantatges de la virtualització de servidors ja que són solucions que aporten molts avantatges, relativament fàcils d'implantar, no requereixen una gran inversió i ofereixen beneficis immediats.

A la llarga, implantar solucions de virtualització d'escriptoris suposarà una reducció de costos per a l'empresa (manteniment, consum elèctric, vida útil dels dispositius). No obstant això, en el moment de la implantació s'ha de fer una inversió econòmica important en l'estructura de xarxa i servidors. A part, suposa canviar la filosofia de treball i el funcionament de tota l'empresa. Per tant, no es tracta únicament d'un canvi en el departament de sistemes, sinó que cal implicar tota la organització.

2.4 Virtualització d'aplicacions

A diferència de la virtualització d'escriptoris remots, en la virtualització d'aplicacions no es recrea totalment un ordinador, sinó que es virtualitza només una aplicació en concret. En aquest cas, cal interpretar la virtualització d'aplicacions com la separació dels llocs on s'executa l'aplicació i on es mostren les dades al usuari. Les aplicacions estan allotjades en el servidor principal, on s'executen a petició dels usuaris a través d'un terminal client. Dins de la virtualització d'aplicacions existeix una variant en què les aplicacions no s'executen en el servidor, sinó que es descarreguen i s'instal·len en el client cada cop que s'han d'utilitzar.

Aquest sistema pot semblar repetitiu, però permet als administradors controlar millor les aplicacions, assegurar-se que tots els usuaris utilitzen la última versió i

que disposen dels pedaços de seguretat instal·lats. Aquesta tècnica s'acostuma a utilitzar en organitzacions amb molts usuaris que han d'utilitzar diferents aplicacions, com per exemple els estudiants d'una universitat.

2.5 Eines per a la virtualització

Actualment existeixen eines per virtualitzar tant de pagament com gratuïtes. És important seleccionar el producte que més s'adeqüi a les nostres necessitats i que sigui compatible amb el programari a utilitzar.

2.5.1 Sistemes propietaris

A continuació es detallen els principals fabricants d'eines de virtualització.

- **VMware**: és la empresa líder del mercat de la virtualització. És la que porta més anys dedicant-se aquesta tecnologia i controla una gran part del mercat. La clau del seu èxit és oferir un bon producte i un excel·lent servei de suport. No obstant això, en els últims anys són moltes les empreses que ofereixen tecnologies similars a un preu més baix o fins i tot gratuïtament. Disposa d'un gran ventall de productes destinats a oferir solucions específiques a cada necessitat. La majoria d'ells són de pagament, tot i que també ofereix alguns productes de forma gratuïta.
  - **Virtualització de centres de processament de dades**: VMware vSphere, Go, vCloud, ESX Server
  - **Virtualització d'escriptoris**: VMware View, ThinApp, ACE, Workstation, Zimbra, MVP (Mobile Virtualization Platform) i Horizon
  - **Virtualització d'aplicacions**: família de productes VMware vFabric
  - **Productes de seguretat**: família de productes VMware vShield
  - **Sistemes de gestió**: família de productes VMware vCenter (gestió d'aplicacions, infraestructures i operacions)
  - **Productes per a MAC**: VMware Fusion
  - **Productes gratuïts**:VMware vSphere Hypervisor, Server, Player i ESXi
- **Microsoft**: empresa líder en el terreny dels sistemes operatius, va entrar en el món de la virtualització més tard, però ho ha fet amb empenta i s'ha guanyat un lloc en el mercat. A diferència de Vmware, Microsoft ha orientat els seus productes a les petites i mitjanes empreses, i es calcula que l'any 2012 Microsoft controlava al voltant del 85% del mercat de la virtualització en aquest sector. A més, Microsoft disposa d'un sistema operatiu propi i pot oferir una solució completa. Per acabar, el seu sistema operatiu Windows 8 inclou per defecte l'Hyper-V. A continuació s'enumeren els principals productes de virtualització de Microsoft.

  - **Virtualització de servidors**: Hyper-V a Windows Server 2008 R2
  - **Virtualització per a la creació de núvols privats**: Microsoft Dynamic Data Center Toolkit i Windows Azure
  - **Virtualització d'aplicacions**: Microsoft Application Virtualization
  - **Virtualització d'escriptoris**: Microsoft Enterprise Desktop Virtualization i Microsoft Virtual Desktop Virtualization

- **Citrix**: empresa multinacional fundada l'any 1989, subministra programari de virtualització de servidors, escriptoris, aplicacions i xarxa. Des del juny de 2009, el seu producte de virtualització de servidors anomenat XenServer pot ser descarregat de forma gratuïta des del seu web.

  - **Virtualització de servidors**: XenServer
  - **Virtualització d'escriptoris remots**: XenDesktop, XenClient, VDI-in-a-Box i XenReceiver.
  - **Virtualització d'aplicacions**: XenApp
  - **Gestió de les màquines virtuals**: NetScaler

2.5.2 Sistemes lliures

De mica en mica, han anat sorgint solucions de virtualització de distribució lliure. Algunes d'aquestes versions gratuïtes són més limitades que les seves versions de pagament, no obstant això, n'hi ha molta varietat i s'hi troben eines força completes, especialment les dissenyades per ser utilitzades en entorns Linux.

Sovint, les grans empreses opten per solucions empresarials, ja que ofereixen un millor suport, és més fàcil trobar-ne documentació i estan més esteses. Les eines de virtualització lliures es destinen majoritàriament a entorns de proves o a l'aprenentatge.

Gràcies a l'aparició d'aquestes eines de virtualització gratuïtes, s'ha pogut apropar la virtualització a tots tipus d'usuaris.

- **VMware**: és la empresa líder en el mercat, i tot i que les seves solucions acostumen a ser de pagament, ha llançat al mercat alguns productes de distribució lliure:

  - **VMware Server**:és una eina dissenyada per ser utilitzada tant a Windows com a Linux. És fàcil d'utilitzar i serveix perquè les empreses s'iniciïn en el món de la virtualització de servidors, optimitzant la utilització dels seus dispositius. Tot i que encara s'utilitza, a finals de 2011 VMware va anunciar que deixava de donar suport tècnic a aquest producte i que llançava altres eines de virtualització més específiques.
  - **VMware vSphere**: evolució del VMware Server, és un producte fàcil d'utilitzar, pensat perquè les empreses s'iniciïn en la virtualització de servidors de manera gratuïta en pocs minuts. Pot executar fins a 100 màquines virtuals i centralitzar-ne la gestió.

  - **VMware Player**: es tracta d'un petit programari de virtualització que permet reproduir màquines virtuals ja creades. És una manera ben senzilla d'entrar en el món de la virtualització a nivell d'usuari.
  - **VirtualBox**: eina de virtualització amb llicència GNU/GPL d'Oracle per a professionals i per a ús domèstic que permet disposar de més d'un sistema operatiu en un mateix ordinador. Ara mateix existeixen versions de VirtualBox per als principals sistemes operatius (Windows, Linux, Mac i Solaris) i s'hi poden virtualitzar un gran nombre de sistemes operatius: Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, DOS/Windows 3.x, Linux (2.4 i 2.6), Solaris, OpenSolaris, OS/2 i OpenBSD.

- **Virtual PC**: programa gestor de virtualització desenvolupat per Connectix i posteriorment adquirit per Windows. És una eina similar a VirtualBox amb la qual els usuaris poden disposar de més d'un sistema operatiu en un ordinador. Pot ser instal·lat en la majoria de versions del sistema operatiu Windows (7, Vista, XP, Server 2003, Server 2008) i pot allotjar els sistemes operatius següents: Server 2003 i 2008, NT, Vista, XP, 2000, OS/2, Me, MS-DOS, 98 6.22, 3.1, 3.11, 2.03, 1.01.

- **QEMU**: és un emulador d'arquitectures basades en x86 amb dos modes de funcionament: emulació del sistema complet i emulació en mode usuari.

  - **Mode complet**: emula un equip sencer, incloent-hi múltiples processadors i perifèrics. Aquest mode s'utilitza per executar sistemes operatius complets. En les últimes versions, el programa accepta fins a 15 arquitectures diferents.
  - **Mode usuari**: el programa pot executar aplicacions compilades per a un processador concret en un sistema que funciona sobre un processador diferent. Pot servir per solucionar problemes d'incompatibilitat entre arquitectures de 32 i 64 bits.

- **KVM (Kernel Virtual Machine)**: solució de virtualització completa en què s'utilitza el nucli de Linux com a hipervisor, de manera que tant el control dels dispositius com la planificació de les tasques i la gestió de la memòria del sistema les realitza el nucli, en anglès *kernel*. En aquest model, les màquines virtuals no deixen de ser un simple procés en el sistema.

- **Linux-Vserver**: sistema de virtualització a nivell de sistema operatiu que s'implementa com una sèrie de modificacions del nucli de Linux. Proporciona les eines necessàries per crear múltiples entorns d'usuari independents entre ells. Com que aquesta tecnologia no està lligada a cap arquitectura concreta, pot executar-se en microprocessadors (x86, x86-64, PowerPC, ARM...).

- **Xen**: solució de paravirtualització i que, per tant, compta amb un hipervisor que s'executa en el nivell més privilegiat de la màquina i que s'encarrega bàsicament de la planificació de tasques i de la gestió de la memòria. Tot i que sovint s'utilitza en entorns Linux, Xen no és un sistema de virtualització lligat al nucli de Linux, sinó que també pot ser utilitzat en versions modificades de NetBSD, Solaris, FreeBSD i Plan9.

2.5.3 Maquinari específic per virtualitzar

Es poden implementar solucions de vitualització en qualsevol servidor. Ara bé, això no vol dir que tots siguin iguals pel que fa a la virtualització; els seus rendiments poden variar considerablement. Per treure el millor partit a aquesta tecnologia, alguns proveïdors de components de maquinari ofereixen solucions orientades a la virtualització. Els dos proveïdors que més han despuntat en aquest camp són Hewlett-Packard i Dell.

- **Hewlett-Packard**: la gama de servidors ProLiant ofereix un gran ventall de solucions de virtualització amb diversos proveïdors: VMware, Citrix, Microsoft, Linux i Solaris. Amb VMware porten més de 10 anys treballant conjuntament. Són considerats líders en aquest sector gràcies a la gran integració entre els dos productes, que ofereix un excel·lent rendiment i un ús eficient de l'emmagatzematge, i evita problemes d'escalabilitat. Entre d'altres, ofereixen solucions per a la virtualització de servidors, escriptoris i fins i tot solucions en núvol.
- **Dell**: ha dissenyat la família de servidors PowerEdge per obtenir el millor rendiment possible en virtualització. Ha optimitzat alguns dels seus productes per tal d'adaptar-los a les necessitats de virtualització: densitat, flexibilitat i rendiment. Dell ha implementat solucions VMware des del primer hipervisor, que es va comercialitzar l'any 2001. No obstant això, en els últims anys han signat acords amb fabricants com Citrix i Microsoft per tal d'oferir un ventall més ampli de possibilitats en el món de la virtualització.

Significat de la nomenclatura de Dell

Dell utilitza per a la gamma PowerEdge una nomenclatura pròpia basada en una lletra i tres dígits. La lletra indica el tipus de servidor: (R) bastidor o *rack*, (M) modular, (T) torre. El primer dígit indica el nombre de sòcols del sistema: del 1 al 3 per a un sòcol, del 4 al 7 per a dos sòcols, 9 per a quatre sòcols i 8 per a dos o quatre sòcols, dependrà del processador. El segon dígit fa referència a la generació: 0 per a la generació 10, 1 per a la generació 11… El tercer dígit indica el fabricant del processador: 0 per a Intel i 5 per a AMD.

2.6 Configuració i utilització de les màquines virtuals

En els últims anys moltes empreses han optat per implantar solucions de virtualització en els seus servidors. Però implantar una solució d'aquest tipus no és una tasca fàcil, ja que els administradors han de disposar de coneixements sobre el tema, cosa que no sempre passa.

Primer cal establir uns objectius clars sobre quina és la finalitat d'aplicar aquesta tecnologia. Un cop es tingui clar l'objectiu, caldrà analitzar tots els productes que hi ha al mercat, tant de pagament com de programari lliure, per veure quin dóna millors resultats. No s'usa el mateix el programari per virtualitzar un servidor que per virtualitzar escriptoris.

Un cop s'ha escollit el tipus de virtualització i el producte que s'implantarà, cal comprovar que el nostre maquinari compleix els requeriments tècnics. Abans d'instal·lar el programa en el servidor de producció, cal fer un simulacre en un entorn de proves per poder valorar el seu funcionament. Si les proves realitzades

són satisfactòries, es pot procedir a la instal·lació del programa en els sistemes productius, prenent totes les mesures de precaució necessàries.

2.7 Migració en calent

Un dels grans avantatges de la virtualització és la gran flexibilitat que ofereix tant per la creació, eliminació i modificació dels recursos de les màquines virtuals com per al canvi de màquina física.

La **migració en calent** (en anglès, *live migration*) consisteix a poder traslladar una màquina virtual des d'una màquina física a una altra sense que l'usuari se n'adoni. S'anomena *migració en calent* ja que mentre s'està movent d'un lloc a un altre la màquina virtual continua estant operativa.

Els principals fabricants (VMware, Microsoft i Citrix) ja disposen de solucions que permeten aquest tipus de migracions.

La migració en calent pot canviar una màquina virtual d'un servidor físic a un altre de manera que el temps d'inactivitat sigui de mil·lisegons. No obstant això, no és una tasca fàcil, ja que s'ha de traslladar el contingut de la memòria, del disc dur, l'estat del processador i les connexions de xarxa. A continuació es detalla cadascun d'aquests aspectes:

- **Migració de la memòria**: es tracta d'un procés complicat, ja que mentre es transfereix aquesta informació del node origen al de destinació, la màquina continua fent modificacions. Aquest traspàs d'informació es pot realitzar de moltes maneres diferents, però sempre s'ha de prioritzar la que permeti minimitzar el temps d'inactivitat i el temps total de la migració.
- **Migració del disc dur**: és força similar al procés de migració de la memòria, tot i que en aquest cas el volum de dades que s'han de transmetre és major i per tant el temps de migració és superior. Per solucionar aquest problema, els fabricants utilitzen sistemes d'emmagatzematge centralitzat com per exemple SAN, NFS o iSCSI. D'aquesta manera, tots els servidors físics estan connectats a un mateix sistema d'emmagatzematge i quan una màquina virtual es mogui de servidor no serà necessària la migració del disc dur i es reduirà així considerablement el temps d'inactivitat.
- **Migració de connexions de xarxa**: per facilitar la migració de connexions de xarxa cal que tots els servidors formin part de la mateixa subxarxa. D'aquesta manera les adreces IP que utilitzin estaran dins del mateix rang. Quan una màquina virtual vulgui canviar de servidor físic, només haurà d'enviar un missatge ARP a l'adreça de difusió indicant l'adreça MAC de la nova targeta de xarxa. Com que aquest canvi només afecta a nivell físic, les connexions que la màquina virtual tenia establertes no es veuran afectades, ja que la seva adreça IP continuarà sent la mateixa.

- **Migració del processador**: en canviar de processador és quan realment es produeix la migració. Per aquest motiu ha de ser l'últim recurs que canviem de lloc. Primer passarem les dades, tant les del disc dur com les de la memòria, després les connexions i per acabar el processador, juntament amb alguna dada que hagi estat modificada amb posterioritat a la seva còpia. Cal tenir present el tipus de processadors dels servidors, ja que poden haver-hi incompatibilitats entre processadors de diferents fabricants.

La migració en calent permet millorar la gestió de rendiment de les màquines, ja que és una eina molt potent per als administradors de clústers. Permet separar el programari del maquinari on es troba allotjat i gestionar un clúster de servidors com si es tractés d'un domini.

La virtualització en calent ofereix molts avantatges. Entre d'altres, redueix el temps d'inactivitat en cas de fallada del maquinari, permet fer un repartiment de càrrega de màquines virtuals, afavoreix l'escalabilitat de les aplicacions i serveis i permet fer un ús més eficient del sistemes.

Aquests són alguns dels productes que permeten la migració en calent: VMware ESX, Hyper-V Windows Server 2008 R2, Xen, KVM i OpenVZ.

2.8 Virtualització i alta disponibilitat

La virtualització és una de les tècniques més eficients i més econòmiques per garantir l'alta disponibilitat en els sistemes d'informació. Pel gran nombre d'avantatges que ofereix, i no només en termes d'alta disponibilitat, és una de les solucions més adoptades per les empreses. En els últims anys han estat moltes les companyies que han apostat per aquesta tecnologia i es preveu que en un futur proper encara seran més les que apostaran per la virtualització.

A continuació es detallen els principals avantatges que aporta la virtualització en termes d'alta disponibilitat:

- **Alta disponibilitat de totes les aplicacions**: la virtualització ofereix una solució d'alta disponibilitat completa, ja que protegeix la continuïtat de negoci tant a nivell físic com a nivell lògic.
- **Repartiment de càrrega**: permet gestionar de manera eficient la càrrega dels servidors físics i evitar que es puguin saturar i entrar en fallada. Fa un ús eficient de les màquines físiques i aconsegueix un procés d'optimització continua.
- **Recuperació en cas de desastre**: simplifica i automatitza els fluxos de recuperació en cas de desastre (prevenció, actuació i recuperació). Converteix algunes instruccions manuals de recuperació en processos automatitzats. Fins i tot permet centralitzar la gestió del pla en cas de desastre des d'una plataforma de gestió.

- **Protecció i gestió dels escriptoris corporatius**: la virtualització d'escriptoris permet poder oferir als usuaris finals solucions d'alta disponibilitat. En cas de fallada del terminal d'accés, l'usuari podrà iniciar sessió en pocs segons des de qualsevol altre dispositiu connectat a la xarxa.

- **Flexibilitat i escalabilitat**: depenent de la demanda d'un servei, les màquines es podran readaptar per fer front a les diferents necessitats. La flexibilitat és molt més alta que en els models convencionals. S'aconsegueix que les màquines s'adaptin a la demanda real i s'evita així que hi pugui haver una sobresaturació i, per tant, una caiguda del sistema.

2.9 Informàtica en núvol

En els últims anys ha sorgit una nou concepte anomenat *informàtica en núvol* (en anglès, *cloud computing*), que permet a les empreses disposar de serveis o aplicacions d'alta disponibilitat sense necessitat de desplegar cap tipus d'infraestructura addicional. Aquesta solució ràpidament va ser adoptada per empreses de nova creació o amb pressupostos ajustats. I els seus bons resultats han fet que cada cop siguin més les companyies que estan adoptant solucions d'aquest tipus.

La informàtica en núvol és un sistema d'emmagatzematge i ús de recursos informàtics basat en el servei en xarxa, que consisteix a oferir a l'usuari un espai virtual, generalment a Internet, en què pot disposar de les versions més actualitzades de maquinari i programari.

Google Apps al Departament d'Ensenyament

L'any 2010 el Departament d'Ensenyament de Catalunya va fer la migració del seu correu intern XTEC a Google Apps, el servei de correu electrònic ofert per Google a les empreses. D'aquesta manera, els usuaris poden accedir al correu des de qualsevol dispositiu com si es tractés d'un compte de Gmail.

EyeOS

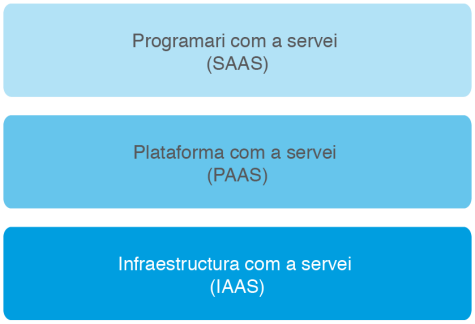
L'any 2006, un grup de joves programadors catalans van llançar al mercat el primer escriptori virtual en núvol. La idea va ser tot un èxit i en pocs mesos van tenir una gran acceptació arreu del món. L'objectiu era que els usuaris accedeixin a les seves aplicacions com si es tractés d'un sistema operatiu des de qualsevol lloc del món. Per defecte, eyeOS porta un gran nombre d'aplicacions, però a més se n'hi poden incloure d'altres i, si s'és programador, programar-ne de noves.

És un nou model de negoci que permet als usuaris accedir a un catàleg de serveis adaptables i flexibles a les necessitats de les empreses. Els usuaris paguen als proveïdors d'aquests serveis per l'ús que en fan. Aquests serveis es poden adaptar totalment a les demandes de negoci i se'n pot sol·licitar un augment o disminució si es produeix un pic o una davallada de feina. D'aquesta manera, les empreses disposen de serveis totalment flexibles sense haver-se de preocupar del maquinari, el manteniment o les actualitzacions.

Les empreses que ofereixen aquest tipus de serveis disposen d'una infraestructura basada en l'alta disponibilitat. La seva línia de negoci es basa en oferir serveis a uns clients distribuïts arreu del món i no es poden permetre una caiguda dels seus sistemes, per petita que sigui. Per evitar aquests temps d'inactivitat tenen implantats sistemes per garantir l'alta disponibilitat com la redundància en la xarxa, les xarxes d'emmagatzematge, la redundància de servidors, la redundància en el subministrament elèctric, els plans de contingència i la virtualització.

El concepte d'informàtica en núvol és molt ampli i engloba diferents models de negoci. Aquests es poden classificar de la manera següent (figura 2.4):

FIGURA 2.4. Tipus d'informàtica en núvol



- **Programari com a servei (SAAS)**: en anglès, *software as a service*. Es caracteritza per oferir com a servei una aplicació completa a la carta. Els usuaris es connecten a través d'una xarxa, habitualment Internet, al servidor del proveïdor. En aquest model de negoci no es paguen llicències de programari sinó que es paga per ús que se'n fa. Les aplicacions estan situades en una infraestructura pública. El proveïdor líder en solucions de programari com a servei és Salesforce, amb el seu CRM *customer relationship management* distribuït. No obstant això, en els últims anys han sorgit noves empreses que ofereixen aquest tipus de servei com Google Apps, Dropbox, Evernote, Basecamp o Workday.

- **Plataforma com a servei (PAAS)**: en anglès, *platform as a service*. És una solució intermèdia en què no només s'ofereix el maquinari, sinó que també contempla els elements bàsics per poder instal·lar una aplicació com són el sistema operatiu, els sistemes gestors de bases de dades i servidors d'aplicacions. Això permetrà al client instal·lar les seves pròpies aplicacions i despreocupar-se del manteniment del maquinari i del programari base. Un dels principals proveïdors de servei és Google App Engine, entre d'altres com Microsoft Azure o Force.

- **Infraestructura com a servei (IAAS)**: en anglès, *infrastructure as a service*. En aquesta capa s'ofereix com a servei la capacitat de procés i d'emmagatzematge, normalment mitjançant un plataforma de virtualització. En comptes d'adquirir servidors i habilitar centres de processament de dades, les empreses lloguen aquests recursos a un proveïdor extern. El principal proveïdor en el mercat és Amazon, amb Amazon EC2, tot i que de mica en mica van sorgint altres empreses com GoGrid o l'empresa catalana Abiquo.

Microsoft Office 365

Microsoft no ha volgut perdre el seu lideratge en paquets ofimàtics i l'any 2011 va llançar al mercat un nou producte d'informàtica en núvol, anomenat Microsoft Office 365. Aquest producte disposa de les eines ofimàtiques Excel, Word, PowerPoint, Outlook, Exchange, Sharepoint i un sistema de conferències de vídeo i àudio. Els usuaris no han d'instal·lar cap d'aquestes aplicacions, sinó que hi accedeixen per Internet i paguen una quota mensual.

Els objectius principals d'aquesta tecnologia són augmentar la flexibilitat, millorar l'accessibilitat, reduir els costos i millorar l'alta disponibilitat:

- **Alta disponibilitat**: permet a les empreses disposar de solucions d'alta disponibilitat a un preu reduït, molt per sota del que haurien d'invertir si implantessin solucions pròpies.

- **Reducció de costos**: com que l'empresa no disposa de servidors propis, no ha de realitzar la inversió inicial de tota aquesta infraestructura, que té un cost molt elevat i que, sovint, en petites i mitjanes empreses es troba infrautilitzada. A més, en no disposar de servidors propis, l'empresa no ha de destinar recursos al seu manteniment. Únicament cal adquirir uns terminals per accedir aquests serveis sense grans requisits tècnics, ja que el procés es realitza en el servidor.
- **Accessibilitat**: el fet d'utilitzar aquest tipus de solucions permet més flexibilitat en els usuaris, ja que poden accedir als recursos des de diferents tipus de dispositius, sistemes operatius i situació geogràfica.
- **Flexibilitat**: permet adaptar ràpidament els sistemes de l'empresa a les necessitats de negoci. Davant d'un creixement molt ràpid es pot donar resposta en qüestió d'hores quan en un sistema convencional es requeririen mesos de planificació i uns costos molt més elevats.

No obstant això, com qualsevol sistema que està en fase d'implantació també genera algunes incerteses en els usuaris, com, per exemple, el control del nivell de servei acordat, la dependència que genera amb el proveïdor de servei i la ubicació i seguretat de les dades.

- **Nivell de servei**: les empreses proveïdores s'han de comprometre a oferir un determinat nivell de servei prèviament acordat amb els usuaris. Sorgeixen dubtes sobre de quina manera s'estableix el nivell de servei a complir per part de les empreses proveïdores i com es pot verificar i controlar que s'estigui treballant dins dels nivells acordats.
- **Dependència**: implantar una solució d'aquest tipus genera una gran dependència amb el proveïdor de servei. Òbviament el grau de dependència dependrà del tipus d'informàtica en núvol que s'estigui aplicant, sent les solucions de programari com a servei, les PAAS, les més dependents. Sovint, en utilitzar solucions d'aquest tipus les empreses han d'adaptar la seva manera de treballar als productes oferts.
- **Ubicació de la informació**: una de les principals pors que tenen les empreses a l'hora d'implantar solucions d'aquest tipus és el fet que les dades no es trobin allotjades en la mateixa empresa, sinó que sigui una empresa externa la que tingui aquesta informació i la gestioni. Això genera als administradors incerteses sobre l'ús, la gestió i el compliment de la normativa associada a les dades.

Algunes de les solucions d'informàtica en núvol que més utilitzen les empreses són:

- **Google Apps**: és un servei de Google que ofereix a les empreses versions personalitzades dels seus propis productes: Gmail, Google Groups, Google Calendar, Google Talk, Google Docs i Google Sites. Alguns dels seus principals avantatges:

  - **Estalvi de costos**: les solucions de Google Apps permeten reduir costos de gestió i manteniment a les empreses. Es calcula que es poden reduir a una tercera part del que suposaria la implantació d'un servidor de correu propi. A goo.gl/HCOqv es detallen els càlculs de l'estalvi que suposaria una solució d'aquest tipus.
  - **Espai d'emmagatzematge superior**: la capacitat d'emmagatzematge de les bústies de correu és de 25 GB, molt superior als sistemes convencionals.
  - **Accés a través del mòbil**: permet accedir a l'aplicatiu des de dispositius mòbils Blackberry, iPhone, Windows Mobile i Android.
  - **Alta disponibilitat**: Google garanteix una disponibilitat dels seus serveis del 99,9% i utilitza la replicació síncrona de les dades entre diferents centres de dades.
  - **Control total i administratiu de les dades**: els administradors poden personalitzar totalment Google Apps per cobrir les necessitats que puguin tenir en relació a l'aparença, aspectes tècnics i empresarials.
  - **Assistència 24/7**: tot i ser molt intuïtiu i fàcil d'utilitzar ofereix assistència als administradors tots els dies de l'any les vint-i-quatre hores del dia.
  - **Compliment de la normativa i seguretat de la informació**: s'implanten les mateixes mesures de seguretat que en els serveis de Google i es garanteix la confidencialitat de les dades.

- **Dropbox**: sistema d'allotjament de fitxers multiplataforma. El servei permet emmagatzemar i sincronitzar fitxers en línia per ser consultats des de diferents dispositius. A més, també permet la compartició de fitxers entre diferents usuaris. Dropbox permet crear comptes gratuïts amb una capacitat de fins a 2 GB i de pagament fins a 1 TB per a grups de treball.

- **Evernote**: eina informàtica multiplataforma per a la gestió d'informació personal a base de notes. És una eina ideal per a executius, ja que permet centralitzar i gestionar de manera eficient informació rellevant com notes, imatges, idees... Disposa de versió gratuïta i de versió de pagament amb un capacitat d'emmagatzematge més alta.

- **Salesforce**: ofereix solucions de CRM per a la gestió dels clients, gestió d'oportunitats i campanyes de màrqueting, entre d'altres. A més, les seves funcionalitats es poden ampliar amb més de 1.000 aplicacions addicionals.

- **Endeve**: sistema de facturació en línia que permet a les empreses portar la gestió de la comptabilitat de l'empresa de manera eficient i centralitzada. Permet crear factures des de qualsevol lloc i dispositiu.

- **Google Drive**: paquet ofimàtic per treballar des de qualsevol dispositiu en l'elaboració de documents de text, fulls de càlcul, presentacions i dibuixos. Permet l'emmagatzematge i la compartició de documents entre diferents usuaris.

2.10 Contenidors

Una alternativa a la virtualització és l'ús de contenidors. Aquests permeten configurar els entorns de desplegament de manera que poden reproduir-se de forma idèntica en qualsevol màquina, independentment del sistema operatiu i la configuració de l'amfitrió.

Tot i que la utilització de **contenidors i màquines virtuals** pot semblar molt similar, no es tracta del mateix concepte.

- Els **contenidors** són molt més lleugers i pràcticament no afecten el rendiment de l'aplicació. El motiu és que utilitzen el mateix nucli del sistema operatiu. A més a més, l'espai que ocupa en disc és molt reduït, ja que només s'hi han d'afegir els fitxers específics que requereix l'aplicació que s'executa en el contenidor.
- Les **màquines virtuals** són instal·lacions completes del sistema operatiu i afegeixen capes extres a l'execució dels programes, ja que cada instrucció ha de passar pel sistema operatiu virtualitzat, el programari de virtualització, el maquinari de virtualització de l'equip hoste i el nucli del sistema operatiu hoste. Això té un cost significatiu en el rendiment. La preparació de la màquina virtual també és més costosa, en haver-se de fer una instal·lació completa i, també, requreix més espai al disc. Un avantatge de la virtualització és que es poden fer servir màquines virtuals amb diferents sistemes operatius independentment de quin estigui instal·lat a la màquina hoste (per exemple, una màquina virtual amb Linux pot executar-se en una màquina hoste amb Windows).

Informació addicional sobre contenidors

Podeu trobar-ne més informació a l'enllaç següent: goo.gl/N44YOg.

En el cas de sistemes distribuïts (una aplicació desplegada a múltiples màquines), és molt útil utilitzar contenidors, ja que només cal preparar el contenidor una vegada i instal·lar-lo en tants servidors com sigui necessari. Aquest és un dels motius pels quals Google fa servir contenidors per desplegar les seves aplicacions en lloc d'haver de configurar milers d'equips individualment. Un inconvenient, però, d'aquesta tecnologia és que no poden fer-se servir contenidors que utilitzen un sistema operatiu en una màquina amb un sistema operatiu diferent (per exemple, no es pot utilitzar un contenidor de Linux en una màquina amb Windows).

Contenidors en entorns virtualitzats

En cas d'haver de treballar amb contenidors en ordinadors amb un sistema operatiu diferent del del contenidor, es pot recórrer a la utilització de màquines virtuals. Cal tenir en compte que es perd part de l'eficiència proporcionada per aquesta tecnologia, però és habitual treballar d'aquesta manera en entorns de desenvolupament, ja que l'equip de programadors pot treballar amb el sistema operatiu que s'adapti més bé a les seves necessitats. A més a més, en aquests casos, la pèrdua de rendiment no és crítica.

Docker és un sistema de contenidors amb llicència de programari lliure.

Tot i que aquesta tecnologia dels contenidors es troba disponible des dels anys 80 al sistema operatiu UNIX, fins a l'aparició de Docker, l'any 2013, no era

gaire popular. Actualment és fàcil trobar proveïdors de serveis d'allotjament que admeten Docker i permeten fer el desplegament de les aplicacions automàticament (per exemple, Amazon Web Services i Google Cloud).

2.10.1 Linux Containers

Linux Containers és el nom del projecte darrere les tecnologies LXC, LXD i LXCFS que té com a objectiu proporcionar un entorn neutral per al desenvolupament de les tecnologies de contenidors a Linux.

- **LXC** és un conjunt d'eines per a la creació de contenidors sobre Linux.
- **LXD** proporciona una nova interfície per treballar amb LXC mitjançant una única eina de línia d'ordres i una forma de treballar més similar a la que s'utilitza habitualment amb màquines virtuals.
- **LXCFS** és un sistema de fitxer per noms d'usuari (FUSE, en anglès) que soluciona alguns problemes amb què es troben els usuaris que fan servir un sistema de contenidors.

Quan es treballa amb aquestes tecnologies es recomana utilitzar la distribució de Linux Ubuntu, ja que inclou totes les dependències necessàries, i Cannonical Ltd inclou suport a llarg termini (LTS o *long term support*, en anglès) per a LXC a les seves pròpies distribucions de tipus *LTS*.

OpenStack

OpenStack és un sistema operatiu per a núvols que permet controlar una gran quantitat de recursos mitjançant un centre de dades. Se'n pot trobar més informació a l'enllaç següent: goo.gl/SZWz5s.

El component LXC és la base del sistema de contenidors i el seu objectiu és crear un entorn el més proper possible a una instal·lació estàndard de Linux, però fent servir el mateix nucli del sistema operatiu de la màquina on s'executa.

Per altra banda, el component LXD fa servir la implementació de LXC internament, però afegeix un sistema de càrrega d'imatges per crear els contenidors. Els contenidors es gestionen de manera similar a com es faria si fossin màquines virtuals i permet realitzar aquestes operacions a través de la xarxa.

Un altre avantatge de fer servir LXD és que pot utilitzar-se conjuntament amb OpenStack (mitjançant el connector nova-lxd), de manera que es pot treballar al núvol tant amb contenidors com amb màquines virtuals de forma transparent de cara als usuaris. Això obre la porta a fer servir sistemes més avançats que incloguin servidors de càrrega i la creació automatitzada d'instàncies, per exemple, per augmentar el nombre de contenidors que serveixen una determinada aplicació segons el nombre d'usuaris connectats al sistema.

2.10.2 Contenidors: Docker

Docker és un sistema de contenidors basat en el nucli de Linux. Es tracta de programari lliure i entre els principals col·laboradors hi ha empreses com Google, IBM, Cisco, Microsoft i Red Hat.

Anteriorment, per utilitzar Docker en sistemes operatius no basats en Linux, s'utilitzava Docker Toolbox. Aquesta eina, però, es troba obsoleta i no s'ha d'utilitzar amb els sistemes operatius actuals.

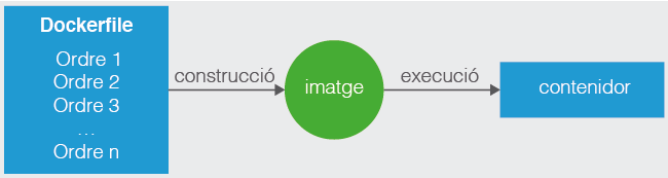
Com que es tracta d'un contenidor basat en Linux, no pot utilitzar-se directament a màquines amb altres sistemes operatius, però és possible utilitzar-lo en altres entorns de desenvolupament mitjançant la virtualització. Al seu web hi ha enllaços a instal·ladors que simplifiquen aquesta tasca i inclouen tots els fitxers necessaris per instal·lar Docker a Linux, Mac i Windows.

Alguns avantatges de desplegar una aplicació utilitzant Docker són els següents:

- L'aplicació funciona igual en el servidor de proves que en el de producció perquè l'entorn és el mateix.
- Cada aplicació es troba aïllada de la resta d'aplicacions, en el seu propi contenidor.
- No cal instal·lar cap altre component, a banda de Docker, per executar l'aplicació en un altre equip. L'aplicació funciona directament en instal·lar el contenidor, perquè totes les dependències es troben al contenidor.

Els contenidors de Docker són instàncies d'una imatge que conté tots els fitxers necessaris empaquetats per crear el contenidor en un sol fitxer. Al seu torn, aquesta imatge és construïda a partir d'un fitxer anomenat Dockerfile, que conté totes les ordres necessàries per assemblar-la (vegeu la figura 2.5).

Figura 2.5. Procés d'execució d'un contenidor



El primer pas per treballar amb contenidors de Docker és instal·lar-lo fent servir l'enllaç següent: goo.gl/n7d5qg. En aquesta pàgina es pot trobar l'instal·lador per utilitzar Docker amb Mac, Windows i diferents distribucions de Linux. La instal·lació és molt simple en tots els sistemes operatius, però en cas de dubte recordeu que podeu trobar tota la informació necessària a la mateixa pàgina de descàrrega.

Una vegada instal·lat, cal executar-lo. En la majoria de sistemes operatius, es necessiten permisos d'administrador per poder gestionar la xarxa. Per comprovar que s'ha instal·lat amb èxit, obriu una finestra amb la terminal o el símbol del sistema (segons quin sistema operatiu feu servir) i escriviu-hi *docker -v*.

El resultat ha de ser similar al següent:

```
~ $ docker –v
Docker version 17.03.1–ce, build c6d412e
```

2.10.3 Creació i desplegament d'un contenidor amb Docker

Per veure el funcionament d'un contenidor, cal crear-ne un per executar una aplicació en PHP que mostri per pantalla el missatge: "Hola món!". Primer, creeu un directori anomenat *prova-docker*, on es desaran tots els fitxers d'aquest projecte. Dintre d'aquest directori, creeu-ne un altre anomenat *src* amb un fitxer de text pla anomenat index.php i el contingut següent:

```
<?php

echo "Hola món!";
```

Repositori d'imatges per Docker

Podeu trobar imatges de Docker fiables per utilitzar com a base a l'enllaç següent: hub.docker.com. En aquest repositori hi ha tant imatges oficials (més fiables) com públiques.

Per poder executar aquesta aplicació és necessari un sistema operatiu, un servidor web (per exemple, Apache) i PHP. Per indicar a Docker que ha d'incloure la imatge, creeu un fitxer de text pla dins del directori *prova-docker* anomenat Dockerfile.

Docker requereix el nom d'una imatge per fer-la servir com a base. Aquestes imatges inclouen els fitxers propis de la distribució (per exemple, Ubuntu o Debian) i en alguns casos algunes aplicacions preinstal·lades com PHP o MySql.

L'enllaç a la imatge de Docker oficial per a PHP es troba a l'enllaç següent: hub.docker.com/_/php/. Al principi de la pàgina hi ha la llista d'imatges disponibles (vegeu la figura 2.6).

FIGURA 2.6. Imatge de Docker oficial PHP

Supported tags and respective `Dockerfile` links

- `7.1.3-cli`, `7.1-cli`, `7-cli`, `cli`, `7.1.3`, `7.1`, `7`, `latest` (*7.1/Dockerfile*)
- `7.1.3-alpine`, `7.1-alpine`, `7-alpine`, `alpine` (*7.1/alpine/Dockerfile*)
- `7.1.3-apache`, `7.1-apache`, `7-apache`, `apache` (*7.1/apache/Dockerfile*)
- `7.1.3-fpm`, `7.1-fpm`, `7-fpm`, `fpm` (*7.1/fpm/Dockerfile*)
- `7.1.3-fpm-alpine`, `7.1-fpm-alpine`, `7-fpm-alpine`, `fpm-alpine` (*7.1/fpm/alpine/Dockerfile*)
- `7.1.3-zts`, `7.1-zts`, `7-zts`, `zts` (*7.1/zts/Dockerfile*)
- `7.1.3-zts-alpine`, `7.1-zts-alpine`, `7-zts-alpine`, `zts-alpine` (*7.1/zts/alpine/Dockerfile*)
- `7.0.17-cli`, `7.0-cli`, `7.0.17`, `7.0` (*7.0/Dockerfile*)
- `7.0.17-alpine`, `7.0-alpine` (*7.0/alpine/Dockerfile*)
- `7.0.17-apache`, `7.0-apache` (*7.0/apache/Dockerfile*)
- `7.0.17-fpm`, `7.0-fpm` (*7.0/fpm/Dockerfile*)
- `7.0.17-fpm-alpine`, `7.0-fpm-alpine` (*7.0/fpm/alpine/Dockerfile*)
- `7.0.17-zts`, `7.0-zts` (*7.0/zts/Dockerfile*)
- `7.0.17-zts-alpine`, `7.0-zts-alpine` (*7.0/zts/alpine/Dockerfile*)
- `5.6.30-cli`, `5.6-cli`, `5-cli`, `5.6.30`, `5.6`, `5` (*5.6/Dockerfile*)
- `5.6.30-alpine`, `5.6-alpine`, `5-alpine` (*5.6/alpine/Dockerfile*)
- `5.6.30-apache`, `5.6-apache`, `5-apache` (*5.6/apache/Dockerfile*)
- `5.6.30-fpm`, `5.6-fpm`, `5-fpm` (*5.6/fpm/Dockerfile*)
- `5.6.30-fpm-alpine`, `5.6-fpm-alpine`, `5-fpm-alpine` (*5.6/fpm/alpine/Dockerfile*)
- `5.6.30-zts`, `5.6-zts`, `5-zts` (*5.6/zts/Dockerfile*)
- `5.6.30-zts-alpine`, `5.6-zts-alpine`, `5-zts-alpine` (*5.6/zts/alpine/Dockerfile*)

For detailed information about the published artifacts of each of the above supported tags (image metadata, transfer size, etc), please see the `repos/php` directory in the `docker-library/repo-info` GitHub repo.

Com es pot apreciar, el llistat és força extens. Si voleu més informació sobre cadascuna de les opcions, podeu consultar la mateixa pàgina. En aquest exemple es fa servir el servidor web Apache i, per consegüent, la imatge base correspon a la fila "7.1.3-apache, 7.1-apache, 7-apache, apache".

Fixeu-vos que a cada fila es mostren, d'esquerra a dreta, les opcions disponibles, de la més concreta a la més genèrica. És a dir, si s'especifica `7.1.3-apache` es farà servir la imatge amb la versió 7.1.3 de PHP i Apache, mentre que si s'especifica en el fitxer `7-apache` es farà servir una versió de PHP 7, però no sabreu quina (habitualment la més recent que s'hagi afegit a aquest repositori). En un cas encara més extrem, si només s'especifica `apache`, la versió de PHP podria ser qualsevol (per exemple, PHP 8 o 9).

Per aquests motius es recomana fer servir sempre una versió concreta. En cas contrari, es poden produir incompatibilitats en les aplicacions i, fins i tot, pot passar que a partir d'una mateixa imatge base es generin diferents imatges, ja que la versió pot canviar en qualsevol moment.

Habitualment els números de versió d'un programa indiquen les diferències següents:

- El primer indica el número de la versió, i no acostuma a ser completament compatible amb l'anterior (per exemple, PHP 7.0 no és compatible amb PHP 5.6).
- El segon número s'utilitza quan s'afegeixen noves funcionalitats.
- El tercer número indica correccions.

Així doncs, a l'hora de seleccionar una imatge, normalment només cal indicar els dos primers números de versió. Per exemple, si s'indica `7.1` com a versió, s'inclou la versió més recent amb totes les correccions actualitzades.

Per indicar a Docker la imatge base, es fa amb l'ordre FROM seguida del nom del repositori (php), dos punts (:) i el nom de la imatge (per exemple, `7.1-apache`):

```
1 FROM php:7.1-apache
```

Com que es vol copiar l'aplicació dins del contenidor, cal utilitzar l'ordre COPY indicant la ruta d'origen i la ruta de destí:

```
1 COPY src/ /var/www/html
```

Aquesta és la ruta que utilitza aquesta imatge en concret, que està basada en la distribució de Debian de Linux. Per saber a quina distribució pertany una imatge i tot el que conté, només cal clicar l'enllaç a la dreta de cada fila per accedir al fitxer Dockfile utilitzat per crear-la.

Finalment, cal indicar a Docker que cal exposar el port 80 del contenidor per poder accedir a la pàgina web. Per fer-ho s'utilitza l'ordre `EXPOSE`:

```
EXPOSE 80
```

Així doncs, el contingut del fitxer Dockerfile per crear la imatge ha de ser:

```
FROM php:7.1-apache
COPY src/ /var/www/html
EXPOSE 80
```

Una vegada creat el fitxer Dockerfile i desat dintre de la carpeta *prova-docker*, per generar la imatge heu d'escriure a la línia d'ordres:

```
docker build -t hola-mon .
```

El paràmetre `-t` es fa servir per indicar el nom de la imatge (en aquest cas, "hola-mon") i el punt final indica que es crearà en el mateix directori. Una vegada es premi la tecla retorn, començaran a descarregar-se els fitxers necessaris per crear la imatge.

El resultat ha de ser similar al següent:

```
~/prova-docker $ docker build -t hola-mon .
Sending build context to Docker daemon 3.584 kB
Step 1/3 : FROM php:7.1-apache
7.1-apache: Pulling from library/php
6d827a3ef358: Pull complete
87fe8fbc743a: Pull complete
f6d1a8d304ab: Pull complete
caf3547d9b73: Pull complete
1004db2760ff: Pull complete
66e2d66a547e: Pull complete
bbfaa62c234a: Pull complete
19ce8807f4d1: Pull complete
63f8d35ca798: Pull complete
a5594b4d2a52: Pull complete
42f1cbd038cf: Pull complete
a739656e85cb: Pull complete
97b6a5f245a1: Pull complete
Digest: sha256:c865c723fbe6a41ccc9006c6c3f3c0225ad06f3ab69c752419d6cd8f7ca51e5e
Status: Downloaded newer image for php:7.1-apache
 ---> b177bfebca36
Step 2/3 : COPY src/ /var/www/html
 ---> a021f0647910
Removing intermediate container 4db2b286aeca
Step 3/3 : EXPOSE 80
 ---> Running in f1da636d83b5
 ---> e991d0ca6063
Removing intermediate container f1da636d83b5
Successfully built e991d0ca6063
```

Seguidament, per executar el contenidor, heu d'escriure des de la línia d'ordres:

```
docker run -p 80:80 hola-mon
```

L'opció `run` indica que es vol executar una instància de la imatge "hola-mon". Fixeu-vos que el nom de la imatge ha d'anar al final de l'ordre. L'opció `-p` indica la redirecció de ports (és el primer el port de la màquina hoste i el segon el port del contenidor). És a dir, s'executarà el contenidor "hola-mon" i es podrà accedir al seu port 80 des del port 80 de la màquina hoste.

El resultat d'executar-lo ha de ser similar al següent:

```
AH00558: apache2: Could not reliably determine the server's fully qualified
    domain name, using 172.17.0.2. Set the 'ServerName' directive globally to
    suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified
    domain name, using 172.17.0.2. Set the 'ServerName' directive globally to
    suppress this message
[Sat Apr 08 12:36:18.758692 2017] [mpm_prefork:notice] [pid 1] AH00163: Apache
    /2.4.10 (Debian) PHP/7.1.3 configured -- resuming normal operations
[Sat Apr 08 12:36:18.758735 2017] [core:notice] [pid 1] AH00094: Command line:
    'apache2 -D FOREGROUND'
```

Tot i que es mostren missatges d'advertència d'Apache, l'aplicació ha de funcionar correctament. Per comprovar-ho només heu d'obrir el vostre navegador i introduir com a URL "localhost". Hauria de mostrar-se per pantalla el missatge "Hola món!".

En cas de voler utilitzar un port diferent de la màquina hoste (per exemple, el 8080, per accedir des de l'URL `localhost:8080`), només cal executar la imatge canviant aquest port, tal com es mostra en l'exemple següent:

```
docker run -p 8080:80 hola-mon
```

Si proveu de modificar el fitxer index.php i actualitzeu la pàgina al navegador, veureu que els canvis no s'hi veuen reflectits. Això és d'esperar, perquè l'aplicació s'ha copiat dins del contenidor. Si es vol actualitzar l'aplicació, cal tornar a construir el contenidor.

Hi ha casos en què aquest comportament no és el desitjat (per exemple, durant el desenvolupament). Per solucionar aquest problema, Docker ofereix l'opció de muntar volums que funcionaran com a directoris compartits entre la màquina hoste i el contenidor.

Per muntar un volum, s'ha de fer des de la línia d'ordres utilitzant l'opció `-v` i indicant el nom del directori de la màquina hoste, dos punts (:), i el nom del directori al contenidor.

```
docker run -p 80:80 -v /provar-docker/src/:/var/www/html/ hola-mon
```

Cal destacar que s'ha d'utilitzar la ruta absoluta. No és vàlid fer servir ~ per indicar que es tracta de la carpeta de l'usuari actual a Linux o Unix, ni `..` per indicar que es tracta del directori pare.

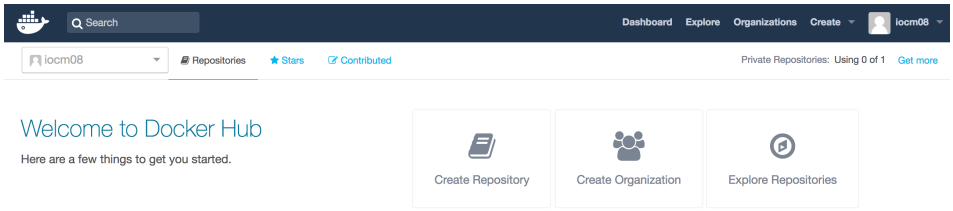
Fixeu-vos que, per muntar un contenidor, s'ha de fer des de la línia d'ordres i no al fitxer Dockerfile: d'aquesta manera s'evita que es trenqui la portabilitat. Com que es tracta de recursos externs al contenidor, Docker no pot assegurar que aquests estiguin disponibles en qualsevol equip.

Si llisteu el contingut del vostre directori, no veureu la imatge creada enlloc. Això és normal: no forma part de la vostra aplicació i no tindria sentit que es mostrés en aquest directori. Per veure un llistat de les imatges instal·lades, s'utilitza l'ordre docker images i el resultat serà similar al següent:

```
REPOSITORY          TAG                 IMAGE ID            CREATED
                SIZE
hola-mon            latest              e991d0ca6063        56 minutes ago
          387 MB
php                 7.1-apache          b177bfebca36        2 weeks ago
             387 MB
```

Per poder desplegar l'aplicació l'heu de pujar al repositori d'imatges de Docker. Per fer-ho, necessiteu crear un compte a Docker Hub (hub.docker.com). Una vegada creat el compte i confirmat mitjançant l'enllaç rebut al correu, podeu connectar amb la pàgina (vegeu la figura 2.7).

FIGURA 2.7. Pàgina principal d'usuari a Docker Hub



Per poder pujar la imatge al repositori, heu d'autenticar-vos amb el nom d'usuari i la contrasenya des de la línia d'ordres, fent servir l'ordre `docker login`. No cal passar cap paràmetre, però us demanarà el nom d'usuari i la contrasenya. El resultat serà similar al següent:

```
~/prova-docker $ docker login
Login with your Docker ID to push and pull images from Docker Hub. If you don't
     have a Docker ID, head over to https://hub.docker.com to create one.
Username: iocm08
Password:
Login Succeeded
```

El següent pas és etiquetar la imatge per pujar-la al repositori. Per fer-ho, cal saber l'identificador (ID) de la imatge i fer servir l'ordre `docker tag` seguida de l'ID, l'espai de noms (que es correspon amb el nom d'usuari de Docker Hub), el nom del repositori, dos punts (:) i l'etiqueta (*tag*, en anglès).

Podeu veure l'identificador de la imatge executant l'ordre docker images, que us mostrarà el llistat d'imatges amb el seu repositori, l'etiqueta, l'identificador, quant fa que es va crear i la mida.

Per exemple, per poder pujar el contenidor amb identificador "0991d0ca6063" al repositori "iocmo8/hola-mon", cal executar l'ordre següent:

```
docker tag e991d0ca6063 iocm08/hola-mon:latest
```

En executar docker images, el resultat serà similar al següent:

```
~/prova-docker $ docker images
REPOSITORY            TAG                 IMAGE ID            CREATED
                SIZE
hola-mon              latest              e991d0ca6063        2 hours ago
             387 MB
iocm08/hola-mon       latest              e991d0ca6063        2 hours ago
             387 MB
```

```
5 php                 7.1-apache          b177bfebca36        2 weeks ago
            387 MB
```

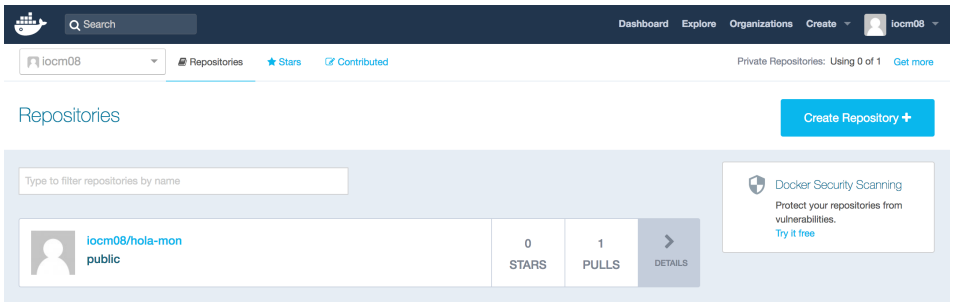
Fixeu-vos que a banda de la imatge utilitzada com a base i la imatge del contenidor creat originalment, s'ha afegit una nova imatge que inclou l'espai de noms, però conserva l'identificador original.

Seguidament, podeu pujar la imatge a Docker Hub fent servir l'ordre `docker push`, i el resultat serà similar al següent:

```
1  The push refers to a repository [docker.io/iocm08/hola-mon]
2  2c16acb979ce: Pushed
3  1c6da1b67140: Mounted from library/php
4  524998ac985c: Mounted from library/php
5  b0048e0cd0f0: Mounted from library/php
6  0739f0fe8939: Mounted from library/php
7  8f3f5d50c083: Mounted from library/php
8  46af8a5b5036: Mounted from library/php
9  4b63183c9b32: Mounted from library/php
10 5e34f9b1cc0a: Mounted from library/php
11 882b0937fe95: Mounted from library/php
12 6b42159d1088: Mounted from library/php
13 0e985d879eb0: Mounted from library/php
14 2b6ca8b57a27: Mounted from library/php
15 5d6cbe0dbcf9: Mounted from library/php
16 latest: digest: sha256:
       bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf size:
       3242
```

Si actualitzeu la pàgina web amb l'usuari autenticat a Docker Hub, veureu com ha aparegut el repositori "hola-mon", tal com apareix a la figura 2.8).

FIGURA 2.8. Pàgina principal d'usuari a Docker Hub



Per poder provar que el contenidor s'ha pujat correctament, podeu descarregar-lo i provar de posar-lo en marxa, però primer heu d'eliminar la imatge creada. Per eliminar una imatge o un *tag*, s'ha d'utilitzar l'ordre `docker rmi`, indicant el nom de la imatge i l'etiqueta en cas que aquesta no sigui "latest" (que fa referència a l'última).

És possible que alguna de les imatges o etiquetes siguin utilitzades per algun contenidor (encara que els contenidors s'hagin aturat). Per forçar-ne l'eliminació, s'ha de fer servir l'opció `-force`. Així doncs, per eliminar la imatge "hola-mon" i l'etiqueta "iocm08/hola-mon", suposant que la segona estigui sent utilitzada, es fa de la manera següent:

```
1 docker rmi hola-mon
2 docker rmi iocm08/hola-mon --force
```

El resultat serà similar al següent:

```
Untagged: hola-mon:latest
Untagged: iocm08/hola-mon:latest
Untagged: iocm08/hola-mon@sha256:
    bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf
Deleted: sha256:
    e991d0ca60632dcf5795cb8e18da70f3aa814b0309539c003ad0bbb468686f7d
Deleted: sha256:
    a021f0647910f846584fdd047aa9e4ec5fb9aebfcbfa2e0ff08c843ac7f10ada
```

Si executeu l'ordre `docker images`, comprovareu que només hi ha la imatge base utilitzada per crear la vostra imatge:

```
~/prova-docker $ docker images
REPOSITORY            TAG                 IMAGE ID            CREATED
                  SIZE
php                   7.1-apache          b177bfebca36        2 weeks ago
             387 MB
```

Per acabar, podeu descarregar la imatge utilitzant l'ordre `docker pull` i indicant el repositori on es troba (espai de noms i nom del repositori). Aquesta informació també es pot trobar a la pàgina d'usuari de Docker Hub fent clic al repositori que vulgueu descarregar. Per exemple, per descarregar la imatge del repositori "iocm08/hola-mon", heu d'utilitzar l'ordre següent:

```
docker pull iocm08/hola-mon
```

El resultat que obtindreu serà similar al següent:

```
~/prova-docker $ docker pull iocm08/hola-mon
Using default tag: latest
latest: Pulling from iocm08/hola-mon
6d827a3ef358: Already exists
87fe8fbc743a: Already exists
f6d1a8d304ab: Already exists
caf3547d9b73: Already exists
1004db2760ff: Already exists
66e2d66a547e: Already exists
bbfaa62c234a: Already exists
19ce8807f4d1: Already exists
63f8d35ca798: Already exists
a5594b4d2a52: Already exists
42f1cbd038cf: Already exists
a739656e85cb: Already exists
97b6a5f245a1: Already exists
a8f59612df6a: Already exists
Digest: sha256:bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf
Status: Downloaded newer image for iocm08/hola-mon:latest
```

Un cop més, podeu utilitzar l'ordre `docker images` per comprovar que la imatge és al sistema i que pot executar-se amb `docker run`. Per exemple, en el cas del contenidor "iocm08/hola-mon" el resultat seria el següent:

```
~/prova-docker $ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
                  SIZE
iocm08/hola-mon     latest              e991d0ca6063        2 hours ago
             387 MB
```

```
4 php                 7.1-apache          b177bfebca36        2 weeks ago
            387 MB
```

I per executar-lo es faria servir aquesta ordre:

```
1 docker run iocm08/hola-mon
```

Fixeu-vos que tot i que el contenidor original no feia servir cap espai de noms, quan s'utilitza una imatge descarregada s'ha d'incloure. En cas contrari, Docker no la troba.

Com heu pogut comprovar, començar a utilitzar Docker no és excessivament complicat, però dominar totes les seves opcions i els desplegaments a una escala major és força complex. Cal tenir en compte que aquí només s'ha presentat un exemple molt simple, però que us pot servir per iniciar-vos en la utilització de contenidors.

Altres aspectes de la utilització de Docker que cal tenir en compte són els següents:

- Quan acaba la tasca que s'està executant al contenidor, el contenidor s'atura automàticament.
- Cada aplicació s'executa en un contenidor diferent, ja que cada contenidor està lligat a un únic procés.
- Un mateix equip pot tenir múltiples contenidors funcionant al mateix temps. Per veure els contenidors en execució es pot fer servir l'ordre `docker ps`.
- Docker fa servir un sistema de capes per generar les imatges; aquestes capes es corresponen amb les línies del fitxer Dockerfile.
- Per automatitzar el desplegament s'acostuma a utilitzar altres eines i serveis de desplegament com Kubernetes (kubernetes.io) o Ansible (www.ansible.com).