UOC Universitat Oberta de Catalunya

SOC Servei d'Ocupació de Catalunya

Aplicacions avançades dels sistemes operatius

Continguts

Xavier Morera Martínez

1 crèdit

Generalitat de Catalunya
Departament d'Empresa i Ocupació

Unió Europea
Fons social europeu
L'FSE inverteix en el teu futur

Continguts

1. Conceptes bàsics dels sistemes operatius

1.1 Introducció als sistemes operatius

De definicions de *sistema operatiu* en podem trobar gairebé tantes com fonts documentals de què parlen. Tot i la majoria es posen d'acord en els trets generals, és a l'hora d'entrar en els matisos quan les diferències es fan evidents.

Ens apareix el terme ***sistema*** que, entendrem com a conjunt d'elements que tenen alguna característica o funció en comú. De fet, la primera característica comuna que trobem en el cas dels elements que formen un sistema operatiu és que són, tots ells, elements de **programari** (***software***). El terme ***operatiu*** fa referència al fet que aquest conjunt d'elements de programari tindran com a objectiu final aconseguir que tots els dispositius de **maquinari** (***hardware***) que tenim en un ordinador puguin fer una tasca o un conjunt de tasques que proporcionin una utilitat pràctica als usuaris finals d'una forma eficient; és a dir, que el maquinari –entenent com a tal tots els dispositius en conjunt– tingui un nivell d'operativitat mínim, sigui, en definitiva, operatiu.

Elements de maquinari
Elements físics, de naturalesa tangible. Dins d'aquest grup tindrem tot l'aparellatge que forma el sistema: ordinadors, dispositius d'entrada, de sortida, d'emmagatzematge, dispositius de comunicació (xarxes), etc. Actualment, la majoria d'aquests elements tenen com a base tecnològica la microelectrònica.

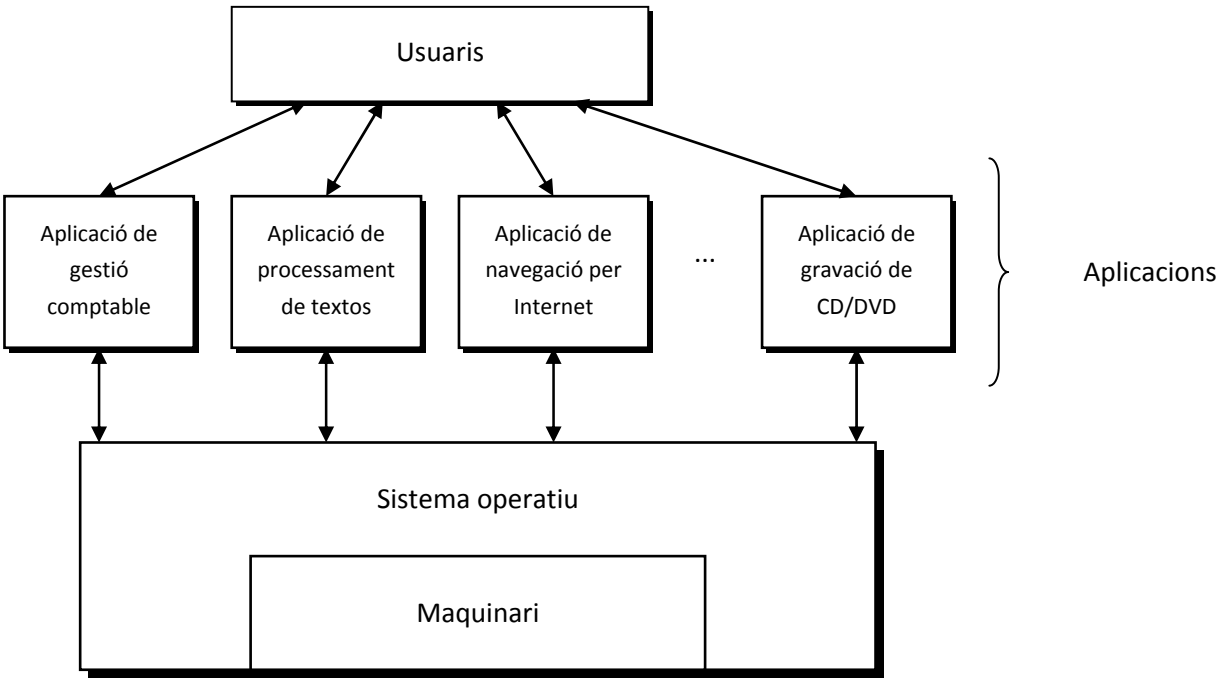
Elements de programari
Elements de naturalesa intangible que no tenen una existència física. Estan inclosos en aquest grup els programes o les aplicacions, les dades i les configuracions, que governen el funcionament dels elements de maquinari fent possible que tinguin una utilitat pràctica per als usuaris finals del sistema.

Però, per què és necessari aquest conjunt d'elements de programari –anomenat *sistema operatiu*– per tal de poder obtenir una utilitat pràctica o concreta del conjunt de dispositius físics de la màquina? Bé, la resposta és, en essència, l'enorme complexitat de funcionament que presenta el maquinari. Aquesta complexitat faria inviable obtenir cap mena de rendiment del conjunt de dispositius de maquinari si, com a usuaris, els haguéssim d'encomanar directament la feina que volem que ens facin. Per simplificar l'ús del maquinari, el sistema operatiu fa d'intermediari de tal manera que rep, d'una banda, les ordres dels usuaris –especificades d'una forma senzilla i fàcil d'interpretar per les persones– i les transforma en ordres cap als dispositius afrontant tota la complexitat implícita en el funcionament d'aquests dispositius.

Ara podem, doncs, definir què és un sistema operatiu:

> **Sistema operatiu**: conjunt d'elements de programari que actua com a intermediari entre els usuaris i el maquinari d'un ordinador, amb l'objectiu de poder obtenir una utilitat pràctica final del maquinari, d'una manera còmoda per als usuaris i utilitzant els recursos dels dispositius d'una manera eficient.

De fet, si volem ser estrictes amb l'explicació que estem donant, hem de dir que el sistema operatiu ens ofereix un entorn que permet l'execució d'aplicacions i que, aquestes aplicacions, són les que finalment acaben proporcionant les diverses utilitats pràctiques als usuaris. Vegem-ho amb el diagrama següent, que ens mostra alguns exemples d'aquestes utilitats:



Interrelacions entre maquinari, sistema operatiu, aplicacions i usuaris d'un sistema informàtic

Cal dir també que els sistemes operatius que podem trobar en el món real solen anar acompanyats d'un conjunt més o menys ampli d'aplicacions (programes) finals, a banda de proporcionar-nos el programari que compon pròpiament el sistema operatiu. D'aquesta manera, el mateix sistema operatiu ja ens ofereix, d'entrada i sense haver d'instal·lar cap aplicació complementària, un paquet mínim d'utilitats que ens permeten cobrir les necessitats més bàsiques dels usuaris.

1.2 Evolució històrica dels sistemes operatius

L'evolució dels sistemes operatius ha anat de manera paral·lela a la dels ordinadors.

Les principals causes de l'evolució dels sistemes operatius es poden resumir en les següents:

- Actualització i nous tipus de maquinari
- Demanda de nous serveis
- Necessitat de resoldre diferents tipus d'errors: *bugs*, vulnerabilitats, etc.

És força habitual parlar de generacions en la història de la informàtica. Cal destacar, però, que no hi ha una unanimitat a l'hora de definir o delimitar aquestes generacions, ni tan sols temporalment. Sovint, la visió històrica varia segons el punt de vista social, o per qüestions polítiques:

Primera generació: els primers sistemes de computadors (1945-1955)

Els principis de la informàtica venen marcats pel fet que només existia el maquinari i que encara no s'utilitzaven els transistors (dispositiu electrònic que, a partir de les generacions següents, permetrà un salt qualitatiu en la tecnologia del maquinari informàtic). La tecnologia utilitzada es basava en les vàlvules de buit o vàlvules termoiòniques. La mida d'aquestes vàlvules obligava a fer unes màquines molt grans.

L'àmbit d'ús d'aquests primers computadors era el militar i la funció era fer càlculs matemàtics com, per exemple, calcular trajectòries balístiques. Els dispositius que s'utilitzaven eren cintes de paper i targetes perforades. Els programes s'escrivien en llenguatge de màquina i no existia el concepte de *llenguatge de programació*. Cada màquina tenia el seu propi llenguatge i sovint els computadors es programaven cablant directament el maquinari, fent que aquest procés de programació de les màquines fos complex i poc productiu.

En aquesta època es considera que no hi havia el concepte de *sistema operatiu*, ja que l'usuari interactuava directament amb la màquina.

Segona generació: l'aparició del transistor (1955-1965)

A mitjan dècada dels anys cinquanta va aparèixer el transistor, la qual cosa va permetre construir computadors molt més fiables, petits i ràpids (els càlculs es duien a terme en unitats de temps de l'ordre dels microsegons o, el que és el mateix, els processadors arribaven a velocitats de fins a 1 MHz). Això va permetre que es poguessin fabricar computadors

amb la idea de vendre'ls. A causa de l'alt preu dels primers computadors, els primers usuaris van ser les grans corporacions i institucions com l'exèrcit, les universitats i els governs.

Pel que fa als dispositius, cal destacar l'aparició dels primers perifèrics: dispositius d'entrada/ sortida (E/S) (lectors de targetes perforades i impressores) i dispositius d'emmagatzematge (unitats de disc i cintes magnètiques).

Vistes les millores en l'àmbit de maquinari, es va fer necessari desenvolupar els primers programes que permetessin obtenir rendibilitat de l'ús d'aquestes noves tecnologies. Van aparèixer els primers llenguatges de programació, com el Fortran i el Cobol, i els primers programes per al desenvolupament d'aplicacions (carregadors, muntadors, compiladors, biblioteques de funcions matemàtiques i rutines per al control de dispositius d'E/S).

Aquests primers sistemes ja utilitzaven els passos habituals del desenvolupament d'aplicacions amb llenguatges compilats (creació del codi font, compilació, muntatge, execució i depuració). Aquests elements de programari normalment no es consideren part del sistema operatiu, però sí que podem considerar sistema operatiu, encara que sigui molt rudimentari, el conjunt de rutines per a treballar amb els dispositius d'E/S, juntament amb les aplicacions que permetien carregar els programes a l'ordinador.

El principal problema d'aquesta època era la diferència de velocitat entre la CPU i els dispositius d'E/S. La baixa velocitat dels perifèrics feia que no s'obtingués el màxim rendiment de l'ús de la CPU (el processador estava molt de temps aturat esperant rebre dades dels dispositius). Per aquesta raó, es van implementar diferents tècniques com el processament per lots, el processament fora de línia, la gestió de cues i els sistemes de memòria intermèdia (*buffers*).

Tercera generació: l'aparició dels circuits integrats (1965-1980)

Aquesta generació sorgeix a mitjan anys seixanta i es basa en l'aparició d'una nova tecnologia electrònica: la integració de circuits. Els circuits integrats permeten desenvolupar màquines més ràpides i molt més petites. També cal destacar l'abaratiment de costos, que va permetre que els ordinadors es comencessin a utilitzar en empreses mitjanes i va afavorir l'aparició d'un sector informàtic comercial.

Respecte als dispositius, la diferència més destacada és la millor eficiència i velocitat. També cal destacar l'aparició dels terminals remots, que permetien accedir a bancs de dades a distància.

Pel que fa al programari, cal destacar l'aparició dels primers llenguatges de programació universals pensats per a poder-se utilitzar en diferents plataformes de

maquinari. En aquesta època s'estandarditzen els llenguatges de programació ja existents i n'apareixen d'altres com el Basic o el Pascal.

Cal destacar, també, l'aparició dels primers sistemes multiusuari i/o multitasca. Fins ara, tots els programes s'executaven de manera seqüencial, però amb l'aparició de la multiprogramació apareix el concepte de *compartició de temps de CPU* (en sistemes de temps compartit i sistemes de temps real). La compartició de temps de CPU permet fer un ús més eficient del processador, ja que pot continuar treballant en l'execució d'altres processos mentre un determinat procés està en espera dels resultats d'una operació d'E/S.

Quarta generació: integració de circuits a gran escala i a molt gran escala (1980-?)

El gran canvi d'aquesta generació és la introducció de la integració a gran escala de circuits electrònics: les tecnologies anomenades *LSI* (integració a gran escala o *large scale integration*) i *VLSI* (integració a molt gran escala o *very large scale integration*). Aquestes tecnologies van permetre reduir els costos fins a fer possible l'obertura del mercat de la informàtica als usuaris domèstics. També cal destacar els constants increments de velocitat marcats per la famosa llei de Moore que ens han portat des dels primers sistemes treballant a velocitats de desenes de MHz fins als sistemes actuals que treballen a velocitats de l'ordre de Ghz.

En l'àmbit dels dispositius, cal destacar l'aparició de múltiples tecnologies de comunicacions entre ordinadors que donarien lloc a les primeres xarxes, l'evolució de les quals ens ha dut a les actuals xarxes de tipus LAN (xarxa d'àrea local o *local area network*) i xarxes de tipus WAN (xarxa d'àrea estesa o *wide area network*), la més coneguda de les quals és Internet. Com a conseqüència d'això, es produeix l'aparició dels sistemes operatius amb capacitat per a treballar en xarxa i l'aparició dels primers sistemes distribuïts que permeten la compartició de recursos entre màquines remotes.

També apareix el concepte de *sistema operatiu en temps real*, molt utilitzat en entorns industrials. Aquests sistemes operatius estan orientats a obtenir temps de resposta ràpids en l'execució de determinats processos amb independència de l'ús efectiu que es faci dels dispositius i dels recursos.

1.3 Recursos. Funcions d'un sistema operatiu

Els sistemes operatius, en la seva condició de capa de programari que possibiliten i simplifiquen el maneig de la computadora, ocupen una sèrie de funcions bàsiques essencials per a la gestió de l'equip. Entre les més destacables, cadascuna exercida per un component intern (mòdul en nuclis monolítics i servidor en micronuclis), podem ressenyar les següents:

- Proporcionar més comoditat en l'ús d'un computador.
- Gestionar de manera eficient els recursos de l'equip, executant serveis per als processos (programes).
- Brindar una interfície a l'usuari, executant instruccions (comandaments).
- Permetre que els canvis deguts al desenvolupament del propi sistema operatiu es puguin realitzar sense interferir amb els serveis que ja es prestaven (evolutivitat).

Un sistema operatiu ocupa cinc funcions bàsiques en l'operació d'un sistema informàtic:

- Subministrament d'interfícies a l'usuari
- Administració de recursos
- Administració d'arxius
- Administració de tasques
- Servei de suport i utilitats

1.4 Gestió de recursos d'un sistema operatiu

1.4.1 Processos

Tot sistema operatiu implementa un conjunt de tecnologies que permeten a l'ordinador fer determinades funcions. El nucli o *kernel* crea un **procés** assignant-li memòria i carregant el codi del programa des d'un disc o un altre dispositiu de memòria al nou espai, que s'ha reservat per al procés. Seguidament l'executa.

> Un **programa** és una seqüència d'instruccions o accions definides *a priori* que poden ser executades per un processador.
>
> Un **procés** és una seqüència d'accions derivades de l'execució d'una sèrie d'instruccions. Això implica que un procés pot requerir l'execució d'un programa o diversos, i que un programa pot formar part de més d'un procés.

Les operacions més comunes que podem trobar en la gestió de processos són les següents:

1) **Crear** és la tècnica que permet crear processos en la qual, en alguns casos, és necessari passar arguments (nom, prioritat, recursos, etc.). Un procés també pot crear un nou procés; en aquest cas, el procés creador s'anomena ***procés pare***, i el que s'ha creat, ***procés fill***.
2) **Destruir un procés.** Elimina un procés del sistema operatiu i retorna els seus recursos al sistema.
3) **Canviar la prioritat d'un procés**.
4) **Adormir o bloquejar l'execució d'un procés.** És una tècnica mitjançant la qual un procés passa a un estat de bloqueig fins que no ha passat un temps determinat.
5) **Despertar un procés** és una manera artificial de desbloquejar processos adormits.
6) **Suspendre un procés.** S'utilitza en moments de mal funcionament del sistema, sobrecàrrega, etc.
7) **Continuar un procés** és activar un procés suspès.

1.4.2 Gestió de la memòria

La gestió de memòria implica, entre d'altres, les tasques següents:

- Portar un registre de les zones que queden lliures (és a dir, que cap procés no les utilitza), de les zones ocupades i, en aquest cas, de quins processos les ocupen.

- En els processos en què no totes les dades o codi del procés no s'ubiquen en la memòria principal, se n'ha de passar una part al disc (o memòria secundària) o viceversa.

La **memòria virtual** és una tècnica de gestió que, combinada amb el maquinari i el programari, permet executar programes carregats parcialment en la memòria real, és a dir, programes que ocupen més espai que la memòria real. La memòria virtual és la separació de la memòria lògica de l'usuari de la memòria física. Aquesta separació proporciona als programadors una gran memòria virtual quan només es disposa d'una memòria física petita. La memòria virtual facilita les tasques de programació, ja que el programador no s'ha de preocupar per la quantitat de memòria física disponible.

1.4.3 Gestió d'E/S

Els dispositius que permeten l'intercanvi d'informació entre el processador i la memòria són els dispositius perifèrics. No és fàcil que els processos utilitzin d'una manera directa els perifèrics; per tant, els processos no necessiten conèixer les característiques dels perifèrics, sinó únicament intercanviar dades. Normalment, el programari de gestió de les operacions d'E/S d'un sistema representa un tant per cent molt elevat del total del programari que forma el sistema operatiu

Una altra característica del gestor d'E/S és que ofereix una interfície als programes d'usuari que permet manipular de la mateixa manera tots els perifèrics gestionats pel sistema operatiu. La interfície, doncs, és independent del dispositiu i no és necessari modificar els programes si es canvia de perifèric.

Una de les funcions principals d'un sistema operatiu és controlar tots els dispositius d'E/S d'un ordinador. Les principals funcions són enviar ordres als dispositius, detectar les interrupcions, controlar els errors i proporcionar una interfície entre els dispositius i la resta del sistema.

Aquesta interfície entre els dispositius i la resta del sistema ha de ser senzilla i fàcil d'utilitzar, i ha de ser la mateixa (preferentment) per a tots els dispositius (independència del dispositiu).

1.4.4 Sistema de fitxers

Des del punt de vista dels usuaris, els arxius són grups d'informacions relacionades sobre les quals podem fer diverses operacions (lectura, escriptura, eliminació, actualització, etc.). El sistema operatiu serà el responsable de fer aquestes operacions. En concret, la part del sistema operatiu que se n'encarrega s'anomena ***sistema d'arxius***, o ***sistema de fitxers***, i la seva missió és la següent:

1) Gestionar l'emmagatzematge. Decidir com s'ha d'assignar l'espai d'emmagatzematge disponible en els fitxers. Quan un usuari vol crear un arxiu, el sistema li ha d'assignar un espai perquè pugui emmagatzemar la informació. Aquest espai l'obtindrà a partir de l'espai lliure disponible. També cal considerar que arribarà un moment determinat en què l'usuari deixarà de necessitar un fitxer i l'eliminarà, i aleshores el sistema haurà d'incorporar aquest nou espai lliure al total disponible.

2) Definir mètodes d'accés. Definir la manera com l'usuari pot accedir a la informació emmagatzemada.

3) Protegir els arxius i garantir-ne la integritat. Garantir la integritat i la privacitat de la informació continguda.

Hi ha diferents criteris i tècniques per a fer aquestes tasques i cada sistema serà dissenyat segons les que responen millor a les seves necessitats i als seus objectius.

Els **drets** en els fitxers són unes capacitats assignades als usuaris per a fer determinades tasques en el sistema informàtic. En són exemples: la gestió d'usuaris per persones diferents de l'administrador, la gestió del sistema de còpies de seguretat, etc.

Els **permisos** en els fitxers són autoritzacions assignades a usuaris determinats per a fer unes accions concretes en els fitxers (per exemple, tenir el permís de lectura i d'escriptura en un fitxer, tenir el permís d'execució en un fitxer, etc.).

Els **atributs** en els fitxers són característiques que tenen els fitxers i afecten tots els usuaris que utilitzen aquests fitxers (per exemple, els fitxers comprimits, els fitxers xifrats, etc.).

1.5 Sistemes operatius més usuals

En aquest apartat, veurem els diferents tipus de sistemes operatius que podem trobar en funció d'algunes de les seves principals característiques. En concret, definirem quatre classificacions de les moltes que es podrien arribar a establir en funció de múltiples criteris.

a) En funció del nombre d'usuaris que poden treballar de manera simultània sobre el sistema operatiu, podrem tenir:

– **Sistemes operatius monousuari**: són els sistemes operatius que estan pensats per a facilitar el treball d'un únic usuari de manera simultània, facilitant-li un accés gairebé exclusiu als recursos disponibles. Actualment, molts dels sistemes d'aquest tipus tenen característiques pròpies dels sistemes multiusuari, tot i estar orientats al treball d'un únic usuari.

– **Sistemes operatius multiusuari**: són els sistemes operatius que permeten el treball simultani de diversos usuaris, els quals comparteixen els recursos del sistema i controlen les possibles interferències que hi pugui haver entre ells mitjançant els mecanismes de seguretat apropiats.

b) En funció del nombre de processos que es poden executar (que poden estar actius) de manera simultània sobre el sistema operatiu, podrem tenir:

– **Sistemes operatius monoprocés o monotasca**: són els sistemes operatius que estan pensats per a executar un únic procés o tasca de manera simultània i que disposen dels recursos del sistema de manera gairebé exclusiva.

– **Sistemes operatius multiprocés o multitasca**: són els sistemes operatius que permeten executar diversos processos de manera simultània, els quals comparteixen els recursos del sistema i controlen les possibles interferències que hi pugui haver entre ells (consum excessiu de recursos, accés a recursos aliens, etc.).

c) En funció del nombre de processadors que el sistema operatiu és capaç de gestionar, podrem tenir:

– **Sistemes operatius monoprocessador**: són els sistemes operatius capaços de gestionar un únic processador o nucli, que serà l'encarregat d'executar tots els programes i processos que s'activin. Si la plataforma de maquinari proporciona diversos processadors o nuclis, el sistema no serà capaç de treure el màxim rendiment d'aquesta característica.

– **Sistemes operatius multiprocessador**: són els sistemes operatius capaços de gestionar diversos processadors o nuclis. L'execució de programes i processos es reparteix (segons una estratègia determinada) entre els diversos processadors o nuclis disponibles.

d) Des del punt de vista de la possibilitat, o no, d'establir un temps màxim de resposta per als programes que s'executen tenim:

– **Sistemes operatius de temps compartit**: sistemes operatius que reparteixen el temps d'execució d'una manera més o menys equitativa entre tots els processos d'usuari actius, de tal manera que el temps de resposta de cadascun dependrà directament del nivell de càrrega del sistema.

– **Sistemes operatius de temps real**: sistemes que permeten donar una prioritat destacada a alguns dels processos actius de tal manera que s'executen molt per sobre de la resta, i així permeten garantir un temps de resposta mínim independentment del nivell de càrrega del sistema.

– La taula següent ens mostra en quines d'aquestes classificacions encaixa cadascun dels sistemes operatius actuals i antics que han tingut més difusió en l'entorn de l'arquitectura PC:

Sistema Operatiu	Mono usuari	Multi-usuari	Mono-procés	Multi-procés	Mono processador	Multi-processador	Temps real	Temps compartit
MS-DOS	X		X		X		X	
Windows 95/98/Me	X			X	X		X	
Windows NT Workst.	X			X		X	X	
Windows NT Server		X		X		X		X
Windows 2000 Prof.	X			X		X	X	
Windows 2000 Server		X		X		X		X
Windows XP	X			X		X	X	
Windows Vista	X			X		X	X	
Windows 7	X			X		X	X	
Windows 2003 Server		X		X		X		X
Windows 2008 Server		X		X		X		X
UNIX / Linux	Depèn de la distribució.			X		X	Depèn de la distribució.	
Novell Netware		X		X		X		X

Per ser més exactes en la catalogació dels sistemes de la família UNIX/Linux i Novell Netware, hauríem de detallar més les diverses versions de sistema operatiu i de nucli que hi ha hagut, cosa que ens portaria a haver de construir una taula molt més àmplia que la que donem. Per tant, si voleu saber de manera exacta quines són les característiques d'un UNIX/Linux o d'un Novell Netware, ens haurem de remetre a les fonts de documentació tècnica acreditades de cada versió/distribució d'aquests sistemes operatius.

Més informació

http://ca.wikipedia.org/wiki/Sistema_operatiu

http://www.fib.upc.edu/retroinformatica/historia/so.html

http://www.softcatala.org/wiki/Categoria:Rebost_Sistemes%C2%B7operatius

2. Configuració de màquines virtuals

2.1 Màquina real, màquina virtual. Descripció

A vegades cal provar un determinat programa, o fer proves amb un altre sistema operatiu diferent del que estem usant en el nostre ordinador. En aquest cas, podríem formatar l'equip i instal·lar-hi el nou sistema operatiu; una altra opció seria crear una nova partició del disc per a fer-ne la instal·lació, o també podríem cercar un ordinador que ja tingués instal·lat el programari que ens interessa. Hi ha una altra solució més senzilla que tot això: l'única que s'ha de fer és instal·lar una eina (programa) que simuli el sistema operatiu que volem provar, d'aquesta manera no hi ha la necessitat de formatar ni canviar el nostre equip informàtic. El sistema operatiu simulat ha de ser totalment independent del sistema operatiu real, de manera que puguin conviure els dos sistemes de manera simultània i es pugui passar de l'un a l'altre amb facilitat.

Una **màquina real** (o **màquina física**) és un ordinador que té elements físics, també anomenats *components*, que donen un servei a molt baix nivell (nivell físic) dins d'una arquitectura coneguda i en què s'obtenen els millors resultats referents a la velocitat de tractament de la informació. En la màquina real és on s'executen els sistemes operatius i altres processos que només necessiten una arquitectura coneguda.

Una **màquina virtual** (o **màquina lògica**) és una màquina que simula el funcionament d'una màquina real sobre la qual es poden instal·lar sistemes operatius, aplicacions informàtiques, navegar de manera segura per Internet, utilitzar diversos dispositius (per exemple, targetes de xarxa, dispositius USB, etc.).

Una màquina virtual és una màquina que simula una màquina real. Com? Doncs mitjançant un determinat programari. D'aquest procés de simulació en diem *virtualització*.

La **virtualització** és un concepte que descriu la capacitat de tenir diversos sistemes operatius funcionant al mateix temps en un sol ordinador.

També podem definir una màquina virtual com un programari que simula una màquina real i on es poden executar programes informàtics com si es tractés d'una màquina real.

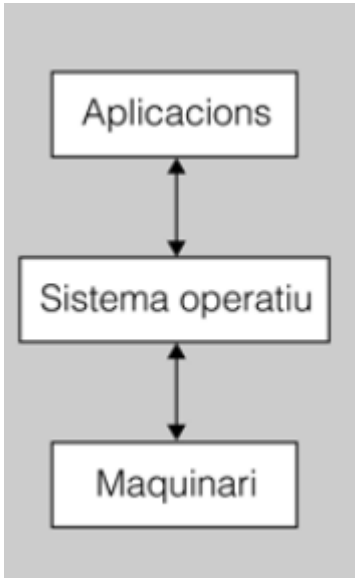
Amfitrió i hoste

Per a poder utilitzar una màquina virtual, necessitem un programari determinat que permeti simular una màquina real. Aquest programari ha d'estar instal·lat en un sistema operatiu de base anomenat ***amfitrió*** (per exemple, la família de sistemes operatius Windows, les distribucions de Linux, l'entorn Macinstosh d'Apple). Els diversos sistemes operatius instal·lats en les màquines virtuals s'anomenen ***hostes***.

El sistema operatiu sobre el qual s'executa el programari per a crear les màquines virtuals s'anomena ***amfitrió*** (en anglès s'anomena ***host***). Per exemple, els sistemes operatius Windows, Linux i MacOS.

Els diversos sistemes operatius instal·lats en cada màquina virtual s'anomenen ***hostes*** (en anglès s'anomenen ***guest***).

Recordem que en una màquina real podem identificar els components següents:



• Les **aplicacions informàtiques** són els programes informàtics que voleu executar en un màquina real.

• El **sistema operatiu** és un programari que facilita la comunicació entre les aplicacions informàtiques i el maquinari.

• El **maquinari** són els diferents dispositius que formen la màquina real i són els responsables de dur a terme les feines finals.

2.2 Avantatges i inconvenients de la virtualització

La utilització de màquines virtuals té tot un seguit d'avantatges i d'inconvenients.

Avantatges:

- **Execució d'entorns complets sense instal·lació ni configuració:** la possibilitat de descarregar màquines virtuals des d'Internet permet estalviar temps en instal·lacions i configuracions. Hi ha moltes màquines virtuals disponibles i funcionant des del primer moment.

- **Proves d'aplicacions**: moltes vegades es necessita un entorn per a provar una aplicació. Utilitzar una màquina virtual permet instal·lar un sistema operatiu des de zero, provar aplicacions i després eliminar la màquina.

- **Recuperació davant desastres:** l'estat d'una màquina virtual es pot emmagatzemar en format de fitxer i, per tant, en el cas de desastre es pot recuperar la informació amb rapidesa.

- **Aplicacions portàtils**: amb l'ús de les màquines virtuals es poden tenir PC completament preparats per a ser utilitzats en dispositius USB o CD, la qual cosa pot ser de gran utilitat per a tenir un entorn privat i utilitzar-lo en qualssevol PC.

- **Consolidació de servidors:** convertir molts servidors físics en virtuals, d'aquesta manera s'aprofita el maquinari disponible de la millor manera possible.

Inconvenients

- **Gran complexitat**: la virtualització provoca un alentiment del sistema virtualitzat, és a dir, el programari no s'executarà amb la mateixa velocitat que en una màquina real.

- **Reserva de recursos:** la màquina virtual utilitzarà una part important de la memòria RAM per funcionar, i també necessitarà un espai considerable d'espai en el disc dur.

2.3 Programari per a la creació de màquines virtuals

De programes de virtualització en trobarem uns quants, cadascun amb unes característiques diferents, que caldrà analitzar abans de decidir-se per un o un altre.

Una manera de classificar els programes informàtics és tenint-ne en compte la propietat. D'aquesta manera, parlarem de *programari propietari* i *programari lliure*.

El **programari propietari** es refereix a qualsevol programa informàtic en el qual els usuaris tenen limitacions pel que fa a utilització, modificació, redistribució (amb modificació o sense) del codi font, o bé no està disponible o l'accés és restringit.

El **programari lliure** és la denominació del programari que dóna la llibertat als usuaris sobre el producte adquirit i, per tant, una vegada obtingut, de poder ser utilitzat, copiat, estudiat, modificat i redistribuït lliurament.

Els principals programes que podem trobar per a la virtualització són:

- Virtualbox (codi lliure) http://www.virtualbox.org/
- VMware (propietari) http://www.vmware.com/es/virtualization/

En l'enllaç següent trobareu una taula comparativa dels programes de virtualització: http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines

2.4 Instal·lació d'un sistema operatiu sobre una màquina virtual

Un cop tinguem instal·lada la nostra aplicació de virtualització, caldrà configurar, entre d'altres, els elements següents:

- Quantitat de memòria RAM a utilitzar.
- Seleccionar el lloc on se situarà la màquina virtual (dins l'arbre de directoris).
- Establir el tipus de comunicació entre els sistemes operatius hostes.
- Fixar la capacitat de la màquina virtual.
- Comprovar el funcionament de la màquina virtual creada.

3. Tasques bàsiques de configuració i manteniment de sistemes operatius propietaris

3.1 Arrencada i parada del sistema

Per tal de poder accedir a un sistema informàtic, hem de disposar d'un compte d'usuari definit en el mateix sistema. S'ha de dir, però, que fins a l'aparició de les distribucions basades en el motor NT aquesta premissa no es complia, es a dir, en l'MS-DOS o el Windows 98 qualsevol usuari podia entrar en el sistema sense cap problema, i això podia provocar un problema de seguretat de la informació greu.

Un **compte d'usuari** és una identificació que utilitzen els sistemes operatius per a gestionar l'accés dels usuaris al sistema informàtic. Aquests comptes són creats i gestionats per l'administrador del sistema informàtic.

Un **administrador d'un sistema operatiu** és l'usuari que té tots els drets, els permisos i els atributs en el sistema en què és definit. El compte administrador és un exemple de compte d'administrador.

En el cas dels sistemes operatius Windows, els comptes d'usuari disposen de la informació següent:

- **Nom d'usuari**, també anomenat *login*.
- **Contrasenya** o *password*.
- **Tipus de compte.** Es poden crear diferents tipus de compte d'usuari que donaran accés a diferents graus d'utilització del sistema. Per exemple, un compte de convidat no permetrà modificar cap registre del sistema ni instal·lar cap tipus de programa.

Iniciar de sessió. A la pregunta ***login*** cal respondre amb el nom d'usuari i la contrasenya que tindrem assignada. Si l'usuari i la contrasenya són correctes, el sistema ens donarà pas i podrem accedir al nostre directori personal (si arranquem en mode text) o al nostre escriptori, si és que hem arrancat en mode gràfic. En aquest moment ja ens trobem en una sessió.

Acabar una sessió significa no que podrem utilitzar el sistema operatiu a partir d'aquest moment. Aquest procés pot ser més o menys complicat depenent del sistema operatiu utilitzat.

Desconnexió de l'usuari del sistema

El procés d'acabar una sessió implica, d'alguna manera, la desconnexió de l'usuari del sistema informàtic. Això representa tancar una sèrie de fitxers i finalitzar els processos que estaven creats. Cal dir que mai no es pot acabar una sessió del sistema apagant directament l'ordinador.

3.2 Interfícies d'usuari

Si estudiem l'evolució dels sistemes operatius utilitzats en els equips anomenats *microordinadors* des dels seus orígens, veurem que la comunicació entre els usuaris i els sistemes operatius utilitzats no ha estat sempre de la mateixa manera.

Un sistema operatiu és un conjunt de programes que té com a objectiu permetre la comunicació entre l'usuari i l'ordinador d'una manera eficient, còmoda i ràpida. Per a aconseguir aquests objectius, els sistemes operatius utilitzen diverses capes de programari, cadascuna de les quals fa unes tasques específiques. Una d'aquestes capes és la interfície de l'usuari.

La **interfície d'usuari** en un sistema operatiu és un entorn de treball de què disposem els usuaris per a poder interaccionar amb els sistemes operatius, és a dir, per a poder-nos comunicar amb els sistemes operatius i donar-los ordres. Aquesta interfície d'usuari (IU, en anglès, *user interface*, UI) es pot basar en la utilització d'un intèrpret d'ordres (o *shell*) en mode text, en la utilització d'un intèrpret en mode menú i en la utilització d'un intèrpret en mode gràfic.

L'intèrpret d'ordres

és un llenguatge de programació mitjançant el qual els usuaris i els programes es comuniquen amb el sistema operatiu. Per exemple, podem parlar d'intèrprets d'ordres com el fitxer **command.com**, utilitzat en el sistema operatiu MS-DOS, el fitxer **cmd.exe** en el Windows XP Professional Edition, etc.

3.3 Actualitzacions del sistema operatiu

Quan es llança un sistema operatiu, s'hi van trobant vulnerabilitats importants que no s'havien tingut en compte i són els mateixos fabricants de programari els que posen a la disposició dels usuaris actualitzacions per compensar-ne les deficiències. Els sistemes operatius necessiten actualitzacions periòdiques per diversos motius:

- **Actualitzacions de maquinari**: com que el maquinari dels diferents dispositius que formen els ordinadors evoluciona, cal crear programes capaços de gestionar aquest nou maquinari.
- **Actualitzacions dels programes**: de vegades, es detecten vulnerabilitats o errors en els programes que són resolts en actualitzacions posteriors.
- **Funcionalitats noves:** amb freqüència, els sistemes operatius incorporen noves funcionalitats que els usuaris poden aprofitar descarregant-se-les en les actualitzacions.

En alguns sistemes (per exemple, en els sistemes Windows), les actualitzacions s'ofereixen en forma de pedaç o de seguretat. Quant als tipus d'actualitzacions, en trobem de diferents nivells i en podem destacar els tipus següents :

- **Alta prioritat**. Són les actualitzacions crítiques, les de seguretat, els *service packs* (*SP*) i els paquets acumulatius de revisions.
- **Programari (opcional)**. Són les revisions no crítiques per a aplicacions.
- **Maquinari (opcional)**. Són les revisions per a controladors i altres dispositius de maquinari, com les targetes de so, les impressores, etc.

Les actualitzacions crítiques, o d'alta prioritat, són essencials per al funcionament de l'equip i, en molts casos, tenen per objecte la resolució de problemes de seguretat, per la qual cosa es recomana instal·lar-les sempre.

***Service pack* (SP)**. Els programes anomenats *service pack* són un grup de pedaços que actualitzen, corregeixen i milloren aplicacions i sistemes operatius. Aquesta denominació va ser popularitzada per Microsoft quan va començar a empaquetar grups de pedaços que actualitzaven els seus sistemes operatius (per exemple, el Service Pack 1, 2 i 3 del Microsoft Windows XP i el Service Pack 1 i 2 del Microsoft Windows Vista).

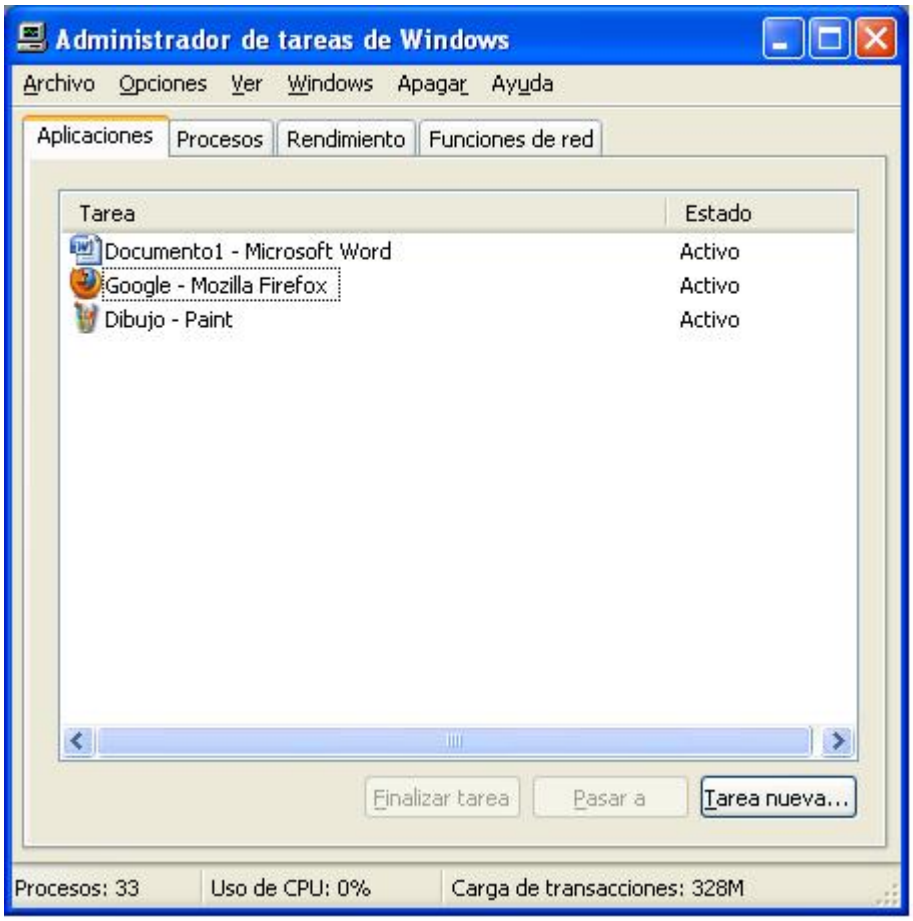
Tipus de *service pack*
1) Incrementals: cada SP no conté actualitzacions anteriors, per la qual cosa s'ha d'instal·lar el *service pack* anterior abans que el *service pack* següent. **2) Acumulatius:** en aquest cas, cada *service pack* conté el *service pack* anterior, cosa que fa més fàcil i ràpida l'actualització.

3.4 Gestió de processos del sistema. L'administrador de tasques

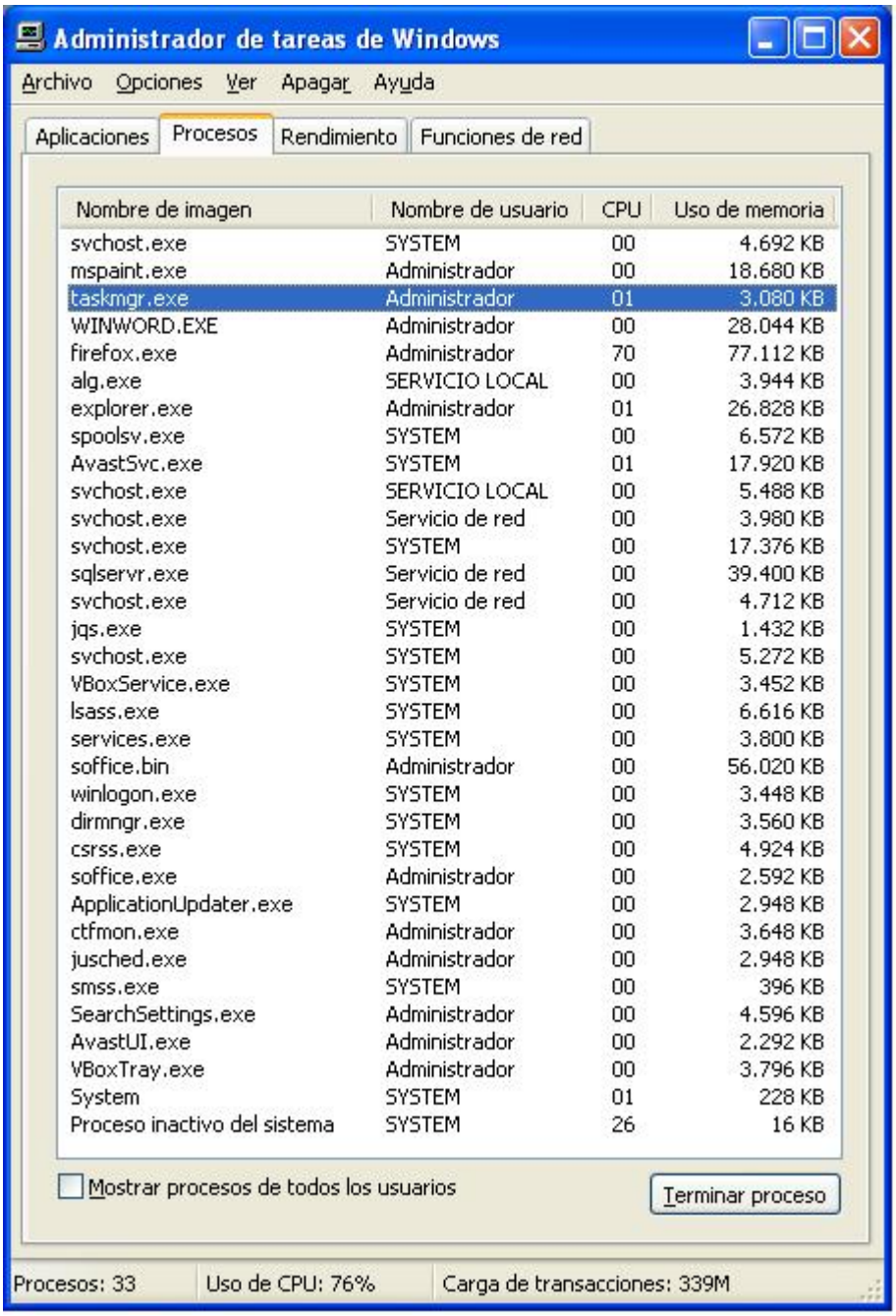
Hi ha diverses eines per a mostrar i manipular els processos en sistemes operatius propietaris. En els sistemes operatius en mode gràfic (per exemple, el sistema Windows), podem utilitzar l'eina anomenada ***administrador de tasques*** per a controlar i gestionar els processos del sistema.

Ho podem fer mitjançant la combinació de les tecles ***Ctrl + Alt + Supr*** o situar-nos en la barra de tasques i fer-hi clic amb el botó dret i seleccionar **administrador de tasques**. Aquesta eina ens subministra informació que fa referència al següent:

• Les **aplicacions** en què podem gestionar els programes que s'estan executant (per exemple, passar a, posar al davant, finalitzar la tasca i anar al procés), tal com es veu en la figura següent:


Administrador de tareas de Windows
Archivo Opciones Ver Windows Apagar Ayuda
Aplicaciones Procesos Rendimiento Funciones de red
Tarea
Estado
Documento1 - Microsoft Word
Activo
Google - Mozilla Firefox
Activo
Dibujo - Paint
Activo
Finalizar tarea
Pasar a
Tarea nueva...
Procesos: 33
Uso de CPU: 0%
Carga de transacciones: 328M

• Els **processos** (figura següent) en què podem gestionar els processos associats als programes (per exemple, acabar, finalitzar l'arbre de processos, depurar i fixar-ne la prioritat). En el moment d'executar un programa, aquest es converteix en procés. Això ho podem veure en seleccionar un programa i amb el botó dret podem anar al procés associat.



Com podeu observar en les dues figures anteriors, hi ha molts processos que el sistema operatiu manté actius i que per als usuaris passen desapercebuts; aquestes tasques o processos s'anomenen *dimonis* (*daemon*).

Els **dimonis** són processos que s'executen en arrencar el sistema (per aquest motiu el sistema triga una estona a estar disponible quan l'engeguem) i no paren d'executar-se fins que no s'atura la màquina, tot i que també n'hi ha que els podem iniciar o aturar manualment. Un tipus de dimonis que s'executen en segon pla són el serveis.
Els **serveis** són programes que llança el sistema operatiu i que s'estan executant d'una manera continuada amb l'objectiu de donar respostes a determinades peticions.

Exemples de serveis
Alguns exemples de serveis són els serveis d'impressió per a poder imprimir, els serveis de pàgines web per a poder visualitzar pàgines web, els serveis de xarxa per a fer comunicacions amb altres dispositius, etc.

3.5 Memòria

L'ordinador és un conjunt de dispositius que té com a objectiu principal executar programes, però per a poder-ho fer necessita disposar de la memòria.

La **memòria** és un conjunt de components electrònics encarregats de l'emmagatzematge dels programes i de les dades que ha d'executar.

En la memòria podem diferenciar els elements següents:
• La **capacitat** d'emmagatzematge. Fa referència a la quantitat d'informació que pot emmagatzemar. S'utilitzen les mateixes unitats de mesurament que per a la informació, per exemple, megabytes (MB), gigabytes (GB), etc.

• La **velocitat** d'accés. El temps que triga l'ordinador a dipositar la informació a la memòria o obtenir-la des que es fa una operació d'escriptura o lectura. Dit d'una altra manera, el temps

que implica la transferència de les dades entre el processador i la memòria. Es mesura en mil·lisegons (ms), microsegons (μs) i nanosegons (ns).

3.6 Mètodes de recuperació del sistema operatiu

Els ordinadors són màquines i, per tant, estan exposades a problemes de funcionament. Els ordinadors són cada vegada més utilitzats per més gent i, en conseqüència, és més freqüent l'aparició de problemes amb els sistemes operatius. Les causes d'aquests problemes les podem resumir en les següents:

• **Ús indegut del programari.** Atès que els usuaris han perdut la por de manipular el sistema, a vegades originen una certa imprudència i s'instal·len a l'ordinador tot el que els arriba a les mans.
• **Ús indegut del sistema operatiu.** Com en el cas anterior, la pèrdua de la por origina que qualsevol persona es vegi capacitada per a modificar aspectes de la configuració del sistema que no sempre produeixen els resultats volguts.
• **Aparició de virus**. La instal·lació indiscriminada de programari comporta l'aparició de virus que ataquen l'ordinador i desestabilitzen el sistema operatiu.
• A més de les causes comentades, en les quals l'usuari té un paper protagonista, n'hi ha d'altres que no són fruit de la mala manipulació, sinó més aviat qüestió de l'atzar i, per què no dir-ho, de la mala sort: fallades en el sistema d'alimentació elèctrica, mal funcionament d'algun dels components de l'ordinador, problemes amb la font d'alimentació, el disc dur, la placa base, etc.

Com diu la dita, "val més curar-se en salut". Això és el que s'ha d'intentar, plantejar una sèrie d'accions per a prevenir aquests problemes:

• **Fer ús dels punts de restauració**. Cal fer de manera periòdica punts de restauració del sistema i sobretot cada vegada que es duu a terme qualsevol manipulació del maquinari del sistema o la instal·lació de qualsevol programari que pot comprometre l'estabilitat del sistema.
D'aquesta manera, sempre podrem restaurar el sistema operatiu al punt anterior davant de qualsevol problema que sorgeixi com a resultat dels canvis.
• **Mantenir el sistema actualitzat**. Cal mantenir el sistema actualitzat mitjançant les actualitzacions o els pedaços de seguretat.

• **Actualitzar els controladors**. També cal mantenir actualitzat el programari que acompanya el maquinari que tenim instal·lat a l'ordinador. Molts fabricants proporcionen actualitzacions i pedaços que eviten les fallades dels controladors.

• **Fer còpies de seguretat**. Cal fer còpies de seguretat de totes les dades que considerem importants i, si és possible i la capacitat ho permet, dividir el disc dur en particions independents per al sistema operatiu i per a les dades, fins i tot utilitzar discos independents.
Una vegada detallats els problemes i plantejades les recomanacions, hem d'abordar com podem recuperar un sistema operatiu quan no arrenca.

Recuperar un sistema operatiu és el conjunt de processos que ens donen la possibilitat de poder arrencar un sistema operatiu i ens permeten tornar-lo a tenir operatiu.

Una manera que tenen algunes distribucions del Windows de poder recuperar un sistema perquè s'ha produït algun problema és el component anomenat ***restaurar sistema***, que podem utilitzar per a restaurar l'equip a un estat anterior sense perdre els arxius de dades personals. Restaurar el sistema supervisa els canvis que es fan en el sistema i en alguns arxius d'aplicació i crea automàticament **punts de restauració** que es poden identificar fàcilment.

Punts de restauració

Si ens trobem davant de la situació que, després d'instal·lar un dispositiu i/o programa o després de fer canvis en la configuració del sistema, detectem un mal funcionament del sistema operatiu, una eina molt útil de què disposen alguns sistemes operatius (per exemple, algunes distribucions del Windows) són els punts de restauració, que és una manera de restaurar el sistema operatiu.

Els **punts de restauració** representen un estat d'emmagatzematge de l'equip. Els punts de restauració els crea el sistema a intervals específics i quan detecta que es comencen a produir canvis en l'equip. A més, els punts de restauració es poden crear manualment en qualsevol moment. Aquests punts de restauració permeten recuperar el sistema a un estat anterior. Es creen diàriament i quan es produeixen successos importants en el sistema (per exemple, en instal·lar una aplicació o un controlador). També podem crear punts de restauració propis en qualsevol moment i assignar-los un nom.

Observacions sobre els punts de restauració

Sobre els punts de restauració, s'ha de tenir en compte el següent:
1) Si es restaura el sistema en un punt anterior a la instal·lació d'un programa, aquest programa no funcionarà posteriorment. Si volem utilitzar el programa caldrà instal·lar-lo novament.
2) Restaurar el sistema no substitueix el procés de desinstal·lació d'un programa.
3) Restaurar el sistema no restaura el contingut de cap opció de configuració associada amb els perfils dels usuaris mòbils.
4) Únicament restaura les particions i les unitats per les quals està configurat.
5) Les utilitats antivirus poden afectar la capacitat del sistema de restaurar-se en un punt anterior.

Una característica important d'algunes distribucions del Windows és el fet de poder crear punts de restauració, amb la finalitat de desar-hi la configuració del nostre equip en un moment determinat. D'aquesta manera, en el cas de tenir un problema de configuració per un programa o per una altra causa similar, podrem restaurar la configuració del nostre equip en el moment en què vam crear el punt de restauració, configuració en què el nostre equip funcionava correctament. El mateix sistema crea els seus punts de restauració, però és recomanable crear-ne alguns quan estem a punt de fer un canvi important de programari o maquinari en el nostre equip.

Inici en mode a prova d'errors

La majoria de les versions del Windows tenen la característica que permet reparar un sistema que no es pot iniciar o carregar utilitzant el mètode d'inici del sistema en mode a prova d'errors. Aquestes característiques són útils quan alguns dels arxius del sistema estan danyats o són eliminats accidentalment, o quan s'ha instal·lat programari o controladors de dispositius que fan que el sistema no funcioni correctament.

El **mode a prova d'errors** permet iniciar el sistema amb un mínim de controladors de dispositius i de serveis. D'aquesta manera, si un nou controlador de dispositiu o un programa instal·lat impedeix que l'equip s'iniciï, ho podrà fer en mode segur i després podrem eliminar el programari o el controlador del dispositiu de l'equip responsable del problema.

Les opcions d'inici en mode a prova d'errors són:

• **Mode segur**. Permet iniciar el sistema únicament amb els arxius i controladors bàsics (per exemple, el ratolí, el monitor, el teclat, les unitats de disc, el vídeo VGA, els serveis predeterminats del sistema i cap connexió de xarxa).
• **Mode segur amb funcions de xarxa**. Permet iniciar el sistema únicament amb els arxius i els controladors bàsics indicats anteriorment juntament amb les connexions de xarxa.
• **Mode segur amb símbol del sistema**. Permet iniciar el sistema únicament amb els arxius i els controladors bàsics indicats anteriorment. Després d'iniciar una sessió, es presenta el símbol del sistema.
• **Habilitar el registre d'inici**. Permet iniciar el sistema mentre es registren tots els controladors i els serveis que el sistema carrega en un arxiu.
• **Habilitar el mode VGA**. Permet iniciar el sistema amb el controlador bàsic de vídeo VGA. S'utilitza quan s'ha instal·lat un controlador nou per a la targeta de vídeo que fa que no arrenqui correctament el sistema.
• **Habilitar l'última configuració vàlida coneguda**. Permet iniciar el sistema amb la informació del registre que el sistema tenia abans dels últims canvis fets en el registre i que provoquen que el sistema no s'inicií.
• **Mode de restauració de servei de directori (servei directori)**. S'utilitza únicament en equips que són controladors de domini del Windows.
• **Mode depuració**. Permet iniciar el sistema mentre s'envia informació de depuració a un altre equip per un cable sèrie.

4. Tasques bàsiques de configuració i manteniment de sistemes operatius lliures

4.1 Introducció al Linux

Per fer aquesta introducció a què és el Linux, o més concretament el **GNU/Linux,** ens remetrem al que diu el web de Softcatalà a http://softcatala.org/wiki/Linux.

"L'any 1991, Linus Torvalds, estudiant de la Universitat de Hèlsinki a Finlàndia, va crear la primera versió de Linux per cobrir les seves necessitats. Es tractava del nucli d'un sistema operatiu, molt rudimentari, fet per a ser executat en un PC 80386 de l'època. Però Linus Torvalds va tenir la bona idea de fer-lo «lliure» per a que tothom que volgués el pogués fer servir i millorar. Gràcies al suport d'Internet, la recent nascuda comunitat de desenvolupadors i la preexistència del projecte GNU, començat uns anys abans per Richard Stallman, el Linux (GNU/Linux) va poder esdevenir, uns anys després, un sistema operatiu complet. Les **distribucions de GNU/Linux** complementen GNU/Linux amb entorns gràfics i altres programes que el fan tant o més fàcil d'utilitzar que el Windows.

Amb aquest lloc web pretenem recopilar informació en català sobre el Linux que sigui útil per als nouvinguts a aquest sistema operatiu.

- Característiques de GNU/Linux
- Distribucions GNU/Linux en català
- Instal·lar distribucions de Linux pas a pas
- Enllaços de Linux - Petita selecció d'enllaços de GNU/Linux.
- Treballs sobre GNU/Linux i el programari lliure
- Experiències de migració - Recull de webs que raonen i descriuen el procés de migració a Linux.
- Linux i educació - Petit recull d'articles en català.
- Cursos, manuals i tutorials de Linux en català
- Presentacions i documents de suport per a xerrades
- Jocs i Linux - Qui va dir que amb Linux no es podia jugar?
- Preguntes més freqüents per a nouvinguts - Si no saps res o gairebé res de Linux, aquesta és la teva secció."

4.2 Arrencada i parada del sistema

Tal com hem dit en el cas dels sistemes operatius propietaris, per a accedir al sistema necessitarem un compte d'usuari.

Un **compte d'usuari** és una identificació que utilitzen els sistemes operatius per a gestionar l'accés dels usuaris al sistema informàtic. Aquests comptes són gestionats per l'administrador del sistema informàtic.

Quina informació conté un compte d'usuari d'accés a un sistema informàtic? Bé, això depèn del sistema operatiu utilitzat. En el cas de sistemes operatius Unix/Linux, podem especificar la informació següent:

• El nom d'usuari que utilitzarem en la connexió.
• La clau d'accés o contrasenya.
• El tipus de compte creat. Això vol dir que podem crear diferents tipus de comptes d'usuaris que impliquen diferents graus d'utilització del sistema: per exemple, comptes administratius, comptes de convidats, etc.

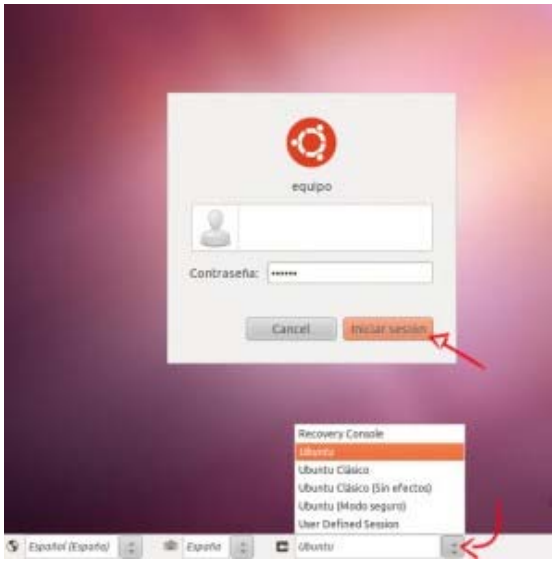
• L'intèrpret d'ordres de connexió utilitzat, per exemple, l'intèrpret d'ordres de bash, l'intèrpret d'ordres de bourne, l'intèrpret d'ordres de C, etc.
• L'estat del compte: habilitat, bloquejat, etc.
• El nom del directori de treball i la situació dins de l'estructura d'arbre de la informació.
• El número d'identificació d'usuari (UID).
• El grup al qual volem que pertanyi l'usuari.
• La gestió de la contrasenya, és a dir, la caducitat, la llargada màxima i mínima, etc.

Durant el procés d'instal·lació dels sistemes operatius, es creen per defecte alguns comptes d'usuari; per exemple, en el cas del sistema Unix, es crea el compte anomenat *arrel* (**root**).

Un **administrador d'un sistema operatiu és l'usuari que té tots els drets**, els permisos i els atributs en el sistema on és definit. El compte arrel és un exemple de compte d'administrador.

El compte arrel s'ha d'utilitzar d'una manera molt restrictiva. Què volem indicar amb aquesta afirmació? Doncs que aquest compte només l'ha d'utilitzar l'administrador del sistema i en tasques administratives. No és un compte per a experimentar amb el sistema ni per a utilitzar el divers programari instal·lat en el nostre equipament informàtic.

El procés de connexió a un sistema operatiu es pot fer tant en mode text com en mode gràfic. Una vegada tenim un compte i una contrasenya que ens ha assignat l'administrador, podem iniciar una sessió en el sistema Unix. En la figura següent teniu un exemple d'inici de sessió.



En aquesta pantalla, també podrem triar el gestor de finestres que volem per a la sessió que obrirem.

Tancar el sistema

Per apagar l'ordinador no podem desconnectar-lo senzillament, ja que com hem comentat abans, hi ha una sèrie de processos i serveis (dimonis) que s'estan executant de manera contínua en segon terme. En la figura teniu següent un exemple de la pantalla de fi de sessió:

El procés d'**acabar una sessió** implica, d'alguna manera, la desconnexió de l'usuari al sistema informàtic. Això representa tancar una sèrie de fitxers i finalitzar els processos que estaven creats.
Val a dir que mai no es pot acabar una sessió del sistema apagant directament l'ordinador.

4.3 Interfícies d'usuari

Si estudiem l'evolució dels sistemes operatius dels equips anomenats *microordinadors* des dels orígens, veurem que la comunicació entre els usuaris i els sistemes operatius no ha estat sempre de la mateixa manera.

Un sistema operatiu és un conjunt de programes que té com a objectiu permetre la comunicació entre l'usuari i l'ordinador d'una manera eficient, còmoda i ràpida. Per a aconseguir aquests objectius, els sistemes operatius utilitzen diverses capes de programari, cadascuna de les quals fa unes tasques específiques. Una d'aquestes capes és la interfície de l'usuari.

La **interfície d'usuari en un sistema operatiu** és un entorn de treball de què disposem els usuaris per a poder interaccionar amb els sistemes operatius, és a dir, per a poder-nos comunicar amb els sistemes operatius i donar-los ordres. Aquesta interfície d'usuari (**IU**) es pot basar en la utilització d'un intèrpret d'ordres en **mode text**, en la utilització d'un intèrpret en **mode menú** i en la utilització d'un intèrpret en **mode gràfic**.

L'intèrpret d'ordres és un llenguatge de programació mitjançant el qual els usuaris i els programes es comuniquen amb el sistema operatiu. Per exemple, podem parlar d'intèrprets d'ordres com els fitxers bash, sh i csh en el Unix/Linux.

Actualment, els sistemes operatius tenen els modes bàsics de funcionament següents:

1) **Menús**. La comunicació entre usuari i sistema es fa mitjançant diferents menús d'opcions disponibles en el mateix sistema operatiu que s'ha d'utilitzar. Només cal seleccionar l'opció del menú que ens interessa perquè el sistema faci una acció determinada (per exemple, el sistema SCO Xenix).

2) **Gràfics (GUI**). La manera més fàcil de comunicar-se entre usuari i sistema es basa en una sèrie d'elements gràfics (les finestres, les icones, etc.) a partir dels quals s'executen les accions (per exemple, l'entorn X Window de les distribucions del Unix/Linux).

3) **Text.** La comunicació amb el sistema es fa mitjançant ordres escrites segons un llenguatge determinat.

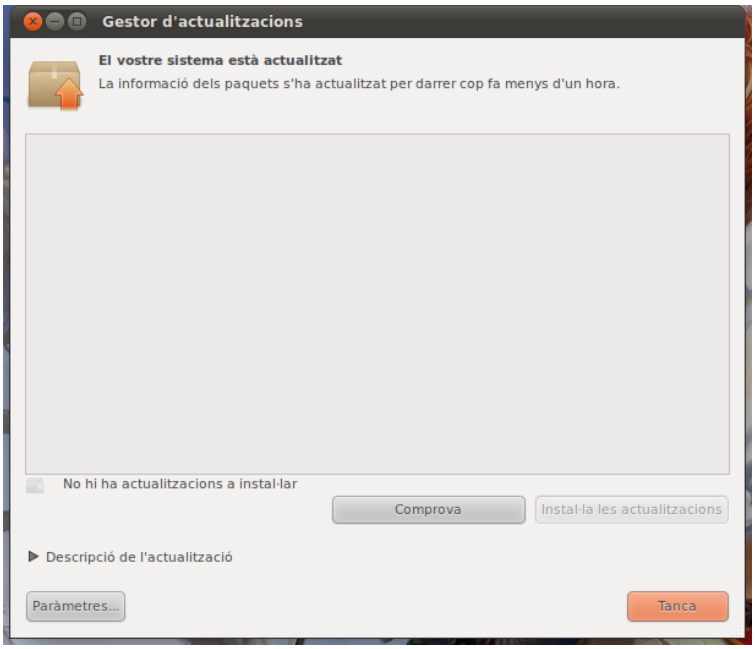
4.4 Actualitzacions del sistema operatiu

En els sistemes operatius lliures, i en particular en les distribucions Linux, les actualitzacions es poden baixar d'Internet de manera gratuïta des de llocs oficials del Linux anomenats *repositoris*.

Els **repositoris** són llocs en què s'emmagatzema la informació digital i se'n fa el manteniment, normalment en bases de dades o en arxius informàtics.

Els repositoris estan preparats per a distribuir-se habitualment utilitzant una xarxa informàtica com Internet o un mitjà físic com un disc compacte. Poden ser d'accés públic, o poden estar protegits, i necessiten una autentificació prèvia.

Els repositoris s'utilitzen de manera intensiva en el Linux; la majoria emmagatzemen paquets de programes disponibles per a instal·lar-los mitjançant un gestor de paquets. En els sistemes Linux, podem actualitzar el sistema operatiu d'una manera automàtica utilitzant Internet o a partir de suports del tipus CD/DVD. Pràcticament cada distribució del sistema Linux utilitza sistemes d'actualització automàtics diferents en l'entorn gràfic. Així, per exemple:



4.5 Afegir / eliminar programari

De la mateixa manera que podem actualitzar el sistema operatiu, també podem afegir, eliminar i/o actualitzar i configurar el programari de diferents tipus del sistema operatiu amb eines tant de tipus text com de tipus gràfic.

En els sistemes operatius lliures podem gestionar el sistema operatiu a partir del que s'anomena *sistema de gestió de paquets*.

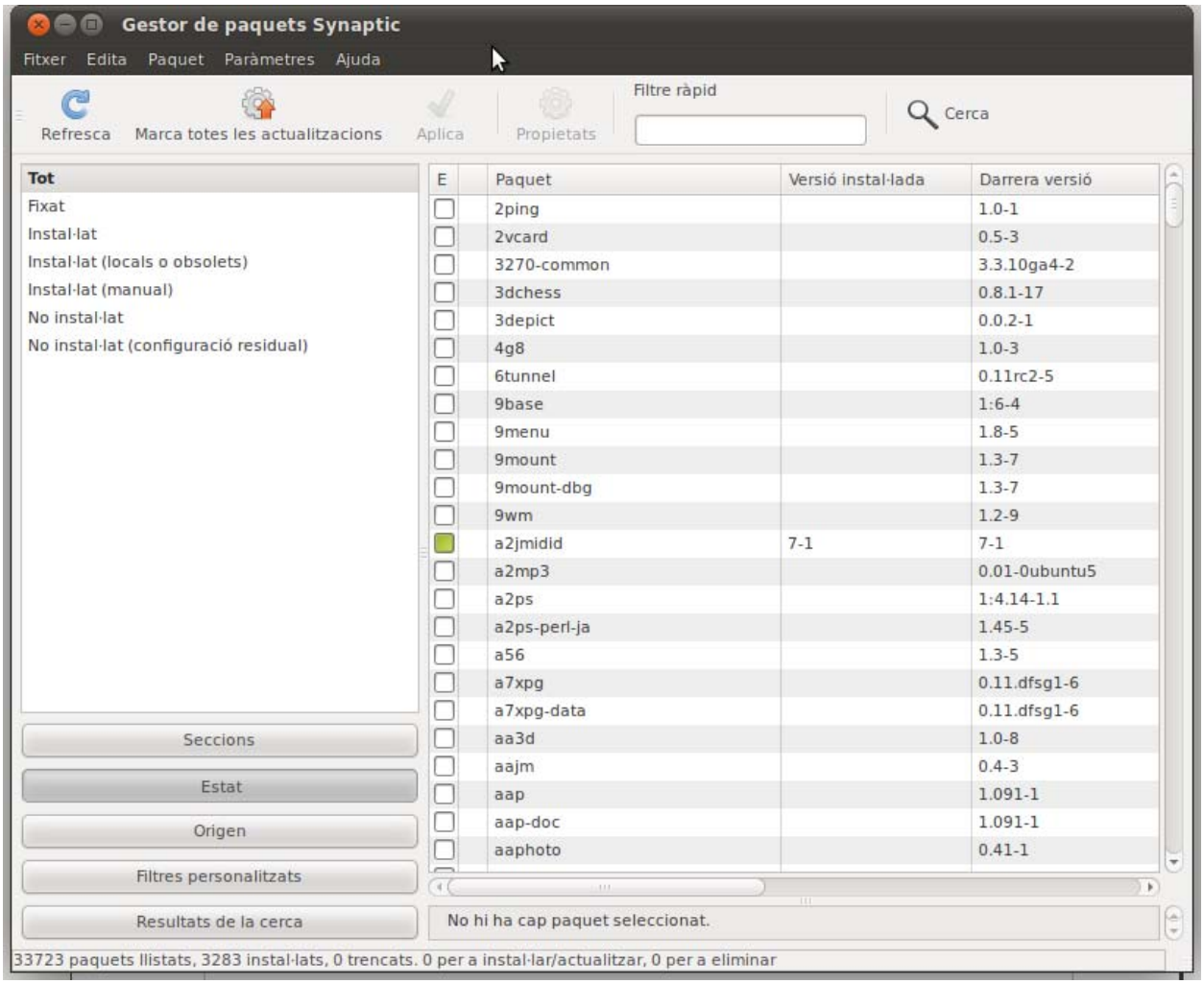
Un sistema de gestió de paquets, també conegut com a ***gestor de paquets***, és una col·lecció d'eines que serveixen per a automatitzar el procés d'instal·lació, d'actualització, de configuració i d'eliminació de programes.

En els sistemes de gestió de paquets, el programari es distribueix en forma de paquet, freqüentment encapsulat en un únic fitxer. Aquests paquets inclouen el nom complet, una descripció de la funció que tenen, el número de versió, el distribuïdor del programa, una llista dels paquets que necessita perquè funcionin correctament, etc. Podem destacar els sistemes basats en paquets binaris següents:

1) El **sistema RPM** (*RPM package manager* o RPM, *Red Hat package manager*). És una eina d'administració de paquets pensada específicament per al GNU/Linux. És capaç d'instal·lar, actualitzar, desinstal·lar, verificar i sol·licitar programes. RPM és el format de paquet de partida del Linux Standard Base. És utilitzat per un gran nombre de distribucions de Linux. Hi ha diverses eines per a treballar amb aquest sistema de paquets:
   • En mode text, podem trobar l'ordre anomenada **rpm**.
   • En mode gràfic, podem trobar diferents eines com **up2date** (Red Hat), **yast** (SuSe), **yum** (Fedora), **krpm**, etc.

2) El **sistema de paquets de Debian**. Debian, i també el seus derivats, utilitza paquets en un format d'arxiu anomenat ***deb***. És capaç d'instal·lar, actualitzar, desinstal·lar, verificar i sol·licitar programes. Hi ha diverses eines per treballar amb aquest sistema de paquets:
   • En mode text, podem trobar les ordres anomenades ***dpkg***, ***apt-get*** i ***aptitude***.
   • En mode gràfic, podem trobar diferents eines com **synaptic** (figura següent), **yast, adept, kynaptic**, etc.

Hi ha una eina anomenada ***alien*** que ens permet passar paquets del format rpm a deb i també a la inversa.



3) El **sistema fink**. El sistema Mac OS X disposa de l'eina anomenada ***fink*** que deriva parcialment de dpkg/apt. Aquesta eina permet fer més senzilla la instal·lació de programes lliures en el Mac OS X.

4) Els **tarballs**. Són una col·lecció d'arxius situats en un fitxer. La utilitat tar s'utilitza per a combinar alguns arxius en un únic arxiu. La utilitat gzip s'usa per a comprimir l'arxiu. Els tarballs tenen extensions com **.tar.gz, tar.bz2** o .**tgz**. La majoria de vegades, un tarball conté arxius de codi o arxius binaris. Si trobem alguna col·lecció amb l'extensió .tar.gz, l'haurem de

descomprimir fent doble clic abans d'instal·lar el programari. Si ho volem fer des de la consola de text, cal utilitzar l'ordre **tar** (per exemple, tar –xvzf nom_arxiu).

Per instal·lar-los, hem de llegir la documentació que acompanya el paquet i seguir les instruccions. En general, podem fer les accions següents:

1) Determinar els objectius del procediment.
2) Seguir el procediment indicat en la documentació tècnica.
3) Configurar: ./configure [opcions].
4) Compilar: **make**.
5) Instal·lar: **make install**.
6) Netejar les restes de la compilació (és opcional): **make clean**.
7) Comprovar el procediment dut a terme.
8) Documentar la instal·lació.

Per a desinstal·lar el programa resultant, podem utilitzar **make unistall**.

5. Seguretat. Nous perills. Seguretat en xarxes sense fil

5.1 Virus i altres amenaces. Pesca (*phishing*), descaminament (*pharming*) i enregistrador de teclat (*keylogger*)

Cal que tingueu el sistema ben protegit. Per tant, heu de tenir clar de qui us heu de protegir i què és el que voleu protegir. També heu de saber quins perills té el vostre sistema, quin és el nivell de propagació i quins són els danys que pot provocar el programari maliciós. Aquesta, doncs, és la primera tasca que cal fer.

El **programari maliciós** és tot el programari que s'instal·la en el vostre ordinador, sense el vostre consentiment ni coneixement, amb la finalitat de perjudicar-lo o d'obtenir-ne un benefici. Aquest últim cas és el més habitual, de manera que les accions del programari maliciós cada vegada són més sofisticades i difícils d'identificar.

Hi ha molts tipus de programari maliciós i, per tant, classificar-los és difícil. Malgrat tot, es poden distingir els més habituals, que són els següents:

1) **Virus**: es tracta d'un programa que es copia automàticament per a alterar el funcionament normal del sistema, sense el permís ni el coneixement de l'usuari. Ells mateixos es repliquen i s'executen. Dins aquest apartat podem trobar els virus següents:

• **Virus residents**: s'executen cada vegada que engeguem l'ordinador i s'oculten en la RAM de manera permanent. D'aquesta manera, controlen totes les operacions que es fan amb l'ordinador i tenen la capacitat d'infectar tots els arxius que obrim, tanquem, copiem, executem, etc. Només s'activen quan es compleix una certa condició imposada pel creador del virus, com la data o l'execució d'una determinada acció. Fins que no es produeix, romanen ocults.

• **Virus d'acció directa**: es reprodueixen i actuen en el mateix moment que s'executen. A diferència dels residents, no són en la memòria. Normalment, només afecten els arxius que són a la mateixa carpeta o directori o els que es troben en el camí (*path*). Tenen l'avantatge que són més fàcils d'eliminar sense deixar cap rastre.

• **Virus de sobreescriptura**: escriuen dins un arxiu i en canvien el contingut. L'arxiu infectat no varia de mida, ja que només se sobreescriu. Els arxius infectats per aquest virus queden inservibles i s'han d'eliminar, de manera que es perd la informació que contenen.

• **Virus de companyia**: per a efectuar les operacions d'infecció, els virus de companyia poden esperar-se en la memòria fins que s'executi algun programa (virus residents) o actuar directament fent copies d'ells mateixos (virus d'acció directa). Contràriament als virus de sobreescriptura o als virus residents, els virus de companyia no modifiquen els fitxers infectats. En algun moment, mentre el sistema operatiu està treballant (executant programes, fitxers amb extensions .exe i .com), pot haver d'executar un programa amb un nom determinat. Aleshores, si hi ha dos fitxers executables, l'un amb extensió .exe i l'altre amb extensió .com, el sistema operatiu executarà en primer lloc el d'extensió .com. El virus de companyia aprofita aquesta peculiaritat per a crear un altre fitxer amb el mateix nom, però amb extensió .com, de manera que el virus que crearà la infecció serà aquest. Quan el sistema operatiu hagi de decidir quin dels dos fitxers ha d'executar, optarà pel d'extensió .com, que s'infectarà, i seguidament executarà el fitxer .exe. D'aquesta manera, l'usuari no s'adonarà de la infecció que s'acaba de produir. Aquesta manera de funcionar d'aquests virus provoca que s'estenguin d'una manera eficaç i en dificulta la detecció.

• **Virus d'arrencada o *boot***: els termes *boot* o *sector d'arrencada* fan referència a una secció molt important d'un disc (tant d'un disquet com d'un disc dur). En aquesta secció es guarda la informació essencial de les característiques del disc i hi ha un programa que permet arrencar l'ordinador. Aquest virus no infecta fitxers, sinó els discos que els contenen. Actuen infectant, en primer lloc, el sector d'arrencada dels disquets, USB, CD o DVD. Quan un ordinador es posa en marxa amb un disquet, un USB, un CD o un DVD infectat, el virus de *boot* n'infecta el disc dur.

• **Virus de macro:** l'objectiu d'aquests virus és infectar els fitxers que s'han creat mitjançant determinades aplicacions que contenen macros: documents de Word (.doc), fulls de càlcul Excel (.xls), bases de dades (.mdb), presentacions en el PowerPoint (.pps), fitxers Corel Draw, OpenOffice Writer (.odt), OpenOffice Calc (.ods), OpenOffice Base, etc. Les macros són microprogrames associats a un fitxer que serveixen per a automatitzar operacions complexes. Com que són programes, les macros es poden infectar. Quan s'obri un fitxer que contingui un virus d'aquest tipus, les macros es carregaran de manera automàtica i produiran la infecció. Tot i que la majoria de les aplicacions que utilitzen les macros

disposen d'una protecció antivirus i de seguretat específica, hi ha molts virus de macro que salten aquesta protecció.

Hi ha un tipus de virus de macro diferent segons si l'eina que s'utilitza és del Word, de l'Excel, de l'Access, del PowerPoint, de multiprograma o d'arxius RTF. De totes maneres, aquest virus pot no infectar tots els programes o eines amb macros.

• **Virus de directori o d'enllaç**: els fitxers s'ubiquen en direccions determinades (unitat de disc i directori) que el sistema operatiu coneix per poder localitzar-los i treballar-hi. Els virus d'enllaç o de directori alteren les adreces que indiquen on estan emmagatzemats els fitxers. Així doncs, en intentar executar un programa (fitxer .exe o .com) infectat per un virus d'enllaç, el que es fa en realitat és executar el virus, ja que aquest modificarà l'adreça original del programa i la reemplaçarà. Una vegada produïda la infecció, és impossible localitzar i treballar amb els fitxers originals.

• **Virus encriptats:** més que d'un tipus de virus, es tracta d'una tècnica que alguns d'aquests virus, que poden pertànyer a altres classificacions, utilitzen. Els virus s'encripten perquè els programes antivirus no els detectin. Quan volen actuar es desencripten i quan han acabat es tornen a encriptar.

• **Virus polimòrfics**: són virus que cada vegada que fan una infecció s'encripten d'una manera diferent. Per a fer-ho, utilitzen diversos algorismes i claus de xifratge. Així, generen moltes còpies d'ells mateixos i impedeixen que els antivirus els localitzin per mitjà de la cerca en cadenes o signatures. Per això són difícils de detectar.

• **Virus multipartides**: són virus que poden fer moltes infeccions mitjançant la combinació de tècniques diferents. L'objectiu és qualsevol element que es pot infectar: arxius, programes, macros, discos, etc. Es consideren els més perillosos per la capacitat que tenen de combinar moltes tècniques d'infecció i pels danys que provoquen.

• **Virus web:** són virus de creació recent i apareixen quan s'entra en una pàgina web que conté ActiveX, Java o Javascript infectat.

3) **Cucs o *worms***: es dupliquen com els virus, però no modifiquen els arxius. Es limiten a fer copies d'ells mateixos de la manera més ràpida possible sense tocar cap fitxer. Poden

arribar a ocupar la memòria i alentir l'ordinador. A més, també poden col·lapsar per saturació les xarxes en què s'han infiltrat.

Les infeccions que produeixen aquests virus es fan per mitjà del correu electrònic, les xarxes informàtiques i els canals de xat (com l'IRC o l'ICQ) d'Internet.

4) **Cavalls de Troia:** no es consideren virus, perquè no infecten altres fitxers per a reproduir-se ni tampoc no fan còpies d'ells mateixos per a propagar-se, com fan els cucs. L'objectiu bàsic que tenen és introduir i instal·lar altres programes en l'ordinador perquè es puguin controlar remotament des d'altres equips. És a dir, arriben a l'ordinador com si fossin programes inofensius, però quan s'executen hi instal·len un segon programa, el cavall de Troia.

En general, els cavalls de Troia són programes que s'oculten en imatges o arxius multimèdia (àudio o vídeo) perquè es puguin instal·lar fàcilment.

Els efectes dels cavalls de Troia poden ser molt perillosos. Com els virus, tenen la capacitat d'eliminar fitxers o destruir la informació del disc dur.

A més, però, poden capturar dades confidencials i enviar-les a una adreça externa. També poden obrir ports de comunicacions, cosa que permet que altres persones tinguin un control remot del vostre ordinador.

De les accions més comunes dels cavalls de Troia, destacaríem les següents:

• Controla remotament equips.
• Espia equips per obtenir informació.
• Obté contrasenyes del Messenger.
• Ataca els arxius del sistema.
• Assigna contrasenyes als arxius i després extorsiona els usuaris (víctimes) perquè paguin diners a canvi de les contrasenyes.
• Captura pantalles, similar a espiar.
• Enganya un usuari amb enginyeria social per aconseguir-ne les dades confidencials, com números bancaris, contrasenyes o noms d'usuari.

Els cavalls de Troia són tan importants que ja ocupen el primer lloc de la llista de programari maliciós, davant dels virus. El fet que a Internet hi hagi models simples per a crear cavalls de Troia sense necessitat de ser cap expert en informàtica ha fet que encara en proliferessin més.

4) **Bombes lògiques**: estrictament, tampoc no es consideren virus, ja que no es reprodueixen i ni tan sols són programes independents, sinó que són segments camuflats dins altres programes.
L'objectiu que tenen és destruir les dades d'un ordinador o causar altres tipus de danys que poden arribar a ser molt destructors.

5) **Falses alarmes o *hoaxes***: no són virus, sinó missatges de correu electrònic que enganyen. Es difonen massivament per Internet i sembren l'alarma sobre suposades infeccions víriques i amenaces contra els usuaris.
Les falses alarmes se solen guanyar la confiança dels usuaris, perquè aporten dades que semblen certes i proposen una sèrie d'accions que han de dur a terme per eliminar la suposada infecció. No cal fer cas de les advertències i les instruccions, simplement s'ha d'esborrar el missatge i prou.

6) **Programes espia o *spyware***: el programa espia és un programari, de la categoria dels programes maliciosos, que recopila informació d'un ordinador i després la transmet a una entitat externa sense el consentiment o el coneixement del propietari de l'ordinador. Aquest programa espia s'autoinstal·la, de manera que s'executa cada vegada que l'ordinador es posa en marxa (utilitza el CPU i la memòria RAM i redueix l'estabilitat de l'ordinador). Funciona sempre i controla l'ús que es fa d'Internet, cosa que serveix a entitats externes per a mostrar-vos, per exemple, anuncis relacionats amb la vostra activitat a la Xarxa.
La funció més comuna que tenen aquests programes és recopilar informació sobre l'usuari i distribuir-la a empreses publicitàries o altres organitzacions interessades. Cal tenir en compte, però, que organismes oficials han utilitzat aquest programari per a recopilar informació contra sospitosos de delictes, pirateria del programari, etc.
El programa espia es pot instal·lar en el sistema de moltes maneres diferents. Per exemple, cavalls de Troia, pàgines web que visitem i contenen determinats controls ActiveX o codis que exploten una vulnerabilitat determinada, aplicacions amb llicència de programari gratuït (*freeware*) o programari de prova (*shareware*) que descarreguem d'Internet, etc.

Atès que, normalment, el programa espia utilitza la connexió del PC a Internet per a transmetre informació, consumeix amplada de banda i, per tant, afecta la velocitat de transferència de les dades.

5.2 Seguretat en xarxes sense fil

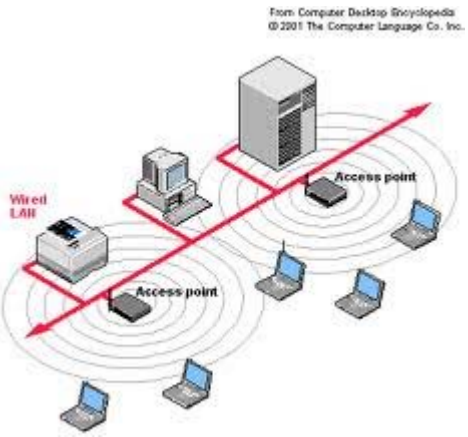
Les xarxes sense fil cada vegada estan més esteses tant en empreses com en xarxes domèstiques, ja que ofereixen avantatges respecte de les xarxes de cable, sobretot pel que fa a la mobilitat i la facilitat en la instal·lació.

Les xarxes sense fil funcionen per radiofreqüència, és a dir, en comptes d'enviar les dades per mitjà d'un cable, les envien per mitjà d'ones electromagnètiques. El funcionament és semblant al de les ones de ràdio. La diferència, però, rau en el fet que les ones electromagnètiques operen a una freqüència molt més elevada, cosa que permet enviar grans volums d'informació.

Les xarxes sense fil no estan aïllades de la resta de xarxes, sinó que intercanvien informació amb les xarxes de cable per poder accedir a tot tipus de continguts.

El **punt d'accés** d'una xarxa sense fil és el que està connectat amb una xarxa de cable. Els dispositius que es connecten a la xarxa sense fil utilitzen el punt d'accés, que és l'encarregat d'autenticar-los i fer circular la informació.

Els punts d'accés disposen d'antenes que distribueixen el senyal de la xarxa sense fil en una àrea determinada. L'abast de l'àrea que pot cobrir un punt d'accés depèn del tipus d'antena, però oscil·la entre 30 i 150 metres.



Quan es vol crear una xarxa sense fil que ha de cobrir una extensió molt gran de territori, cal disseminar diversos punts d'accés per tal de crear una teranyina que doni cobertura a l'àrea que es vol cobrir.

Hi ha certes xarxes sense fil que operen sense punt d'accés. S'anomenen **xarxes *ad hoc***. Aquestes xarxes funcionen mitjançant l'intercanvi d'informació entre els dispositius sense fil i no necessiten cap dispositiu central.

Les xarxes sense fil tenen molts avantatges, però també tenen inconvenients. El problema més acusat que han tingut aquestes xarxes des que van aparèixer és la seguretat.

Si un atacant vol accedir a una xarxa de cable ha de tenir accés físic als cables, cosa que implica haver de superar mesures de seguretat físiques com murs, portes o finestres. Els atacants poden accedir a les xarxes sense fil sense necessitat de tenir accés físic a les instal·lacions, perquè les ones electromagnètiques van més enllà de murs i finestres.

Es recomana no instal·lar els punts d'accés prop de finestres, però fins i tot amb aquestes precaucions, els atacants poden fer ús d'antenes direccionals per a accedir al senyal de les xarxes sense fil.

Identificador de servei (SSID)

SSID és l'acrònim dels termes anglesos *service set identifier*, que vol dir identificador de servei. Cada punt d'accés té un SSID que serveix per a identificar el servei de connexió sense fil dels dispositius que pretenen connectar-s'hi.

Quan des d'un portàtil, un ordinador o un dispositiu es fa una cerca per a saber quines xarxes hi ha disponibles, apareixen els SSID que hi ha a prop. Un punt d'accés pot tenir més d'un SSID per a definir serveis diferents.
Per defecte, els punts d'accés difonen el seu SSID perquè estigui disponible per als receptors. Una mesura de seguretat és inhabilitar la difusió de l'SSID per a donar menys informació a possibles atacants.

Encara que l'SSID no es difongui, hi ha mètodes que permeten esbrinar-lo. Per a fer-ho, s'"ensumen" les connexions dels dispositius que es connecten al punt d'accés.

Autenticació per a MAC

MAC és la sigla dels termes anglesos *media access control.* Tots els dispositius de xarxa (o targetes Ethernet o targetes Wireless) tenen una adreça MAC. Aquesta adreça és un codi de 6 bytes.

L'adreça MAC equival a la matrícula dels automòbils. És un conjunt de números que identifiquen de manera unívoca un dispositiu. No hi pot haver dos dispositius amb la mateixa adreça MAC.

Un dels mecanismes més senzills és utilitzar les adreces MAC per a autenticar els dispositius que es connecten a un punt d'accés. Així doncs, es crea una llista amb les adreces MAC autoritzades i <u>només</u> aquests dispositius són vàlids.

Aquest sistema d'autenticació presenta alguns problemes. D'una banda, implica conèixer prèviament quins usuaris s'hi poden connectar, cosa que en determinats casos no és factible. De l'altra, aquest sistema és vulnerable a l'atac de falsejament d'identitat (*MAC spoofing*).

El falsejament d'identitat consisteix en el fet que un atacant suplanta l'adreça MAC d'un usuari autoritzat.

Quan un dispositiu es vol connectar a un punt d'accés, aquest punt d'accés li demana l'adreça MAC per comprovar si està autoritzat. Moltes vegades, aquesta informació viatja sense xifrar. Si un atacant intercepta la comunicació, pot esbrinar l'adreça MAC de l'usuari autoritzat i utilitzar-la per a connectar-se al punt d'accés.

Protocol WEP

El primer protocol que va sorgir per a solucionar els problemes d'autenticació i confidencialitat en les xarxes sense fil va ser el protocol WEP. *WEP* és la sigla dels termes anglesos *wired equivalent privacy*, és a dir, que pretén atorgar una privacitat que equival a la de les xarxes de cable.

El protocol WEP ha provocat molts problemes de seguretat a causa, principalment, del fet que l'algorisme criptogràfic en què es basa (RC4) ha resultat inadequat.

Quan no feia gaire que havia aparegut el WEP, es va descobrir que tenia una vulnerabilitat: si s'aconseguia un volum prou gran de dades xifrades, es podia esbrinar la clau per a desxifrar-les.

Actualment, un atacant sense gaires coneixements de *hacking* és capaç de trencar la seguretat del protocol WEP gràcies a eines que circulen per Internet.

Des de l'any 2004, l'organisme regulador de les comunicacions a les xarxes sense fil desaconsella el protocol WEP. Tanmateix, encara hi ha molts punts d'accés que el fan servir.

Protocol WPA

WPA és la sigla dels termes anglesos *wireless protected access*, és a dir, accés protegit a les xarxes sense fil.

El WPA va aparèixer per a solucionar els problemes que ocasionava el protocol WEP. Fins ara, el protocol WAP ha demostrat ser un protocol robust.

Molts dels dispositius de xarxa que incorporen funcionalitats WEP es poden configurar per a treballar amb el protocol WPA. Per a fer-ho, s'ha d'actualitzar el microprogramari (*firmware*), és a dir, el programari que opera el dispositiu de xarxa.

El protocol WPA soluciona tant la problemàtica de l'autenticació dels usuaris com la de la confidencialitat de les comunicacions. Té dos mecanismes d'autenticació possibles: el WPA-PSK i el 802.1X. Per a xifrar les dades fa servir l'algorisme TKIP.

• **WPA-PSK**. *PSK* és la sigla dels termes anglesos *preshared key*, és a dir, clau compartida prèviament. L'usuari i el punt d'accés comparteixen una contrasenya secreta que té entre vuit i seixanta-tres caràcters i es fa servir en el procés d'autenticació.

La comunicació entre el dispositiu i el punt d'accés està xifrada mitjançant un algorisme robust que fa molt difícil que un atacant pugui esbrinar la clau secreta.

Els atacants poden intentar esbrinar la contrasenya secreta mitjançant atacs de diccionari, és a dir, provant, a partir de les paraules d'una llista, una infinitat de contrasenyes. És molt important escollir una contrasenya secreta que sigui difícil d'esbrinar, que combini lletres amb números i caràcters alfanumèrics.

• **802.1X**. L'autenticació basada en el 802.1X permet utilitzar diferents tipus de mecanismes (certificat electrònic, Kerberos, etc.) per al procés d'autenticació entre un dispositiu i un punt d'accés.

Aquest sistema d'autenticació fa ús d'un servidor d'autenticació, és a dir, delega l'autenticació en un altre dispositiu. Habitualment, el 802.1X no s'aplica en xarxes domèstiques.

• ***TKIP*** és la sigla dels termes anglesos temporal *key integrity protocol*, és a dir, protocol d'integritat basat en claus temporals. El TKIP és l'algorisme que s'encarrega de xifrar les comunicacions en el protocol WPA. Es basa en la generació de valors aleatoris que es fan servir en el procés de xifratge per a fer molt més difícil els atacs de possibles *hackers*.

Protocol WPA2

El WPA2 és l'evolució del WPA. Incorpora les mateixes funcionalitats i característiques que el WPA, però, a més, inclou el xifratge basat en l'algorisme AES.

A diferència del WPA, cal actualitzar el maquinari per a fer que un dispositiu antic funcioni en el WPA2. Això és degut al fet que l'algorisme AES requereix un maquinari específic.

AES és la sigla dels termes anglesos *advanced encription standard*, és a dir, estàndard de xifratge avançat. Actualment, és l'algorisme més robust que hi ha per al xifratge de dades.