MP01 – UF 1 | INSTAL·LACIÓ, CONFIGURACIÓ I EXPLOTACIÓ DEL SISTEMA INFORMÀTIC

RA 1 | Instal·la sistemes operatius, analitzant les seves característiques i interpretant la documentació tècnica

1. El sistema informàtic i els seus mecanismes d'interconnexió
   - ACT 1 | Els components de hardware d'un sistema informàtic
   - ACT 2 | El software del sistema
   - ACT 3 | Topologies de xarxa
2. Característiques i funcions de l'arquitectura dels sistemes operatius
   - ACT 4 | La gestió del processador
   - ACT 5 | La gestió de la memòria principal
   - ACT 6 | La gestió de dades/informació
3. Tipus i llicències de sistemes operatius
   - ACT 7 | Classificació de sistemes operatius
4. Procés d'arrancada i registre del sistema
   - ACT 8 | Els firmware i els gestors de particions en l'arrancada del sistema
   - ACT 9 | Els nivells d'execució
   - ACT 10 | El registre de Windows
5. Identificació i manteniment dels controladors de dispositius
   - ACT 11 | Llistar els dispositius de hardware a Windows
   - ACT 12 | Llistar els dispositius de hardware a Ubuntu
6. Programari instal·lat al sistema i instal·lació de noves aplicacions
   - ACT 13 | Instal·lar i llistar el software a Windows
   - ACT 14 | Instal·lar un paquet de codi font en Ubuntu

ANEX 1 | Màquines virtuals

PT1 | Instal·lació de sistemes operatius
PT2 | Punts de restauració i mecanismes de recuperació de sistemes operatius
PT3 | Gestors d'arrencada i actualització de sistemes operatius

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

1. EL SISTIEMA INFORMÀTIC I ELS SEUS MECANISMES D'INTERCONNEXIÓ

En l'actualitat és difícil imaginar un món on l'ésser humà pogués treballar i processar totes aquelles dades i tota aquella informació que l'envolta sense l'ajuda i l'existència dels **sistemes informàtics**. Per tant, depèn de que la ciència informàtica, o computació, estudiï mètodes, tècniques i processos, amb la finalitat de processar, emmagatzemar i trametre informació i dades en format digital.

1.1. DEFINICIÓ I COMPONETS

Un sistema informàtic és aquell que amb una **entrada** de dades inicial, és capaç de **processar i/o emmagatzemar** aquesta informació, per proporcionar una **sortida** amb unes dades noves, que a la seva vegada, poden retoalimentar l'entrada d'informació al propi sistema informàtic. Figura | 1

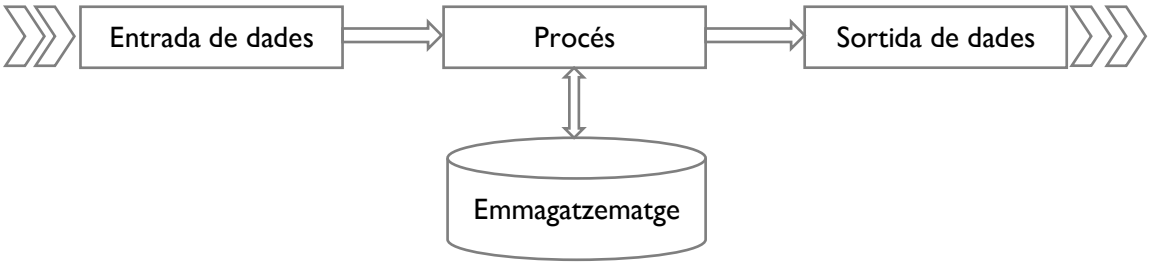


Figura 1 | El sistema informàtic

Segons el volum d'informació a tractar un sistema informàtic pot ser un sol ordinador amb un o pocs usuaris, passant per un sistema informàtic amb diversos ordinadors connectats entre ells utilitzant una gran diversitat de programari i un nombre elevat de persónes, fins arribar a organitzacions que requereixen que diferents sistemes informàtics a nivell internacional estiguin tots interconnectats i treballant plegats.

Per tractar tota aquesta informació, el sistema informàtic, ha de ser el conjunt de tres parts interrelacionades entre elles: Figura | 2

1. Component **Hardware**
2. Component **Software**
3. Component **Humà**

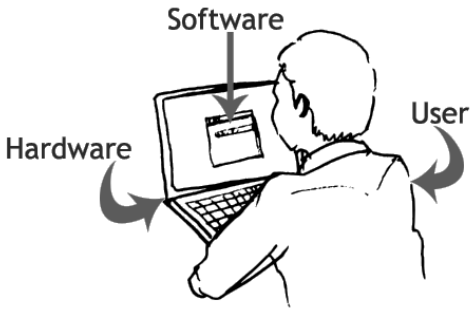


Figura 2 | Components del sistema informàtic

1.2. EL HARDWARE

Entenem com a hardware a tots aquells components del sistema informàtic que són parts tangibles, **físiques**, en aquell sistema: components interns (CPU, memòria, circuits, etc.), cablejat, perifèrics (pantalla, teclat, ratolí, etc.), unitats d'emmagatzematge, etc.

ACT 1 | **Els components de hardware d'un sistema informàtic**
Classifica els següents components físics del sistema informàtic:

CPU, ratolí, RJ45, placa base, memòria RAM, disc dur SATA, teclat, webcam, font d'alimentació, HDMI, pantalla, targeta gràfica, altaveus, impressora, targeta de so, pendrive, pantalla tàctil, dissipador, micròfon, escàner, targeta de xarxa i impressora multifunció.

Components interns	Perifèrics			Cablejat	Emmagatzematge
	Entrada	Sortida	Entrada/sortida		

Segons l'arquitectura de **Von Neumann**, tot sistema informàtic consta de 3 components de hardware principals: CPU, memòria principal i E/S, enllaçades entre si a través de 3 busos: dades, adreces i control: Figura | 3

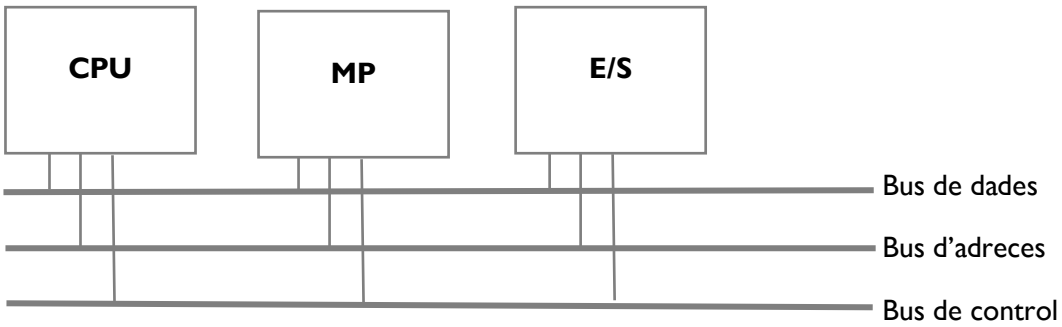


Figura 3 | Arquitectura de Von Neumann

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

La **CPU** (Control Process Unit) és l'anomenat component principal, o cervell, del sistema informàtic, i és l'encarregada d'interpretar i executar instruccions, així com de processar dades. Actualment sol estar formada per més d'un microprocessador[1]. En la CPU podem distingir 3 components:

1. **ALU (Arithmetic Logic Unit):** encarregada de realitzar operacions aritmètiques simples i operacions de lògica booleana.
2. **CU (Control Unit):** encarregada de interpretar les instruccions i d'enviar dades i senyals de control a altres d'altres components.
3. **Registres:** petites memòries integrades de gran velocitat i poca capacitat dedicades a emmagatzemar de manera transitòria valors molt utilitzats o utilitzats recentment.

A més, les CPU poden integrar coprocessadors matemàtics FPU (Floating-point Unit) per tal de resoldre operacions complexes per la ALU (amb números racionals molt grans o molt petits).

La **MP** (Memòria Principal), també anomenada memòria interna o memòria central, és el component hardware en el qual s'emmagatzemen temporalment les dades i instruccions de programa que la CPU està processant o processarà en un determinat moment. Normalment és tracta de mòduls de memòria volàtils[2]. Molts cops ens referim a aquesta memòria com a **RAM** (Random Acces Memory), tot i que hem d'entendre que la MP, és un conjunt de memòries, de les quals la memòria RAM és la principal, però també consta de memòries cau ("caché") del propi processador, memòries ROM (Read Only Memory) o registres.

La **E/S** (Entrada/Sortida) fa referència a tots els dispositius perifèrics que proporcionen als usuaris la capacitat d'interacció amb el component físic i/o lògic del sistema informàtic. Per tal de funcionar correctament, cada perifèric ha de disposar dels controladors ("divers") apropiats[3]. Actualment, els dispositius d'E/S poden comunicar-se a través dels busos del sistema directament tant amb la CPU com amb la MP, gracies al sistema **DMA** (Direct Memory Access), fet que allibera molta carrega a la CPU i resol antics problemes dels sistemes d'interrupcions amb diferents velocitats de resposta.

Els **Busos del sistema** compleixen cadascun una **funció de transport** determinada: el bus de dades transporta blocs d'informació d'un component a un altre, el bus d'adreça transporta direccions de memòria d'on llegir o escriure les dades i el bus de control transporta els bits que marquen el temps i l'ordre perquè tot el sistema informàtic treballi de manera coordinada. Aquests busos estan formats per diversos cables, actualment 32/64, per on poden circular de manera paral·lela aquells bits d'informació[4]. Aquesta capacitat, junt a la seva velocitat de treball, marcaran en gran mesura la velocitat del sistema informàtic.

[1] S'entén per microprocessador a una CPU que es manufacturada com a un únic circuit integrat
[2] Un cop apagat el sistema informàtic (no te corrent elèctrica), el contingut de la memòria es borra, es buida.
[3] Els *drivers* són dependents de cada sistema operatiu, per tant, un mateix dispositiu pot necessitar diferents *drivers* segons el sistema operatiu del sistema informàtic on treballarà.
[4] Els busos delimiten, per tant, si un sistema es de 32 o 64 bits, amb les limitacions que això pot comportar.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

1.3. EL SOFTWARE

Entenem com a software al suport **lògic** del sistema informàtic, tot allò intangible que ens facilita la intercomunicació amb el hardware del ordinador.

La programació d'aquest software es fa per part dels desenvolupadors d'aplicacions normalment en un llenguatge d'alt nivell (C++, JAVA, Python, etc.) que són més "semblants" al llenguatge natural que el llenguatge màquina que entén el hardware del ordinador. Per tant, cal un compilador i/o intèrpret que faci aquesta traducció. Aquest intèrpret són llibreries pròpies de cada sistema operatiu que es el software de base, o principal, d'un sistema informàtic. A partir d'això, podrem dividir el software en 3 grans blocs:

1. **Software del sistema:** desvincula als usuaris i programadors dels detalls interns (físics) del sistema informàtic. Dins d'aquest grup trobem:
    a. Sistemes operatius
    b. Controladors de dispositius
    c. Eines de diagnòstic
    d. Eines de correcció i optimització
    e. Altres utilitats del sistema operatiu
2. **Software de programació:** inclou aquell software que permet crear nou software:
    a. Editors de text (sense format)
    b. Compiladors
    c. Intèrprets
    d. Depuradors
    e. IDE (Integrated Development Environment)
3. **Software d'aplicació:** és aquell que permet als usuaris dur a terme una determinada tasca o tasques de molt diversos propòsits:
    a. Aplicacions ofimàtiques
    b. Aplicacions empresarials
    c. Aplicacions de disseny gràfic
    d. Videojocs, i un interminable etc.

ACT 2 | **El software del sistema**
Cerca el nom d'algun software del sistema dels següents sistemes operatius:

Software del sistema operatiu	Windows 10	Ubuntu Desktop 18.04
Gestor de controladors de dispositius		
Eines de diagnòstic		
Eines de correcció i optimització		
Eines de supervisió		
Altres utilitats del sistema operatiu		

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

1.4. EL COMPONENT HUMÀ

No hem d'oblidar que sense l'acció i intervenció d'un esser humà, el sistema informàtic no estaria complert, ja que, en major o menor mesura, sempre necessita d'un usuari o usuaris per poder funcionar i als que poder proporcionar un sortida a mode de solució a les seves demandes o necessitats.

Aquest recurs humà pot ser només a nivell d'usuari final, que utilitza el hardware i software del sistema per treballar, estudiar, informar-se, comunicar-se o entretenir-se. Existeixen però uns altres usuaris "avançats" o tècnics, el **persónal informàtic** que desenvolupen diferents funcions amb els sistemes informàtics, per exemple, d'una empresa. Segons les seves funcions els podem classificar en els següents rols:

a. **Direcció:** coordinació de departaments o àrees informàtiques.
b. **Anàlisi:** persónal responsable de torbar solucions als problemes que sorgeixin o proposar millores sobre els procediments actuals.
c. **Programació:** tradueixen en codi, llenguatge de programació, les solucions i/o propostes dels analistes.
d. **Explotació:** responsables d'executar programes i comprovar el seu funcionament en els equips i sistemes existents.
e. **Operadors:** responsables del funcionament dels sistemes operatius, els seus processos i suport informàtic, manteniment d'equips i perifèrics i/o responsables de les xarxes d'interconnexió.

1.2. INTERCONNEXIÓ DE SISTEMES INFORMÀTICS

Com ja hem comentat anteriorment i segons el volum d'informació a tractar un sistema informàtic pot ser un sol ordinador amb un o pocs usuaris, passant per un sistema informàtic amb diversos ordinadors connectats entre ells utilitzant una gran diversitat de programari i un nombre elevat de persónes, fins arribar a organitzacions que requereixen que diferents sistemes informàtics a nivell internacional estiguin tots interconnectats i treballant plegats.

Per tant, ens cal conèixer com són les **xarxes** que permeten aquesta interconnexió de sistemes informàtics. Per fer-ho podem fer una classificació de xarxes segons diferents aspectes:

1. **Segons el seu abast:** Figura | 4

    a. Xarxes d'àrea local
    b. Xarxa d'àrea metropolitana
    c. Xarxes d'àrea estesa

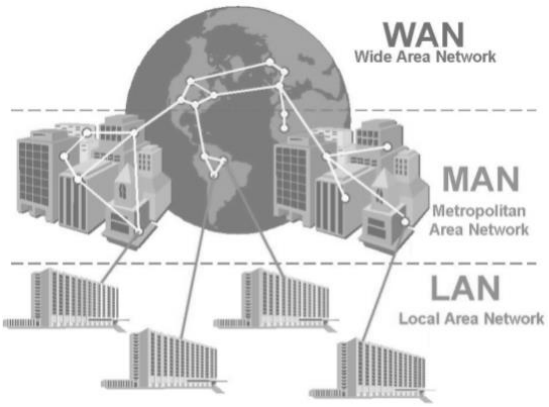


Figura 4 | Classificació de xarxes segons el seu abast

2. **Segons el mètode de connexió:**

    a. Xarxes guiades (cablejada)
    b. Xarxes no guiades (sense fils, "wireless")

3. **Segons la funcionalitat:** Figura | 5

    a. Xarxes basades en servidor (maquines servidor i maquines clients)
    b. Xarxes P2P (totes les màquines d'igual a igual, "peer to peer")

4. **Segons la seva topologia:**

    a. Xarxes en anell
    b. Xarxes en anell doble
    c. Xarxes en estrella
    d. Xarxes en bus
    e. Xarxes en arbre
    f. Xarxes en malla

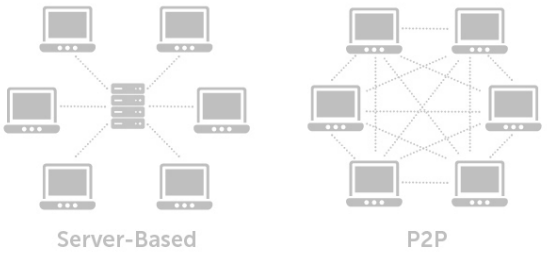
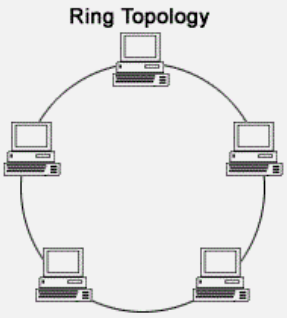


Figura 5 | Classificació de xarxes segons la seva funcionalitat

ACT 3 | **Topologies de xarxa**

Hem vist que tenim fins a 6 tipus de topologies de xarxa. Busca per cadascuna d'elles una petita definició i un esquema (dibuix) de com es la connexió, per exemple:

TOPOLOGIA EN ANELL: cada node o ordinador de la xarxa té una única connexió d'entrada i una de sortida, cada node o ordinador es connecta amb el següent fins que al final l'últim es connecta amb el primer.



2. CARACTERÍSTIQUES I FUNCIONS DE L'ARQUITECTURA DELS SISTEMES OPERATIUS

Com ja hem pogut començar a intuir, hi ha un software necessari a tots els equips informàtics que fa de pont entre el hardware i la resta d'aplicacions i programes (Figura | 6) a través d'uns controladors específics, un software de programació concret i unes eines de diagnòstic, monitorització o correcció específiques. Aquest software de base és el **sistema operatiu** i en aquest apart estudiarem les seves característiques i funcions.

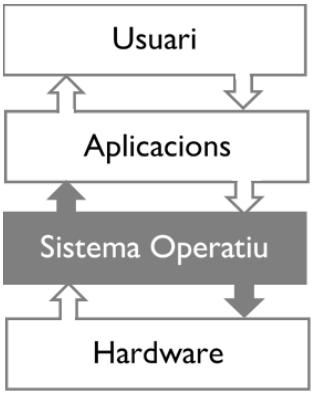


Figura 6 | Situació del sistema operatiu dins el sistema informàtic

2.1. EL SISTEMA OPERATIU, UN GESTOR DE RECURSOS

Els sistemes operatius són abans de tot **administradors de recursos**: Figura | 7

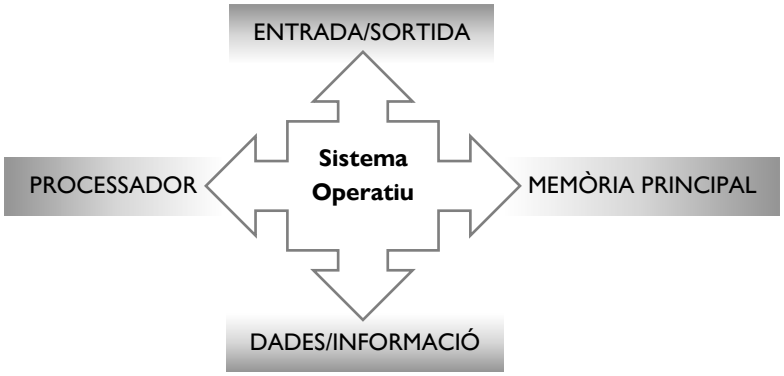


Figura 7 | El sistema operatiu com a gestor de recursos

2.2. LA GESTIÓ DEL PROCESSADOR

Quan una aplicació es posa en marxa, esdevé un **procés**, que requereix de l'atenció del **processador** per poder dur a terme la seva activitat. Un processador, entès com un nucli de CPU, només pot tractar un procés en cada moment. Per tant, és tasca del sistema operatiu, planificar quin procés utilitzarà a cada instant cadascuna del nuclis de processadors dels que disposi el sistema.

Per fer-ho ha de seguir com a norma el utilitzar la CPU el major temps possible i reduir el temps de resposta dècada procés. Per fer-ho ha d'intentar alternar els processos de manera que, quan un està esperant una dada de la MP, el disc dur, o una acció d'E/S, un altre pugui "ocupar la CPU" i fer-la servir.

Aquesta **planificació** (Scheduling) és pròpia de cada sistema operatiu i en trobem algorismes que realitzen aquesta planificació dividits en 2 grans grups:

1. Algorismes de planificació **no apropiatius** (Non-Preemptive): més sencills i menys eficaços, per exemple, **FCFS** (First Come First Serverd) o **SJF** (Short Job First). En aquests algorismes el flux d'execució de processos es **seqüencial**, és a dir, un procés ocupa la CPU fins que acaba no deixant espai a d'altres processos, i és propi de sistemes antics, com per exemple Windows 3.11.

2. Algorismes de planificació **apropiatius** (Preemptive): més complexos de programar però permeten una execució **concurrent**, és a dir, diversos processos poden utilitza "alhora" la CPU, alternant-se segons unes normes preestablertes. Són exemples d'aquest tipus d'algorisme els **SRTF** (Shortest Remaining Time First) o **RR** (Round Robin).

Els sistemes operatius actuals utilitzen bàsicament algorismes apropiatius, als que incorporen conceptes com **prioritats**, no tots els processos són igual d'importants, o fan **combinacions multinivell** amb diferents cues de processos gestionades segons un ordre establert i mitjançant diferents algorismes a cada cua de processos[5].

ACT 4 | **La gestió del processador**

Quan parlem de Sheduling hi ha uns quants termes habituals que cal conèixer. Busca i defineix els següents conceptes:

CPU Utilization	**Turnaround Time**	**Load Average**
Throughput	**Waiting Time**	**Response Time**

[5] Pots veure alguns sistemes operatius i el sheduling que utilitzen https://en.wikipedia.org/wiki/Scheduling_(computing)#Summary

Autor | RAFAEL GARCÍA SUÁREZ
Contacte | rgarc259@xtec.cat

2.3. LA GESTIÓ DE LA MEMÒRIA PRINCIPAL

La memòria principal és un recurs escàs[6] pel qual competeixen els diferents processos a l'hora de llegir o escriure informació necessària pel seu funcionament. Les posicions de memòria es van omplint, i cal que el sistema operatiu determini quines queden lliures o quines s'han d'alliberar per poder emmagatzemar la informació requerida per un procés.

La manera d'**organitzar** l'espai disponible a memòria i els mètodes d'**adreçament** cap a les posicions de memòria és una organització pròpia de cada sistema operatiu. Distingim dos grans tipus:

1. **Paginació:** per implementar la paginació, els espais de memòria física i lògica es divideixen en els mateixos **blocs de mida fixa**. Aquests blocs de mida fixa de memòria física es diuen **marcs**, i els blocs de mida fixa de la memòria lògica es diuen **pàgines**. Quan es necessita executar un procés, les pàgines del procés de l'espai de memòria lògica es carreguen en els marcs de l'espai d'adreces de la memòria física. Ara, l'adreça generada per la CPU per accedir al marc es divideix en dues parts, és a dir, el número de pàgina i el desplaçament de la pàgina. La taula de pàgines utilitza el número de pàgina com a índex i cada procés té la seva taula de pàgina separada que assigna una adreça lògica a l'adreça física. La paginació permet que un procés s'emmagatzemi en una memòria de **forma no contigua**, i per tant, es resol el problema de la fragmentació externa. Tot i això, el que si genera és **fragmentació interna** dins dels marcs.

2. **Segmentació:** en la segmentació, l'espai d'adreces lògiques és la recopilació de **segments de mida variable**. Cada segment té el seu **nom** i una **longitud**. Per a l'execució, els segments de l'espai de memòria lògica es carreguen a l'espai de memòria física. Els segments es numeren i es fa referència pel número del segment en lloc del nom del segment. Aquest número de segment s'utilitza com a índex de la taula de segments i la longitud determina el límit del segment. Aquest sistema suporta la visualització de la memòria per part de l'usuari, i pot generar una **fragmentació externa** a mesura que la memòria s'omple amb els blocs de mida variable.

> ACT 5 | **La gestió de la memòria principal**
> Per acabar de comprendre el funcionament dels sistemes de gestió de memòria per paginació i segmentació, cerca un esquema (dibuix) explicatiu del funcionament de cadascun d'ells.
>
> ¿Quin tipus de sistema de gestió de memòria utilitzen les versions actuals dels sistemes operatius d'escriptori de WINDOWS, LINUX i MAC OS X?

[6] Alguns sistemes operatius permeten utilitzar una part reservada de la memòria secundària (discs durs) com si fos part de la memòria principal (Swapping)

2.4. LA GESTIÓ DE L'ENTRADA/SORTIDA

L'E/S d'un sistema informàtic la composen un conjunt de **dispositius molt variats** i complexos de programar. En aquest cas els objectius del sistema operatiu per tal de gestionar-los seran:

1. Proporcionar una **interfície uniforme** per a l'accés als dispositius (independència del dispositiu), com per exemple, el DMA.
2. Proporcionar **controladors** (drivers) per als dispositius concrets.
3. Solucionar automàticament els errors més típics dels dispositius.
4. Utilitzar la memòria cau ("caché") per als dispositius d'emmagatzematge secundaris (discos).
5. Planificar de forma òptima les peticions a CPU i MP que s'originin des dels dispositius.

2.5. LA GESTIÓ DE DADES/INFORMACIÓ

A nivell intern, els components de hardware entenen les dades o la informació com un seguit de zeros i uns, un **codi binari**. Per tant, conceptes com el d'arxiu o **fitxer**[7] que podem utilitzar habitualment al parlar de les dades i/o informació que tenim al nostre sistema informàtic és un concepte d'alt nivell allunyat del maquinari del sistema.

Per tant, els usuaris, necessiten un sistema per poder comprendre i saber gestionar i localitzar les dades binaries emmagatzemades a les memòries secundàries del sistema informàtic (discs durs). El sistema d'arxius o **sistema de fitxers** és el component del sistema operatiu encarregat d'administrar i facilitar l'ús de memòries d'aquestes perifèriques. Les seves principals funcions són:

- **L'assignació d'espai als fitxers.**
- **L'administració de l'espai lliure**
- **L'accés a les dades resguardades.**

Ho fa estructurant la informació guardada en un dispositiu d'emmagatzematge de dades i és capaç, després, de representar-la d'una forma comprensible al usuari, ja sigui textual o gràficament utilitzant un gestor d'arxius. La majoria dels sistemes operatius gestionen el seu propi sistema d'arxius.

En un sistema informàtic el més habitual és utilitzar dispositius d'emmagatzematge de dades que permeten l'accés a les dades com una cadena de blocs de la mateixa mida, de vegades anomenats **sectors**, normalment de 512 bytes de longitud (també denominats clústers). El programari del sistema d'arxius és responsable de l'organització d'aquests sectors en **arxius i directoris** i manté un registre de quins sectors pertanyen a quins fitxers i quins no s'han utilitzat. En la pràctica, un sistema d'arxius també es pot utilitzar per accedir a dades generats dinàmicament, com els rebuts a través d'una xarxa de computadors (sense intervenció d'un dispositiu d'emmagatzematge).

Els sistemes d'arxius proporcionen mètodes per **crear**, **moure**, **renombrar** i **eliminar** tant fitxers com directoris. A més, haurien de garantir l'**accés segur** a aquests fitxers o directoris oferint diferents privilegis, o l'absència d'aquests, a determinats usuaris del sistema.

[7] Entenem per fitxer un conjunt de dades relacionades i agrupades que s'identifiquen per un nom.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

ACT 6 | **La gestió de dades/informació**
Treballarem amb els sistemes de fitxers propis dels sistemes operatius que instal·larem a les pràctiques, i aprendrem a utilitzar-los tant en mode text (intèrpret de comandes) com en mode gràfic. Tot això ho farem al RA1 de la UF2. De moment, consulta la següent taula i contesta aquestes preguntes:

1. Quin sistema de fitxers utilitzen els sistemes operatius WINDOWS actuals de manera predeterminada?
2. És el sistema de fitxers anterior compatible amb els sistemes operatius LINUX? I amb els sistemes MAC OS X?
3. Quin sistema de fitxers utilitzen els sistemes operatius LINUX actuals de manera predeterminada? Quins eren els seus sistemes de fitxer antecessors?
4. És el sistema de fitxers anterior compatible amb els sistemes operatius WINDOWS? I amb els sistemes MAC OS X?
5. HFS+ és el sistema de fitxers predeterminat de MAC OS X. És compatible amb les versions anteriors dels sistemes MAC OS?
6. Als discs durs externs o als pendrives és habitual trobar que s'han formatjat amb un sistema de fitxer FAT32, per ser un dels més compatibles, sense necessitat de complements, amb els diferents sistemes operatius. Tot i això, és un sistema de fitxers força antic. Cerca els que possiblement són els seus dos principals inconvenients.

3. TIPUS I LLICÈNCIES DE SISTEMES OPERATIUS

Quan parlem de sistemes operatius ens venen de seguida al cap un quants de coneguts i fins i tot, que utilitzem diàriament a casa, la feina, les classes, el mòbil, etc. Aquests sistemes es poden classificar en diversos tipus segons diferents punts de vista, i es poden utilitzar sota diferents tipus de llicències, ja siguin privatives (de pagament) o lliures (gratuïtes).

Tal i com veurem en aquest punt, hi ha molts tipus de sistemes operatius i moltes llicències d'ús al mercat. Tot i això, hi ha una sèrie de "**característiques desitjables**" que hauria de tenir qualsevol sistema operatiu:

1. **Eficiència:** no hauria d'utilitzar una gran quantitat de recursos del ordinador (a nivell de CPU i MP) per funcionar.
2. **Fiabilitat:** no hauria de fallar, i si ho fa, hauria de tenir mecanismes de recuperació i no afectar a la resta d'aplicacions.
3. **Facilitat de manteniment:** hauria de disposar d'un sistema d'actualitzacions, millores i correccions.
4. **Mida reduïda:** tot i la gran capacitat dels disc durs actuals, no hauria d'ocupar molt espai.
5. **Seguretat:** hauria de proporcionar eines de control de virus i intrusions.
6. **Compatibilitat de recursos:** hauria de proporcionar eines per la gestió simultània d'aplicacions, fer quotes de disc, auditar successos del sistema, etc.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

3.1. TIPUS DE SISTEMES OPERATIUS

El primer que em de conèixer a l'hora de classificar el sistemes operatius, es la seva estructura interna:

Monolític: són els sistemes operatius d'estructura més simple. Totes les funcionalitats del sistema (drives, sistema de fitxers, gestió de memòria, etc.) s'executen sobre el nucli (kernel) d'aquest. Cadascuna de les rutines del nucli pot cridar a la resta, cosa que presenta inconvenients ja que la fallada d'una servei afecta a tot el sistema operatiu. A més cada correcció d'un error o la incorporació d'una nova característica implica la recompilació de tot el kernel, cosa que requereix una gran quantitat de memòria i temps.

Micronucli: en aquest tipus de sistemes operatius les operacions centrals són manejades pel kernel i la interfície d'usuari es manejada per l'entorn (shell). El microkernel s'encarrega de tot el codi d'un sistema i de planificar els fils dels processos (threads) amb la finalitat de poder incloure la multitasca. Les seves principals avantatges són: la uniformitat d'interfícies, la portabilitat i la fiabilitat.

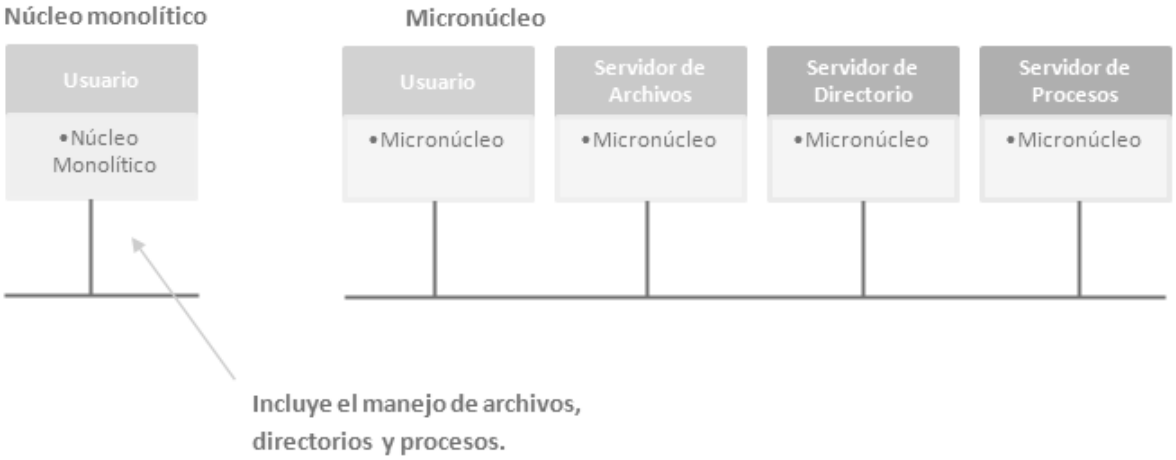


Figura 8 | Diferències entre un sistema amb kernel monolític i un sistema amb microkernel

Client-Servidor: aquesta estructura la podríem afegir dins dels sistemes amb micronucli, tot i que en aquest tipus d'estructura es defineixen dos tipus de processos: els processos servidors, cadascun dels quals proporciona un servei concret, i els processos clients, que utilitzen aquests serveis. La idea és minimitzar el nucli traslladant el codi de tots els seus serveis a les capes superiors, i deixant al kernel l'única funció de comunicar (mitjançant missatges) els processos clients amb els processos servidors, i aquests últims amb el hardware. El fet de que els serveis s'utilitzin a nivell de procés d'usuari i no de nucli fa que sigui una estructura robusta ja que una fallada afecta a aquell procés però no a tota la màquina.

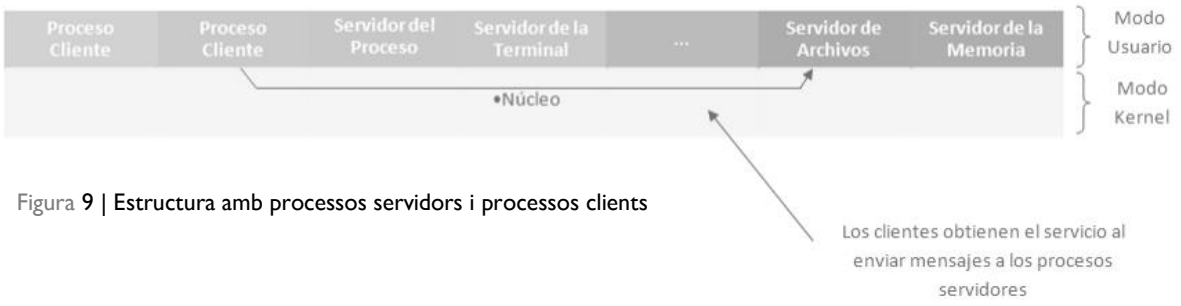


Figura 9 | Estructura amb processos servidors i processos clients

Jeràrquic (per capes): en aquesta estructura el sistema operatiu queda definit modularment per capes o nivells. És una estructura jerarquitzada on cada capa només es pot comunicar amb la capa immediatament inferior, la seva predecessora, i on cada capa més interna requereix més privilegis que l'anterior. En la capa més interna (la capa 0) s'ubica el control del hardware, en la capa 1 trobaríem la gestió de memòria, en capes següents la gestió de processos, la gestió d'E/S, fins arribar a les capes més externes on trobaríem les aplicacions d'usuari i la seva interfície de treball (Figura | 10). La seva principal avantatge es que proporciona facilitat de construcció de funcionalitats i depuració d'errors. Per contra, requereix un esforç inicial de planificació de tasques (per cada capa) i el temps que empra el sistema per anar passant de capa a capa per funcionar.

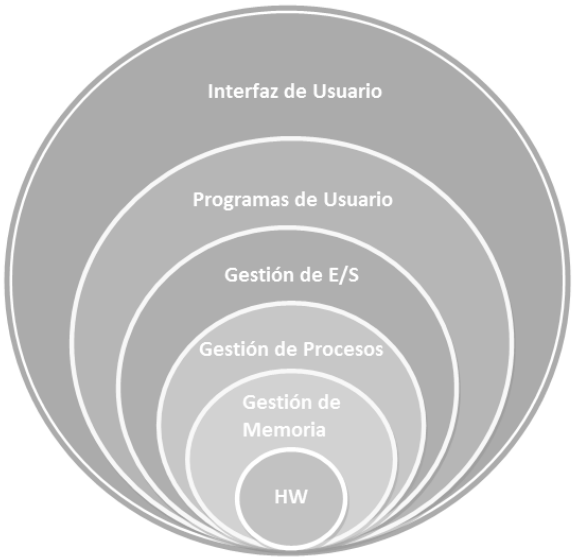


Figura 10 | Capes d'un sistema operatiu amb estructura jeràrquica

Per mòduls: es el tipus d'estructura que presenten la majoria de sistemes operatius moderns. Es basa en disposar d'un kernel composat de diferents mòduls separats de forma independent, és a dir, si un mòdul falla no afecta a la resta, ni al nucli. Aquest mòduls es poden carregar dinàmicament (quan es necessari, o al arrencar el sistema operatiu) al nucli. Per tant, el nucli només conté components fonamentals i es connecta altres serveis i/o components per fer les funcions addicionals[8].

En general, veiem que l'estructura actual per mòduls es sembla força a l'estructura de capes, però és molt més flexible ja que qualsevol mòdul pot cridar a un altre. També és similar a l'estructura de micronucli, doncs també tens les funcions essencials, però és molt més eficient ja que no necessiten un mecanisme basat en passar missatges per comunicar-se, només li cal una sèrie d'interfícies conegudes.

3.2. CLASSIFICACIÓ DE SISTEMES OPERATIUS

Un cop hem vist com pot ser l'estructura interna d'un sistema operatiu, podrem classificar-los també sota altres criteris, segons si ofereixen o no una determinada prestació:

1. **Pot realitzar més d'una tasca alhora?**

   En cas negatiu, ens trobarem amb sistemes **monotasca** que treballen de forma seqüencial. En cas afirmatiu, en trobarem davant de sistemes **multitasca** que poden executar diversos processos de manera simultània. Dins dels sistemes multitasca podem trobar-nos sistemes **cooperatius**, el processos són els que prenen el control de la CPU i decideixen quan poden deixar-la lliure per d'altres processos, o sistemes **apropiatius**, on es el propi sistema operatiu qui decideix els temps d'utilització de la CPU per cada procés[9].

[8] El sistemes operatius amb estructura modular utilitza programació orientada a objectes per la gestió de la carrega de mòduls, components i serveis al nucli del sistema.
[9] Recorda el punt 2.2. d'aquest document pel que fa als diferents tipus d'algorismes en la gestió del processador.

2. **Suporta la creació de més d'un usuari?**

   Si el sistema no permet ni tant sols crear, o fer "login" amb diferents usuaris estem parlant d'un sistema **monousuari**. De vegades, monousuari també fa referència a sistemes, que tot i poder crear diferents usuaris, no permeten el treball en el mateix temps, amb usuaris diferents. Llavors, els sistemes **multiusuari**, seran aquells que permeten definir diferents comptes d'usuari que a més, podran realitzar tasques dins del sistema de manera simultània.

3. **És capaç d'utilitzar més d'un processador?**

   Els sistemes operatius antics només podien gestionar un únic processador, i per tant, eren **monoprocés**. Amb l'aparició de chips amb més d'un nucli[10] i més tard d'ordinadors amb més d'un processador incorporats, van aparèixer també els sistemes **multiprocés**. La manera de gestionar aquests múltiples processadors es divideix en dos: els sistemes **simètrics**, on el treball es divideix de manera equitativa en parts que executen cadascun dels processadors, i els sistemes **asimètrics**, on cada processador porta a terme diferents tasques.

4. **Es poden obtenir resultats en un temps determinat?**

   En la majoria de sistemes operatius que coneixem, el executar un programa determinat no sempre triga el mateix temps, ja que depèn molt de la càrrega del sistema operatiu en aquell moment, i són, per tant, sistemes operatius de **temps compartit**. Però també existeixen un tipus de sistemes operatius, els sistemes de **temps real**, on la clau es que el temps de resposta sempre sigui igual (o dins d'unes restriccions de temps concretes), ja que afecten a operacions sensibles que requereixen aquesta fiabilitat i determinació quan ho requereix l'usuari[11].

3.3. LLICÈNCIES PER SISTEMES OPERATIUS

Ja podem classificar els sistemes operatius segons la seva estructura i/o segons el tipus de funcionalitat que proporcionen. També podríem tipificar-los segons el **tipus de llicència** que utilitzen per la seva distribució.

Bàsicament una llicència per a sistema operatiu (o de software en general) és un contracte que existeix entre aquell que posseeix els **drets d'autoria** i l'entitat, persónal o corporativa, que l'està adquirint. En aquest contracte es defineixen amb certesa els **drets i obligacions** d'ambdues parts, i també, es pot establir el temps de durada de dita llicència, permanent o limitada, o el territori sobre el qual seran aplicades les estipulacions contractuals, ja que cada país teles seves pròpies regulacions sobre les llicències de software.

Podem establir dos grans tipus de llicències:

1. **Llicències de codi lliure**.
2. **Llicències de codi propietari**.

[10] Els primers chips multinucli van aparèixer cap al 1980, tot i que no trobem un "ús domèstic" generalitzat fins a principis del segle XXI amb els primers processadors Intel Core Duo.

[11] Molts sistemes operatius en temps real són construïts per aplicacions molt especifiques com el control del tràfic aeri, bosses de valors, control de refineries, control de laminadores, en la branca de la automobilística, de l'electrònica de consum, etc.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

El nom de **llicències de codi lliure** pot confondre a primera vista ja que el fet de ser lliure no implica directament a que sigui gratuït, o que no pugui tenir regulacions legals. Un cop fet aquest aclariment, podem definir el sistemes de codi lliure com aquells que ofereixen al consumidor el seu **codi font** original, i que a més els proporciona la capacitat per **usar-lo**, **modificar-lo** i **distribuir-lo** (amb o sense modificacions).

La filosofia darrera d'aquest tipus de llicència es troba sustentada en el benefici de la comunitat a través de la retroalimentació i la col·laboració entre programadors. Un exemple seria el nucli (kernel) de Linux, que ha estat utilitzat per la comunitat com a peça angular en el disseny de sistemes operatius que operen sota aquesta llicència de codi lliure.

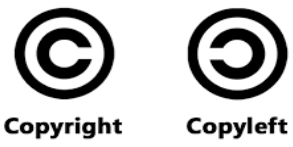
Aquesta llicencia es pot dividir en altres subtipus segons unes clàusules més específiques regulades per una legislació que impedeix, o no, la utilització del codi font sense autorització o sota quines condicions. Aquesta legislació rep el nom de **Copyleft**[12]. Per tant, tindrem:

a. Llicències de codi lliure **sense protecció Copyleft**: s'autoritza a tercers per no sols modificar el codi sinó que també per poder llicenciar el mateix sota els seus propis termes (cosa que pot provocar la privatització per par d'algun programador que ho modifiqui). És el tipus de llicència que empra el conegut com software de domini públic.
b. Llicències de codi lliure **amb protecció Copyleft**: aquestes obliguen als programadors que vulguin distribuir el codi a seguir l'alienació i restriccions que s'hagin imposat, i per tant, podem impedir, per exemple, la situació anterior de privatització del codi lliure original.

Dins del grup de llicències de codi lliure amb protecció Copyleft, trobem diversos estàndards:

- **GNU GPL** (Llicencia Pública General). És un tipus especial de llicències lliures amb Copyleft ja que permet integrar-se amb mòduls de software no lliure, i fins i tot la seva comercialització. Aquesta llicència declara de forma explicita "que qualsevol obra de llicència GPL pot ser venuda a qualsevol preu o be distribuïda gratuïtament".
- **Debian Free Software Guidelines**. És un dels tipus que te més definides i clares les seves línies d'actuació (guidelines), i aquestes s'apliquen estrictament entre Debian i la comunitat programadora. Exigeix que qualsevol distribució feta sota llicència Debian estigui acompanyada del seu codi font i aquest ser lliure. A més aquestes línies no s'han de modificar segons el pais on es trobi i els productes derivats han d'estar sota aquest tipus de llicència.
- **BSD** (Distribució de Software de Berkeley). Aquestes llicències serien les més permitives del software lliure, ja que les seves línies permeten la comercialització del software sense restriccions, tampoc obliga a compartir el codi font i només es garantitza el reconeixement pels programadors que participen en la elaboració del producte. Un pas intermig entre les llicències BSD i les llicències GNU serien les llicències **MPL** que obliga a entregar el codi modificat al creador original i només permet llicenciar arxius binaris.

[12] Es pot dir que el Copyleft es el Copyright de les llicències de codi lliure. Normalment el Copyright te la funció d'evitar que algun material sigui modificat i distribuït per algú aliè a l'autoria del producte, cosa que es contraposa a la filosofia del codi lliure, i d'aquí va néixer el Copyleft.



Anomenarem **llicències de codi propietari**, a totes aquelles on l'autor del projecte limita els drets de copia, modificació i distribució. Per protegir-se utilitzaran llicencies sota **Copyright**, i no distribuiran de manera oberta el codi font del seu projecte. Dins d'aquest tipus de llicència trobarem:

- **Retail**. Llicència atorgada a tot aquell software desenvolupat amb intencions de ser comercialitzat. Dona dret a l'usuari final per instal·lar-lo de manera il·limitada, a cedir-lo o fins i tot vendre-ho a un tercer.
- **OEM**. Aquestes van lligades a que es distribueixin quan el sistema operatiu s'instal·li en un equip nou. Per tant, prohibeix la seva venda sota altres circumstàncies. A més, es poden establir altres limitacions, com per exemple, el nombre de cops que pot ser reinstal·lat.
- **Per volums**. És un tipus especial de llicència OEM normalment pensada per a empreses. En aquest tipus de llicència normalment no es limita que l'equip a de ser nou en la instal·lació, però si que s'estipula la quantitat d'equips que poden utilitzar el sistema operatiu de manera legal.

ACT 7 | **Classificació de sistemes operatius**

Durant el decurs del punt 3 hem vist moltes maneres de classificar els sistemes operatius, des de la seva estructura interna fins al seu tipus de llicència. Omple ara la següent taula per aquests sistemes operatius:

MS-DOS, Windows 10, Ubuntu Desktop 18.04, Windows CE, Mac OS X "El Capitán", LynxOS i Solaris.

SISTEMA OPERATIU	Estructura del nucli	Monotasca / Multitasca*	Monoprocés / Multiprocés**	Temps real / Temps compartit	Codi lliure / Codi privat	Tipus de llicències
MS-DOS						
Windows 10						
Ubuntu Server 18.04						
Windows CE						
MAC OS X v10.11						
Solaris v11.2						
Android 8.1.0						

* En cas de sistemes multitasca especifica si són cooperatius o apropiatius
** En cas de sistemes multiprocés especifica si són simètrics o asimètrics

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

4. PROCÉS D'ARRANCADA I REGISTRE DEL SISTEMA

Hi ha alguns fitxers, serveis i aplicacions dels sistemes operatius que conformen la base de tot allò que esta configurat al sistema, ja sigui des del punt de vista de com es posa en marxa, ja sigui de com està configurat, o quins dispositius i aplicacions hi estan instal·lades. En aquest punt ens centrarem en conèixer el procés d'arrencada i el registre del sistema operatiu, concretament de les versions que utilitzarem durant les pràctiques del curs, és a dir, les versions actuals dels sistemes Windows i Ubuntu.

Però abans d'entrar a les peculiaritats de cada sistema operatiu, em de considerar que hi ha un procés previ des de que un usuari prem el botó de "power" del equip informàtic fins que els sistema operatiu agafa el control de la màquina. És, per tant, un procés sempre igual i independent del sistema o sistemes operatius que tinguem instal·lat/s a la màquina. Aquests són els seus passos: Figura | 11

1. **Subministrament de corrent:** quan premem el botó d'encesa el que fem és permetre la connexió de la font d'alimentació i que el corrent elèctric arribi a la placa base, i al seu temps al processador, ventiladors, disc durs, etc. Aquest pas del procés acaba amb una senyal de "power good" generada pel chipset de la placa base.

2. **La BIOS (Basic Input Output System):** el processador s'inicia i carrega la BIOS en memòria (en un àrea reservada de 64KB que els fabricants de memòries RAM deixen abans del primer megabyte al rang F000-FFFF) o directament llegeix la ROM (Read Only Memory) del mateix chip de la BIOS i l'executa. La BIOS és un firmware[13] que te com a finalitat configurar i detectar els elements connectats al sistema informàtic, **POST** (Power On Self Test). Aquesta també conté el programa BIOS SETUP que ens permet, si així o volem, ajustar aspectes com la velocitat d'accés a la RAM, el multiplicador de la CPU, habilitar o deshabilitar components, gestió d'energia, voltatges, etc., o com és un cas habitual, canviar el ordre d'arrancada a través d'un dispositiu o un altre (primer des de disc dur, o des de lector òptic, o des de USB o xarxa).

3. **POST:** el primer que es testeja és la targeta gràfica (situada a la posició C000) i s'arranca el sistema de vídeo. A partir d'aquí podrem veure (si no hi ha una pantalla del fabricant pel mig) com el POST fa les següents comprovacions:

    a. **Verificar la RAM i recompte de memòria**
    b. **Verificar la pròpia BIOS**
    c. **Verificar dispositius i busos del sistema**
    d. **Executar programes específics com el SCSI-BIOS, Video BIOS, etc.**
    e. **Donar la possibilitat d'accés al BIOS SETUP**
    f. **Assignar canals de DMA i IRQ (Interrupt Request)**
    g. **Detecció dels elements Plug&Play connectats**

[13] Firmware fa referencia a aquell component de hardware (en cas de la BIOS una memoria EEPROM) que conté un software propi (en aquest cas el SETUP) implementat en ell mateix.

4. **Trobar una unitat d'arrancada:** arribat a aquest punt, segons la seqüencia d'arrancada marcada pel SETUP BIOS, es busca que podem arrancar al nostre ordinador. Posem el cas de que ja tenim instal·lat algun/s sistema/s operatiu/s. S'accedeix a la unitat de disc designada com unitat d'arrancada i es busca el **MBR (Master Boot Record)** o alternativament el **GPT (GUID Partition Table)**, una versió que inclou millores de seguretat i permet la utilització de discos i/o particions de mida més gran.

5. **Carregar el Boot Manager:** al MBR/GPT trobarem segons el sistema o sistemes que tinguem instal·lats un programa, el Boot Manager, que ens permetrà escollir (si hi ha més d'un sistema operatiu disponible) quin agafarà el control del procés d'arrancada.

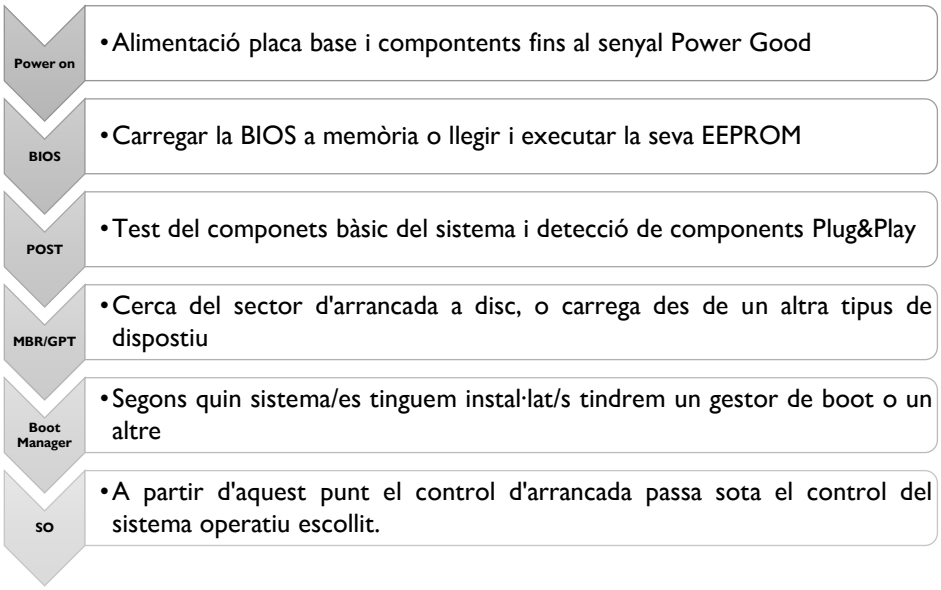


Figura 11 | Resum del procés d'arrancada previ al control del sistema operatiu

4.1. EL PROCÉS D'ARRANCADA ALS SISTEMES WINDOWS

Els sistemes operatius de la família de Microsoft Windows, com en totes les famílies de sistemes operatius, han anat evolucionant al llarg de la seva història, i els mètodes d'arrancada del sistema, no han estat una excepció. Així, els sistemes Windows han evolucionat de la lectura d'un simple fitxer de test pla on s'indicava quins sistemes operatius hi havia instal·lats a l'ordinador, quin s'havia d'arrancar i unes poques configuracions (el boot.ini amb Boot Manager NTLDR) i que executava 3 o 4 aplicacions del sistema; passant per un sistema basat en la consulta d'una base de dades (BSD amb Boot Manager BOOTMGR) que invocava crides més segures; fins a l'actualitat on s'ha anat millorant i ampliant els sistemes existents posant èmfasi en dos factors: la **velocitat** d'arrancada i la **seguretat** (incloent canvis en l'ús de la BIOS explicada anteriorment) durant aquest procés[14].

[14] NTLDR amb boot.ini fins a Windows XP, inclòs. BOOTMGR amb BSD a partir de Windows Vista.

Començarem parlant de les amenaces actuals que pateixen els equips informàtics, i veurem, que no podem estar segurs tant sols utilitzant un sistema de protecció de virus, un tallafocs o un detector d'aplicacions malicioses al nostre sistema, ja que, actualment tenim noves amenaces com els **rootkits** que poden iniciar un codi maliciós abans de que arranqui el sistema, ometent la seva seguretat, i quedant totalment ocults.

Els rootkits, són un tipus de software maliciós sofisticat i perillós que s'executa en mode kernel amb els mateixos privilegis que el sistema operatiu. Donat que els rootkits tenen els mateixos drets que el sistema operatiu i s'inicien abans, poden ocultar-se completament, tant a ells mateixos com a d'altres aplicacions. Sovint, els rootkits formen part d'un conjunt complert de malware que pot burlar els inicis de sessió locals, enregistrar les contrasenyes i pulsacions de tecles, transferir arxius privats i capturar dades criptogràfiques.

Diferents tipus de rootkits es poden carregar durant diferents fases del procés d'arrancada:

- **Rootkits de firmware:** sobreescriuen el firmware del sistema bàsic d'E/S de l'equip (BIOS) per poder iniciar-se abans que el sistema operatiu.
- **Bootkits:** reemplacen el carregador d'arrancada del sistema operatiu (Boot Manager) per què l'equip carregui el bootkit abans que el sistema operatiu.
- **Rootkits de kernel:** reemplacen una part del kernel del sistema operatiu per què el rootkit es pugui iniciar automàticament quan es carrega el sistema operatiu.
- **Rootkits de controlador:** es fan passar per un dels controladors de confiança que el sistema operatiu utilitza per comunicar-se amb el hardware de l'equip.

Totes aquestes amenaces han fet que Windows 10 implementés fins a 4 contramesures per evitar que es carreguin aquests rootkits durant l'arrancada del sistema: Figura | 12

1. **Arrancada segura:** si l'equip disposa d'un firmware UEFI (Unified Extensible Firmware Interface)[15] i un mòdul de plataforma segura TPM (Trusted Platform Module)[16], es poden configurar per què carreguin únicament els carregadors d'arrancada del sistema operatiu de confiança. Per a Windows 10 el certificat de Microsoft® es de confiança, tot i que si el mateix equip disposa d'altres sistemes operatiu d'altres famílies, poden utilitzar algun carregador diferent ja certificat per Microsoft (existeix ja un boot manager de codi obert per a sistemes Linux amb la certificació), o fins i tot, afegir manualment un certificat tot i que no estigui sota certificació de Microsoft.

2. **Arrancada de confiança:** Windows comprova la integritat de cada component del procés d'arrancada abans de carregar-lo. Primer es comprova la signatura digital de Windows 10, i és aquest qui després comprova si s'han modificat els arxius corresponents als controladors d'arrancada, als fitxers d'inici o el ELAM. Si torba algun problema no carrega aquell component, o en moltes ocasions, disposa de mecanismes per a la recuperació de la integritat i permetent un inici normal.

[15] UEFI reemplaça la antiga interfície BIOS, i és, des de Windows 8, l'únic firmware vàlid per aquests sistemes operatius.
[16] TPM és el nom d'una especificació publicada que detalla un criptoprocessador segur que pot emmagatzemar claus de xifrat per protegir la informació, entre d'altres mesures de seguretat física.

3. **ELAM (Early Launch AntiMalware):** és un controlador antimalware[17], de Microsfot o un altre, que proba totes les aplicacions i tots els controladors d'arrancada abans de que es carreguin i impedeix que es carreguin controladors no aprovats.

4. **Arrancada mesurada:** el firmware de l'equip registra el procés d'arrancada i Windows pot enviar-lo a un servidor de confiança (a través de l'ús de hash i claus) que pot avaluar objectivament l'estat de l'equip. Molts cops podem estar infectats per un rootkit (malware) i ni saber-ho per estar ocult. Això pot generar problemes de propagació del software maliciós dins una xarxa empresarial. Les organitzacions haurien de disposar d'un servidor d'atestació que fes aquest procés de comprovació i donés accés al client a tota la xarxa de la organització, o en cas de la detecció d'una amenaça, a una xarxa de quarantena limitada.

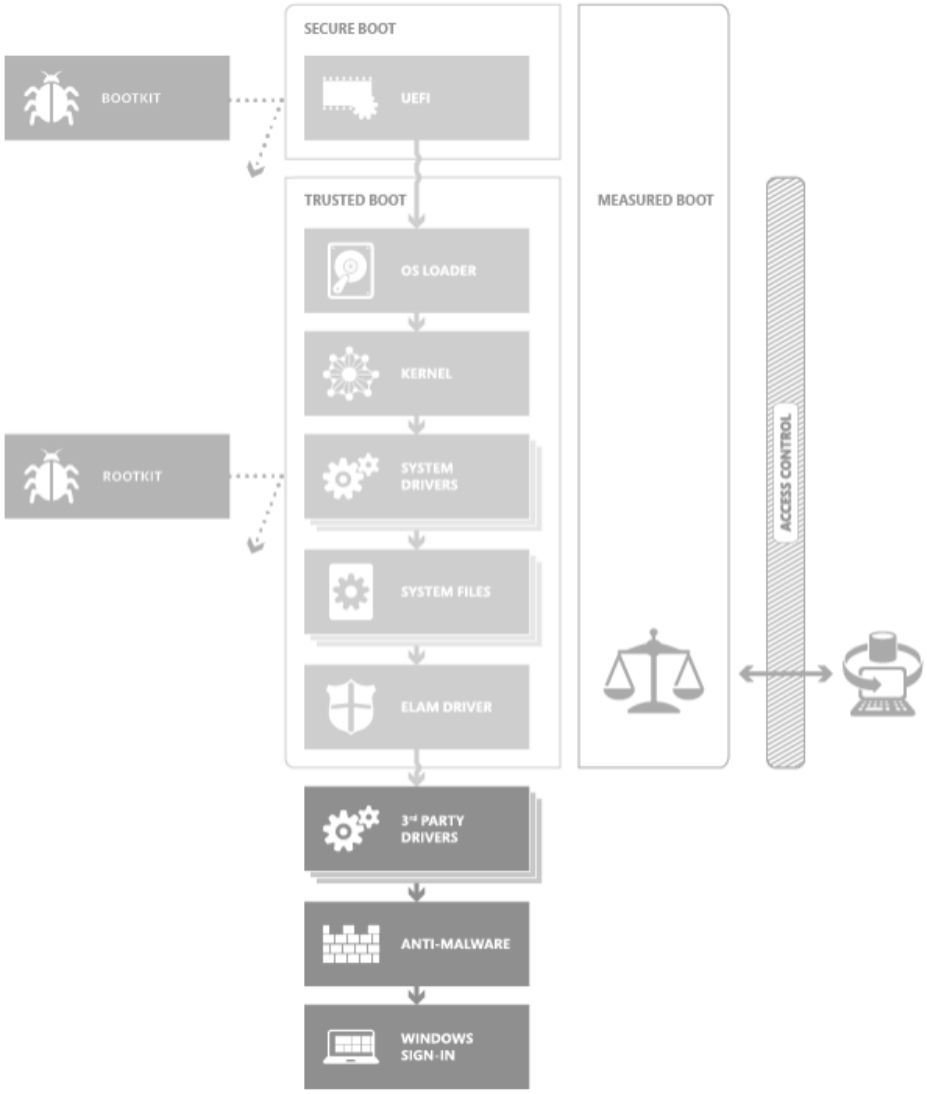


Figura 12 | Procés d'arrancada de Windows 10

[17] No es un software antimalware complert, i per tant, no és útil per fer aquesta tasca un cop iniciat el sistema operatiu.

ACT 8 | **Els firmware i els gestors de particions en l'arrancada del sistema**
Ja hem vist com fins i tot els sistemes encarregats de posar en marxa l'ordinador, fins i tot abans de la gestió per part del sistema operatiu, han evolucionat durant el temps. Respon a les següents qüestions:

a. Cerca informació i fes una comparativa sobre els firmware: BIOS i UFEI.
b. Cerca informació i fes una comparativa sobre els gestors de particions MBR i GPL.

4.2. EL PROCÉS D'ARRANCADA ALS SISTEMES UBUNTU

Tal i com passa a Windows, en la família de sistemes operatius Linux també ha existit una evolució dels seus gestors d'arrancada, i més, si tenim en compte la quantitat de distribucions de sistemes que hi ha basades en el nucli de Linux. En general podem parlar de 3 grans gestors d'arrancada: el GRUB (GNU GRand Unified Bootloader), el LILO (LInux LOader) i el Loadlin (Load Linux). D'aquests, els primer (GRUB) és el que encara avui s'utilitza més, tot i que ha evolucionat durant diferents versions i /o distribucions, i el LILO i el Loadlin (que permetia compatibilitats amb sistemes Windows antics), han caigut més en desús.

El procés d'arrancada a Ubuntu es pot estructurar en 4 fases de la següent manera: Figura | 13

1. **BIOS:** fa referència a tot el que ja hem vist des del moment que prenem el botó de **power** de l'equip, es carrega la **BIOS** i s'executa el testeig **POST**.

2. **GRUB:** el gestor d'arrancada es carrega i s'executa en 4 etapes:

   - **Etapa 1:** la primera etapa del carregador la llegeix la BIOS des del MBR (o GPT).
   - **Etapa 2:** la primera etapa carrega la resta del gestor d'arrancada[18].
   - **Etapa 3:** la segona etapa del gestor d'arrancada executa i mostra el menú d'inici de GRUB que permet al usuari escollir un sistema operatiu i examinar i modificar els paràmetres d'inici.
   - **Etapa 4:** després d'escollir un sistema operatiu, es carrega i aquest agafa el control.

3. **Kernel:** el primer pas d'aquesta etapa es **carregar en memòria** (funció startup) el codi del kernel (és carrega comprimit i després es descomprimeix). També es carreguen els drivers necessaris a traves del **initrd**, que també crea un sistema d'arxius temporals utilitzat al següent pas d'aquesta etapa, la **execució** del kernel. Després a és munta el sistema d'arxius definitiu (funció pivot_root()) i per últim es llença el procés **Init** (situat a /sbin/init) amb totes les funcions d'interrupcions ja carregades i la possible intervenció, per tant, del usuari.

[18] Si la segona etapa està en un dispositiu gran, es carrega una etapa intermèdia (anomenada etapa 1.5), que conté codi extra que permet llegar cilindres majors que 1024 o dispositius de tipus LBA.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

4. **El procés Init:** la seva funció es "aconseguir que tot funcioni com ha de funcionar" un cop el kernel s'ha posat en marxa. Bàsicament estableix i opera tot l'espai d'usuari: la comprovació i muntatge del sistema d'arxius, la posada en marxa de serveis d'usuari necessaris i, finalment, canviar l'entorn d'usuari quan l'inici del sistema s'ha completat. Init s'executa sota un paràmetre anomenat **nivell d'execució** (runlevel) amb un valor d'entre 1 i 6 que determina quins subsistemes poden ser operacionals. Cada nivell te els seus propis scripts[19] que codifiquen els diferents processos involucrats en la creació o sortida del nivell d'execució concret i que possibiliten el procés d'arrancada. Aquest procés (Init) és pot configurar a l'arxiu /etc/inittab.

Figura 13 | Procés d'arrancada de Ubuntu 18.04

ACT 9 | **Els nivells d'execució**

L'últim pas en el procés d'arrancada d'Ubuntu es variable segons el nivell de privilegis que es posa en marxa a través del procés INIT. Aquest tindrà un RUN LEVEL per defecte, tot i que també pot deixar a elecció de l'usuari sobre quin nivell iniciar la màquina. En tot cas, aquest nivell d'execució marcarà quins scripts s'executaran abans d'iniciar la sessió. Contesta les següents preguntes al voltant d'aquest tema:

a. Existeixen 7 nivell d'execució (del 0 al 6), quins són aquests nivells?
b. Cada nivell d'execució te una sèrie de enllaços a scripts de la carpeta /etc/init.d. Aquests enllaços els trobarem a les carpetes /etc/rd0.d, /etc/rd1.d, ... , /etc/rd6.d, segons el RUN LEVEL. Els noms dels enllaços tenen una nomenclatura concreta; quina és aquesta nomenclatura? (per exemple, si ens torbem un enllaç anomenat S01apache que significaria?)
c. Si en algun moment un usuari d'Ubuntu vol conèixer sota quin RUN LEVEL està treballant, amb quina/es comanda/es ho podria esbrinar?

4.3. EL REGISTRE DEL SISTEMA

Cada sistema operatiu té formes variades d'emmagatzemar la configuració dels components de baix nivell del sistema operatiu, així com de les aplicacions instal·lades en ell. Hi ha sistemes, com el cas dels de la família Windows, que ho fan de manera centralitzada, a través d'una base de dades, i d'altres, com el cas dels basats en Linux, que ho fan a través d'una estructura de directoris estàndard on es guarden els diferents fitxers de configuració agrupats segons el seu propòsit.

[19] Els scripts son arxius de processament per lots, és a dir, arxius que permeten executar un codi amb un seguit d'ordres programades.

Per tant, sigui un punt centralitzat, o sigui de manera distribuïda, les bases de dades i/o els fitxers de registre són útils pel propi nucli del sistema operatiu, els controladors de dispositius, els serveis, la interfície d'usuari i les aplicacions de tercers.

En **Windows** el registre del sistema és del tipus **base de dades jeràrquica** que s'emmagatzema en un únic punt, i que proporciona una interfície operativa molt útil per guardar i/o consultar les configuracions d'usuari, les rutes d'arxius o carpetes, els drivers utilitzats pel hardware, els ajustos bàsics del sistema operatiu, les aplicacions instal·lades (i les seves configuracions), quins tipus d'arxiu es poden crear i quin programa obre cada tipus.

A aquesta interfície s'accedeix a través de l'execució de l'ordre **REGEDIT.EXE**, i conté dos elements bàsics: **claus** i **valors**.

Les **claus del registre** son similars a carpetes i poden contenir, valors, o altres subclaus que al mateix temps poden contenir altres subclaus i així successivament. Per tant, es poden referenciar les claus amb rutes semblants a les rutes jeràrquiques de Windows (utilitzant barres diagonals inverses). Per exemple, la clau HKEY_LOCAL_MACHINE\Software\Microsoft\Windows fa referència a la subclau "Windows" de la subclau "Microsoft" de la subclau "Software" de la clau arrel HKEY_LOCAL_MACHINE. Hi ha 7 claus arrel al registre:

1. **HKEY_LOCAL_MACHINE** o HKLM: conté configuracions de l'equip local.
2. **HKEY_CURRENT_CONFIG** o HKCC : conté la informació sobre el perfil de hardware del sistema al iniciar sessió i es va creant i configurant de manera constant i dinàmica segons els requeriments del sistema i les aplicacions en cada moment.
3. **HKEY_CLASSES_ROOT** o HKCR: conté configuracions de les aplicacions instal·lades.
4. **HKEY_CURRENT_USER** o HKCU: conté la configuracions del usuari que te iniciada la sessió en aquells moments (és un enllaç a una part concreta de la següent rama)
5. **HKEY_USERS** o HKU: conté les configuracions dels usuaris que han iniciat sessió al sistema activament en algun moment.
6. **HKEY_PERFORMANCE_DATA**: només en les versions de Windows basades en NT, però invisible per l'editor del registre, proporciona informació sobre les dades de rendiment visibles a través d'aplicacions del sistema (monitor de rendiment, administrador de tasques, etc.)
7. **HKEY_DYN_DATA**: desfasada (només en Windows 9x/Me) proporcionava informació sobre el hardware del sistema.

Els **valors del registre** son parells de nom (que és únic) i dades, i estan emmagatzemats dins les claus. Els valors es referencien per separat de les claus, és a dir, quan Windows utilitza en alguna de les seves API un valor, ho fa a través del nom únic independent de la clau que el contingui. Les dades dels valors son de mida i codificació variable però associats a un tipus simbòlic de dades definit com una constant numèrica[20].

No és recomanable editar manualment les claus i/o els valors del registre, a no ser que sigui necessari, i és molt recomanable exportar una copia de seguretat del registre abans de la seva edició. A més, existeixen comandes especifiques (en forma de scripts) per editar els arxius .reg de manera més controlada.

[20] Pots consultar més informació sobre les dades dels valors a https://docs.microsoft.com/es-es/windows/desktop/SysInfo/registry-value-types.

ACT 10 | **El registre de Windows**

Anem a veure un cas pràctic on podríem entrar a editar el registre de Windows manualment. Imagina que un virus infecta el teu ordinador i tot i que saps que pot estar emmagatzemat en una carpeta concreta, al entrar no aconsegueixes veure l'arxiu de virus per eliminar-lo. Penses que potser està ocult:

a. Com pots mostrar els arxius ocults d'una carpeta?

Imagina que el virus ha eliminat aquesta opció a les opcions de carpeta de Windows. Cal afegir-la de nou al registre:

b. Primer de tot, com es fa una exportació d'una copia del registre?
c. Quina clau i amb quin valor hauríem de crear per tornar a veure l'opció per mostrar els arxius ocults?

Un altre cas, podria ser que el virus, no hagués eliminat l'opció de les opcions de carpeta però si que l'hagués deixat inservible. En aquest cas:

d. Quina clau i amb quin valor hauríem de configurar?

A diferència del model de base de dades binaries del registre de Windows, els sistemes operatius de Linux, utilitzen **arxius separats de text sense format** per al procés daemon[21] i la configuració de les aplicacions, tot i que s'agrupen per facilitar la seva administració.

Els sistemes Linux segueixen una **jerarquia estàndard** (Figura | 14) en el sistema d'arxius. Dins d'aquesta jerarquia podem trobar els arxius de configuració de tot el sistema (una informació similar a la que apareixia en HKEY_LOCAL_MACHINE de Windows) i que s'emmagatzemen en el directori /etc i els seus subdirectoris, o fins i tot, alguns cops, en /usr/local/etc. Un altre exemple seria la informació per usuari (el que seria aproximadament el HKEY_USERS / HKEY_CURRENT_USER), s'emmagatzemen en directoris i arxius ocults dins del directori d'inici (Home Directory) de cada usuari.

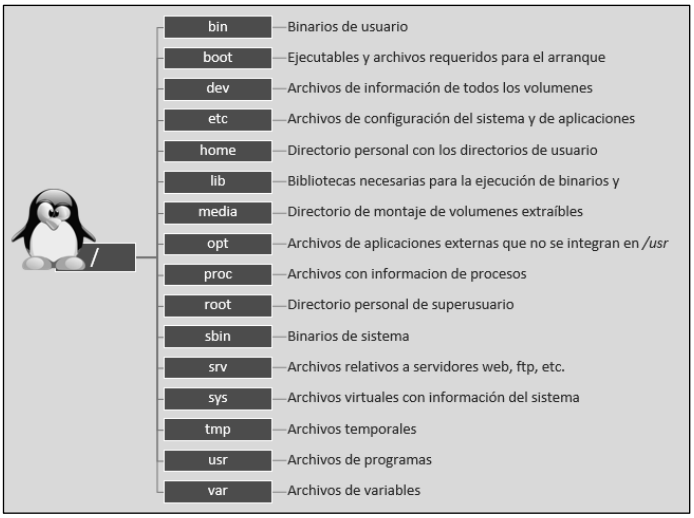


Figura 14 | Estructura de directoris als sistemes Linux

[21] Un daemon (Disk ANd Execution MONitor), es un servei o programa resident, i es un procés especial, o interactiu, i que s'executa de manera persistent en segon pla.

5. IDENTIFICACIÓ I MANTENIMENT DELS CONTROLADORS DE DISPOSITIUS

Com ja hem vist, una de les funcions bàsiques de qualsevol sistema operatiu és la de fer de intermediari entre les aplicacions (software) i el maquinari (hardware) a través del diferents controladors de dispositiu (drivers), que han de ser específics per aquell sistema operatiu concret.

A més, el sistema operatiu, haurà d'aportar mètodes per conèixer, actualitzar i/o modificar els controladors dels dispositius connectats, a més, de poder afegir nous en cas necessari.

5.1. ADMINISTRACIÓ DE DISPOSITIUS EN WINDOWS

Windows 10 permet una configuració ràpida d'alguns dels dispositius connectats al sistema a través del menú de Configuració a la pestanya Dispositius. Aquí podrem, per exemple, cercar i connectar dispositius Bluetooth, establir el funcionament del teclat o ratolí, accedir a impressores o establir termes per la reproducció automàtica al introduir un USB o un dispositiu òptic.

Totes aquestes configuracions, però, no estan relacionades amb els propis controladors d'aquests o altres dispositius. Per poder accedir al control d'aquests controladors cal accedir a la consola **Administració de dispositius**, a través del botó dret al menú inici o amb la comanda **devmgmt.msc** (entre altres accessos directes que podem trobar pel sistema).

Un cop hem accedit veurem un llista dels dispositius connectats, així com alguna "alerta" (marca) en aquells que potser no funcionen correctament. Si no apareix un dispositiu nou, que acabem de connectar, podem provar el botó de "Buscar canvis de hardware", que a més, podrà cercar actualitzacions per a controladors antics.

Els dispositius els trobarem agrupats per tipus, i en desplegar cada "família" de dispositius veurem els controladors instal·lats. Fent botó dret sobre qualsevol d'ells podrem:

- **Actualitzar el controlador**: busca canvis automàticament, o permet la configuració manual del controlador buscant-lo a la ruta on el tinguem localitzat.
- **Deshabilitar dispositiu**: permet d'una manera temporal, fer que un dispositiu no funcioni, estigui "apagat".
- **Desintal·lar el dispositiu**: treu el controlador per aquell dispositiu de manera permanent.
- **Propietats**: accedir a tota la informació del dispositiu, el controlador específic i la seva versió, els canvis (actualitzacions) que ha sofert al llarg del temps, etc.

A més a més, podem trobar més informació sobre el hardware del nostre dispositiu buscant **Informació del sistema** o executant **msinfo32**. Accedirem a una consola amb informació en 4 apartats:

- Resum del sistema
- Recursos de hardware
- Components
- Entorn de software

ACT 11 | **Llitar els dispositius de hardware a Windows**
Hem vist dos consoles en les que podem veure i/o administrar els nostres dispositius en l'entorn de Windows: Administració de dispositius i Informació del sistema. També podem cercar aquest tipus d'informació a través de comandes del CMD.

a. Utilitza les opcions necessàries de la comanda DRIVERQUERY per obtenir una llista amb informació detallada dels dispositius.
b. Utilitza la comanda SYSTEMINFO i obté informació sobre la memòria física i virtual del sistema.
c. Per últim, utilitzant la comanda DISM, prova de realitzar una copia de seguretat dels teus drivers.

5.2. ADMINISTRACIÓ DE DISPOSITIUS EN UBUNTU

Ubuntu també incorpora mecanismes per a la configuració ràpida d'alguns dispositius de hardware a través del que denomina "Centre de Control", tot i que, com en el cas de Windows, aquestes configuracions son més sobre el ús dels dispositius que sobre els seus controladors (drivers).

Per conèixer el hardware a nivells de quins son els controladors instal·lats i el seu estat podem trobar diferents eines gràfiques de entre les més comuns tenim:

- **SYSINFO**
- **HARDINFO**
- **HARDWAREMAP**

Aquestes eines ens permetran consultar i/o modificar/actualitzar els controladors dels dispositius que tenim instal·lats al sistema.

Com es habitual a Ubuntu, la utilització de la línia de comandes serà habitual i podrem trobar una bona quantitat de comandes per obtenir informació referent al hardware i els seus controladors. En general l'eina més complerta és **lshw** que dona una informació completa sobre aquests aspectes.

Després podrem utilitzar diferents comandes per veure components de hardware específics com poden ser:

- **lscpu**: donarà informació detallada del processador.
- **wmstat**: informació en temps real sobre la memòria principal.
- **lspci**: informació sobre els dispositius PCI connectats al sistema, per exemple, la targeta gràfica.
- **lsusb**: informació sobre tots els dispositius connectats al sistema a través d'un port USB.

Per últim, cal recordar que la estructura jeràrquica de directoris de Linux disposa d'un directori concret on es tots els dispositius del sistema anomenat **/dev** (Figura | 14). Aquest directori conté un arxius especials anomenats **arxius de dispositius** i que tenen una nomenclatura especial. Es creen durant la instal·lació del sistema, i també, es poden crear amb un parell de scripts: /dev/MAKEDEV (dispositius estàndards) i /dev/MAKEDEV.local (personalitzat per l'administrador per dispositius no estàndards)[22].

[22] Podeu veure alguns directoris típics del directori /dev aquí.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

ACT 12 | **Llitar els dispositius de hardware a Ubuntu**
Ja hem vist que tenim diverses eines gràfiques i diverses comandes per poder examinar el hardware del nostre equip en Ubuntu. Escriu la comanda lshw al terminal del teu equip. Com veuràs surt una informació que és molt extensa i complerta, però potser una mica farragosa de llegir. Anem a intentar veure aquesta informació a través del navegador web. Per fer-ho utilitza la comanda lshw -html per crear un fitxer que contingui la informació relativa al hardware del teu equip visible des del teu navegador.

Per últim, comprova si el teu sistema te instal·lada alguna de les 3 eines gràfiques per la gestió del hardware que hem anomenat en aquest apartat. Si és així, quina? Sinó instal·la una de les 3. Quines funcionalitats t'ofereix? Et semblea més o menys útil que la comanda lshw?

6. PROGRAMARI INSTAL·LAT AL SISTEMA I INSTAL·LACIÓ DE NOVES APLICACIONS

Tot i que el sistema porta incorporades algunes aplicacions pròpies que s'instal·len durant el propi procés d'instal·lació del sistema, o que fins i tot incorporin aplicacions de tercers en el procés d'instal·lació, no és habitual trobar equips que no tinguin una sèrie de programari instal·lat per dur a terme multitud de tasques específiques. A més a més, alguns dels controladors de dispositius (drivers) dels que parlàvem a l'apartat anterior, també s'hauran d'instal·lar com si d'una aplicació més es tractés.

En aquest apartat veurem com podem consultar, actualitzar i/o eliminar el software que tenim al nostre equip així com mètodes per afegir nous programes al nostre sistema operatiu.

6.1. SOFTWARE ALS SISTEMES WINDOWS

El primer que hem de saber és com podríem aconseguir una llista del programari que tenim instal·lat al nostre sistema. La manera gràfica és des del menú **Configuració** a l'apartat **Aplicacions**. Aquí trobarem una llista de programes instal·lats, que a més, ens permetrà fàcilment modificar una instal·lació o desintal·lar un programa si així ho desitgem. A més, trobarem altres opcions com quines aplicacions estan predeterminades per dur a terme algunes tasques (reproductor de vídeo, navegador web, etc.) o quines estan ancorades al menú d'inici.

Hi ha altres mètodes menys usuals a Windows a través de la línia de comandes (CMD o PowerShell), que ens permetran, obtenir ràpidament un fitxer amb tot el programari instal·lat (ACT 13).

Un cop sabem com localitzar software al nostre equip Windows, veiem com podem instal·lar nous programes i/o aplicacions. La majoria d'aplicacions per a Windwos porten un **Install** o **Setup** que ens permet realitzar directament la instal·lació, o simplement son un executable (**.exe**) que realitza aquesta tasca.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Igualment, un cop instal·lades incorporen un **Unistall** per eliminar-les. Per tant és un procés directe, que com a molt, ens requerirà descomprimir el paquet de software abans de poder instal·lar-lo (cosa senzilla ja que el propi sistema operatiu incorpora un compressor/descompressor **ZIP**).

ACT 13 | **Instal·lar i llistar el software a Windows**
Anem a instal·lar en un equip Windows 10 el reproductor d'àudio/vídeo VLC:

a. Ves a la pàgina oficial de VLC i descarrega la versió apropiada pel teu sistema operatiu.
b. Executa l'instal·lador. Requereix algun permís o confirmació? Realitza la instal·lació.
c. Anem a buscar el nou software instal·lat:
   - De forma gràfica (fes al mateix temps que sigui el teu reproductor de vídeo per defecte)
   - A través de la línia de comandes. Executa al CMD (com administrador) la següent comanda: `wmic /output:C:\LlistaSoftwareCMD.txt product get name,version`
   - A través del PowerShell (també com adminsitrador): `Get-WmiObject -Class Win32_Product | Select-Object -Property Name > c:\LlistaSoftwarePS.txt`
   - Busca el reproductor VLC a les 2 llistes i compara el format en que mostra la informació.
   - Per últim, anem a consultar el registre de Windows. Accedeix i busca el programa VLC. Després executa la següent comanda (com administrador) al PowerShell que farà la consulta de tot el software instal·lat a través del registre: `Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize`

6.1. SOFTWARE ALS SISTEMES UBUNTU

A Ubuntu tenim moltes més possibilitats, i complicacions, a l'hora d'instal·lar paquets de programes i/o aplicacions. De fet, tenim que fer una primera elecció inicial sobre si instal·lar el software a partir d'un paquet **binari** o un paquet de **codi font**.

Els paquets binaris ja han estat compilats (traduïts per tal de que el hardware pugui entendre el codi d'alt nivell del programa), i es podran instal·lar directament a la màquina (si aquesta té una arquitectura que suporti aquella compilació). En canvi els paquets de codi font, no estan compilats i per tant requeriran de l'ús d'un compilador abans de poder ser instal·lats al nostre sistema, i per tant, ens donaran més feina en la instal·lació.

Per treballar amb paquets binaris hem d'escollir un **gestor de paquets**. En Ubuntu treballem amb paquets compilats amb extensió **.deb**[23], que tenen com a gestor de paquets **dpkg**. Aquest gestor ens permetrà consultar paquets instal·lats (dpkg -L), instal·lar nous paquets (dpkg -i nompaquet), desintal·lar paquets (dpkg -r nompaquet), entre moltes altres opcions[24] (depenent si volem instal·lar o no dependències, si volem eliminar els paquets d'instal·lació quan desinstal·lem un programa, volem veure el estat d'algun paquet, etc.).

[23] Ubuntu és una distribució de Linux basada en Debian i d'aquí que utilitzi aquest tipus de paquets. Altres distribucions utilitzen altres tipus de paquets (per exemple, .rpm). També podrem instal·lar-los un cop que els "transformem" a .deb a través de la comanda **alien**.
[24] Consulta el manual complert del gestor dpkg aquí.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Molts cops, però, utilitzar dpkg es torna força complicat i utilitzarem altres gestors amb entorns més amigables, tot i que, no hem d'oblidar que cadascun d'aquests serà només **font-end** que utilitza el gestor base (dpkg) per darrera. Aquests seràn executables a través de la línia de comandes o per interfície gràfica:

- **Interfície gràfica**: Ubuntu incorpora per defecte el **Centre de Software** que ens ofereix una imatge de moltes aplicacions catalogades per tipus i puntuades per la seva popularitat. Buscar una aplicació, fer clic i instal·lar-la serà molt fàcil. De vegades, volem una mica més de control (tot i que fem servir la interfície gràfica) i volem, per exemple, conèixer quines **dependències** té un paquet de software concret abans d'instal·lar-les juntament amb la aplicació. Per mode gràfic disposem del gestor de paquets **Synaptic** que ens ofereix una interfície gràfica amb més informació, i control (fins i tot un cop escollim un paquet a instal·lar podem veure el rerefons que s'executa a la línia de comandes mentre s'instal·la un programa, i les seves dependències, si les té).

- **Línia de comandes:** tenim un parell d'opcions populars per descarregar i instal·lar paquets des dels **repositoris oficials** d'Ubuntu:
  - La primera és **apt** (Avanced Packaging Tool) que permet opcions fàcils com **install** o **remove** (afegint --purge eliminarà també els arxius d'instal·lació). Durant el procés d'instal·lació ens informarà dels paquets que es descarregaran i copiaran, així com les dependències que té, i la mida de la descarrega i ens demanarà confirmació per fer-ho. A més, permet actualitzar la llista de paquets disponibles als repositoris (**apt update**), o actualitzar tots els paquets que tenim instal·lats si hi ha noves versions als repositoris (**apt upgrade**).
  - La segona és **aptitude** (basat en apt) que obre un entorn a la línia de comandes on podem trobar llistats els paquets del nostre sistema classificats (instal·lats, només descarregats, etc.). A més, disposa d'un cercador per localitzar els paquets ràpidament, ja sigui per instal·lar un de nou (opció i) o per desintal·lar un existent (opció r). També accepta les opcions update i upgrade (equivalents a apt).

De vegades, volem instal·lar algun programa que no es troba en aquestes llistes de paquets dels repositoris oficials, amb la qual cosa ens caldrà descarregar-los via web (de la pàgina dels programadors) i després instal·lar-los, o obtenir-los a través de la línia de comandes[25].

A més, molts d'aquests paquets descarregats estan en formats diferents al .deb, com per exemple, els paquets **.bin**, els paquets **.sh** o els paquets **.run**. Per fer-ho normalment cal atorgar permisos al paquet (sudo chmod +x paquet.bin/sh/run) i després executar-los des de la ruta on estigui (sudo ./paquet.bin/sh, o sudo sh ./paquet.run).

Finalment, també és habitual (sobretot en el cas del paquets de codi font, per la seva mida i quantitat de fitxers), que aquests els descarreguem **empaquetats** (fitxers agrupats) i/o **comprimits** (mida reduïda) en diferents formats, i per tant, caldrà primer desempaquetar-los i/o descomprimir-los. Per exemple, si descarreguem un paquet amb extensió tar.gz (o tar.bz2) caldrà executar: tar-xzvf nomarxiu.tar.gz(o bz2).

[25] En aquest cas primer cal afegir el repositori "no oficial" a la nostra llista de repositoris (que es troba al fitxer /etc/sources.list): sudo add-apt-repository ppa:nomrepositori. Després actualitzar els paquets disponibles (sudo apt update) i per últim instal·lar el paquet (sudo apt install nompaquet).

ACT 14 | **Instal·lar un paquet de codi font en Ubuntu**

Hem vist mètodes per gestionar paquets binaris (que ja estan compilats). Ens queda però aprendre a instal·lar paquets dels que tenim el codi font, i per tant, que cal compilar abans d'aconseguir el script que ens permeti llançar la instal·lació del paquet al nostre sistema operatiu. Aprendrem els **3 passos claus** a través de la instal·lació de l'aplicació de DropBox a través del seu codi font al nostre equip Ubuntu:

a. Accedeix a la pàgina de descarregues de paquets de DropBox (https://linux.dropbox.com/packages/) i descarrega la última versió (de codi font, començarà per nautilus...) disponible.
b. Accedeix a la ruta on s'ha descarregat el paquet i desempaqueta'l i descomprimeix-lo.
c. Accedeix al nou directori creat i executa **./configure** per configurar el paquet. Et fan falta dependències? Descarrega-les i instal·la-les amb l'ajuda de apt.
d. Quan el ./configure no doni errors de configuració, has de compilar el paquet executant la comanda **make**.
e. Per últim, veuràs que s'ha un fitxer install, per executar-lo fes **sudo make install**.
f. Arranquem Dropbox i ens sortirà un missatge informant de que es descarregarà el deamon de l'aplicació i s'instal·larà al equip.

ANEX 1 | MÀQUINES VIRTUALS

Durant el curs no treballarem sobre la màquina real per realitzar les diferents instal·lacions i configuracions dels sistemes operatius sinó que ho farem a través de la **virtualització** d'aquests sistemes cosa que ens permetrà simular diferents sistemes operatius sobre el nostre sistema operatiu "real" sense perill de deixar la màquina física inutilitzable.

Per dur a terme aquesta tasca utilitzarem el software de virtualització **Oracle VM VirtualBox**[26] sota llicència PUEL (Personal Use and Evaluation License) que ens permetrà crear i modificar quantes màquines virtuals desitgem dins del nostre entorn acadèmic.

Anem, abans de tot, a fer una petita introducció teòrica sobre els conceptes claus de la virtualització:

Molts cops no utilitzem el 100% dels recursos de hardware (CPU, Memòria, etc.) que ens ofereix el nostre ordinador. Per tant, podem aprofitar aquests recursos per **virtualitzar** aquests elements de hardware i simular un nou maquinari específic, o **maquinari virtual**, per a un nou sistema operatiu. Per tant, la virtualització consisteix en l'abstracció dels recursos de la màquina per poder utilitzar els que "sobren" i crear **màquines virtuals** utilitzant aquest hardware. Això ho podem aconseguir creant una capa d'abstracció entre el hardware físic (o host) i el sistema de la màquina virtual (guest).

Tenim dos grans tècniques per implementar màquines virtuals (Figura | 15):

- Execució **nativa** o **unhosted**: si tenim de base un software de virtualització directament sobre el hardware. No li cal un sistema operatiu amfitrió (o host). Per exemple: Vmware Server ESXi, Xen o Micorsoft Hyper-V Server.
- Execució **no nativa** o **hosted**: el programari de virtualització s'instal·la com una aplicació més al nostre sistema operatiu (sistema operatiu amfitrió o host). Aquest és el mètode utilitzat per VirtualBox i, per tant, serà el nostre cas d'ús. Altres exemples serien: VMware Workstation o Microsoft Virtual PC.

Figura 15 | A l'esquerra el model natiu o unhosted i a la dreta el model no natiu o hosted

[26] Pàgina oficial de Oracle VM VirtualBox: https://www.virtualbox.org/

Per últim veurem un seguit d'avantatges i desavantatges de la virtualització:

- **Avantatges**: permet l'**aïllament** d'aplicacions/serveis i usuaris sobre la mateixa màquina perquè no interfereixin entre si. És per tant, un entorn ideal per fer **proves i/o avaluacions** de sistemes operatius i/o aplicacions. Ens facilita l'**optimització de la infraestructura** aprofitant més el hardware existent ja que un mateix equip servidor pot fer córrer diferents màquines estalviant en costos de hardware, consum, etc. A més, proporciona **millores operacionals** ja que ofereix noves formes de gestionar la infraestructura i permet guanyar temps als administrador en tasques d'aprovisionament, configuració, monitorització i administració. Per últim, cal destacar que facilita la **alta disponibilitat** ja que proporciona eines de recuperació ràpida davant de caigudes del sistema, per l'actualització del hardware o la gestió del balanceig de càrrega de treball.

- **Desavantatges**: una errada de hardware pot perjudicar a més sistemes a la vegada, cal invertir en formació i software de virtualització, pot suposar problemes de rendiment si les màquines no estan ven dimensionades, necessita d'espai i ample de banda gran per la realització de copies de seguretat de (moltes) màquines virtuals complertes.

D'aquests desavantatges deduirem els **passos preliminars** a tenir en compte a l'hora de crear màquines virtuals al nostre sistema operatiu, ja que molts els podem mitigar (o reduir) amb una bona planificació prèvia de les nostres instal·lacions:

1. Requisits mínims del sistema operatiu convidat (o guest) tenint en compte futures aplicacions que tindrà instal·lades.
2. Quins tipus d'adaptadors de xarxa utilitzarem i amb quina finalitat (Internet, visió entre màquines locals, crear una xarxa LAN privada, etc.)
3. Espai disponible en el meu disc dur real i memòria RAM física lliure i ocupada.
4. Serveis instal·lats i iniciats (per controlar possibles incoherències o contradiccions).
5. Compatibilitat dels softwares (amfitrió, convidats, programari de virtualització, etc.).

Com transportar les nostres MV i treballar amb elles des de diferents ordinadors?

Més d'un cop haurem de portar-nos feina a casa per acabar i/o revisar les pràctiques que fem a classe. Sempre guardarem les nostres màquines virtuals al nostre disc dur portable. Tot i així, en arribar a casa tindrem que seguir una sèrie de passos per treballar amb elles amb garanties, ja que, segurament, no tindrem exactament el mateix hardware al ordinador de casa que al institiut.

Per tant, sempre que arribem a casa, exportarem cap al nostre disc dur local (de l'ordinador de casa) la/les màquina/es virtual/s amb les que anem a treballar en format **.ova**. Des d'aquest format farem una importació des de VirtualBox (que procurarem sigui la mateixa versió de l'instal·lat al institut), amb la qual cosa la màquina virtual "recompilarà" el seu maquinari virtual per adaptar-lo al del teu ordinador de casa. Un cop haguem treballat amb la/les màquina/es virtual/s, podrem sobreescriure el nostre disc dur portable amb la/les nova/es màquina/es virtual/s. De tornada al treball en l'institut procedirem de igual manera però inversament, és a dir, exportar una (o varies) ova al nostre disc dur portable, importar aquestes màquines des del nostre VirtualBox del institut i treballar amb elles un cop s'ha "recompilat el hardware".

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

PT 1 | INSTAL·LACIÓ DE SISTEMES OPERATIUS

En finalitzar aquesta pràctica coneixerem el procés d'instal·lació de diferents sistemes operatius sobre màquines virtuals pròpies.

OBJECTIUS

- Estudiar els requisits previs per la instal·lació de diferents sistemes operatius (clients i servidors).
- Crear màquines virtuals seguint els requisits d'instal·lació.
- Instal·lar quatre sistemes operatius:
  - Windows 10 Enterprise Edition
  - Ubuntu Desktop 18.04 LTS
  - Windows Server 2016 Datacenter
  - Ubuntu Server 18.04 LTS
- Buscar, analitzar i interpretar la documentació tècnica necessària.
- Realitzar manuals tècnics dels procediments realitzats.

Requisits mínims i recomanables per la instal·lació de diferents sistemes operatius

Busca informació i omple la següent taula amb els requisits mínims i recomanables per instal·lar els nostres sistemes operatius en màquines virtuals:

	Windows 10 Enterprise Edition		**Ubuntu Desktop 18.04 LTS**		**Windows Server 2016 Datacenter (amb GUI)**		**Ubuntu Server 18.04 LTS (sense GUI)**	
	Min.	Rec.	Min.	Rec.	Min.	Rec.	Min.	Rec.
Processador								
Memòria								
Espai de disc dur								
Altres								

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Creació de màquines virtuals

Abans de virtualitzar em de conèixer la nostra màquina i sistema operatiu amfitrió. Respon:

- Quin sistema operatiu i en quina versió tenim instal·lat al nostre equip? És un sistema de 32 o 64 bits?
- Tenim instal·lat Oracle VM VirtualBox? En quina versió?
- Quin processador, memòria RAM tenim disponibles? Quina capacitat té el teu disc dur portable?
- La nostra BIOS permet la virtualització del processador per sistemes de 64 bits? Comprova-ho buscant informació del processador i/o accedint a la BIOS i buscant opcions VT-x (en cas de processador Intel) o AMD-v (en cas de processador AMD).

Ara ja tenim tota la informació necessària, tant de la nostra màquina física, com dels sistemes operatius que volem virtualitzar sobre de ella. Obre Oracle VM VirtualBox i crea una nova màquina virtual tenint en compte totes les especificacions anteriors i que s'haurà de guardar al teu disc dur portable (no cal afegir molt més disc dur del que requereixi el sistema, més tard si cal afegirem unitats de disc dur complementaries, a més, fes que aquest espai és reservi dinàmicament per anar més ràpids en la creació). Aquesta màquina servirà, més tard, per fer la instal·lació de Windows 10 Enterprise Editon, i s'haurà d'anomenar **VM_w10**.

Després repeteix el procés per crear una màquina anomenada **VM_ud1804** (per Ubuntu Desktop 18.04 LTS). Torna a fer-ho per una tercera màquina anomenada **VM_w2016** (per a Windows Server 2016 Datacenter). Per acabar, repeteix el procés per crear la màquina **VM_us1804** (per a Ubuntu Server 18.04 LTS).

- Quins passos has tingut que seguir dins del programa VirtualBox per crear aquestes quatre màquines virtuals?

Instal·lació de sistemes operatius

Ara ja tenim el nostre escenari virtual creat i podrem instal·lar els diferents sistemes operatius. Abans, però, ens cal un últim pas previ, descarregar les ISO (imatges de CD/DVD) dels sistemes operatius a instal·lar.

Descarrega-les tenint en compte que:

- Amb el cas d'Ubuntu no tindrem cap problema, ja que en ser un software lliure i gratuït, el podrem descarregar directament des de la seva web (http://releases.ubuntu.com/18.04/).
- Amb Windows podreu descarregar unes versions de "prova" des del nostre servidor local.

Ara només cal introduir aquestes imatges dins del nostre lector de CD/DVD virtual en cadascuna de les màquines virtuals. Explica com ho fas?

Ja podem posar en marxa la nostra primera màquina virtual (VM_w10). Has de documentar pas a pas tot el procés d'instal·lació tenint en compte que l'usuari inicial que hauràs de crear tindrà com a login nomXX (amb nom el teu nom i XX el teu número d'alumne) i la màquina s'anomenarà wclientXX. També utilitzarem tot el disc dur per fer la instal·lació. Davant de qualsevol dubte de configuració pregunta al professor.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Haurem de repetir el procés d'instal·lació i documentació per a les altres tres màquines, sempre tenint en compte el nom d'usuari inicial, i recordant que en el cas de VM_w2016 hem d'instal·lar el sistema amb GUI i en el cas de MV_us1804 sense entorn gràfic i afegint només les opcions bàsiques de servidor, sense cap altre servei addicional. Recorda preguntar al professor davant de qualsevol dubte de configuració.

Un cop realitzades les instal·lacions i manuals corresponents respon:

- Tens connexió a Internet en cadascuna de les quatre màquines virtuals? Per què? En cas de no tenir connexió, quines modificacions et calen?
- Quines diferencies trobes entre el procés d'instal·lació de Windows 10 Enterprise Edition i de Windows 2016 Datacenter? I entre les versions Desktop i Server de Ubuntu 18.04?

RESULTATS

Arribat el final de la pràctica l'alumnat haurà de tenir al seu disc dur el següent escenari de màquines virtuals:

- **VM_w10:** màquina virtual de Windows 10 Enterprise Edition amb el sistema instal·lat, amb connexió de xarxa i usuari nomXX com usuari amb privilegis de la màquina anomenada wclientXX.
- **VM_ud1804:** màquina virtual de Ubuntu Desktop 18.04 LTS amb el sistema instal·lat, amb connexió de xarxa i usuari nomXX com usuari amb privilegis de la màquina anomenada uclientXX.
- **VM_w2016:** màquina virtual de Windows Server 2016 Datacenter amb el sistema instal·lat amb interfície gràfica, amb connexió de xarxa i usuari nomXX com usuari amb privilegis de la màquina anomenada wserverXX.
- **VM_us1804:** màquina virtual de Ubuntu Server 18.04 LTS amb el sistema instal·lat sense interfície gràfica, amb connexió de xarxa i usuari nomXX com usuari amb privilegis de la màquina anomenada userverXX.

A més, haurà de tenir un document on s'hagin resolt les diferents preguntes plantejades a la pràctica, incloent, quatre a manuals pas a pas, del procés d'instal·lació dels diferents sistemes operatius. Cal lliurar aquesta documentació a través del **Moodle del curs** dins del **termini establert**.

PT 2 | PUNTS DE RESTAURACIÓ I MECANISMES DE RECUPERACIÓ DE SISTEMES OPERATIUS

En finalitzar aquesta pràctica coneixerem els diferents mètodes que podem utilitzar als nostres sistemes operatius per tal de crear i recuperar punts de restauració i així com diferents mecanismes per la recuperació del sistema si aquest ni tant sols arrenca.

OBJECTIUS

- Utilitzar correctament els punts de restauració a Windows.
- Conèixer les eines per tal de restablir el PC a Windows.
- Crear una unitat de recuperació per restaurar i/o restablir el PC a Windows.
- Utilitzar l'eina Systemback a Ubuntu Desktop (via gràfica) per:
  - Crear punts de restauració del sistema.
  - Utilitzar l'eina de reparació del sistema.
  - Crear un LiveCD en base al nostre sistema.
- Utilitzar l'eina Systemback a Ubuntu Server (línia de comandes).
- Buscar, analitzar i interpretar la documentació tècnica necessària.
- Realitzar manuals tècnics dels procediments realitzats.

Opcions de recuperació de Windows

Realitzarem aquesta part de la pràctica amb la màquina virtual **VM_w10** tot i que tenim exactament les mateixes funcionalitats a la màquina virtual **VM_w2016**.

El primer que farem serà utilitzar una senzilla eina del sistema: **Punts de restauració**. Els punts de restauració a Windows porten al sistema a un punt anterior en el temps. Aquests es generen automàticament quan instal·les una nova aplicació, un nou controlador de dispositiu i quan actualitzes el sistema a través de Windows Update. Es poden, però, crear manualment:

- Busca a la barra de tasques "Crear un punto de restauración" i crea un punt de restauració amb nom **elmeupunt**.

Ara ja tenim el nostre propi punt de restauració. Descarrega i instal·la qualsevol aplicació lleugera (per exemple, el compressor 7zip). Aprofita i crea un document de text al escriptori. Ara anem a restaurar el sistema des del punt **elmeupunt**:

- Accedeix al Panel de Control i cerca "Restauració". Selecciona "Abrir Restaurar sistema". Selecciona **elmeupunt** i comprova la llista de programes que es veuran afectats per aquesta acció. Executa la restauració del sistema. Què ha passat amb l'aplicació que havies instal·lat? I amb el document de text del escriptori?

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Ja hem vist que es molt fàcil dur a terme aquesta tasca i a més aquesta només elimina aplicacions, controladors de dispositius o actualitzacions del sistema que poguessin causar un mal funcionament del mateix però no els nostres arxius personals.

Com ens sembla una eina útil hem decidit de programar-la per fer-nos un punt de restauració de manera setmanal. Cauria esperar que hi hagués un sistema fàcil de programació horària, com passa a les copies de seguretat, per exemple, però no és així. Per fer-ho cal accedir al registre de Windows i crear un valor "SystemRestorePointCreationFrequency".

- Busca la clau concreta del registre on crear el valor tipus DWORD de 32 bits anterior i estableix en temps (compte es mesura en minuts, per tant, una setmana = 10080 minuts).

Una altra opció per tornar a un punt anterior, de fet a un punt inicial del sistema, eliminant totes les aplicacions, controladors de dispositius i actualitzacions, així com restablint totes les configuracions fetes fins al moment al sistema és **Restablir el PC**. A més ens permet netejar-lo dels nostres arxius de manera completa si per exemple, aquests podrien estar infectats per un virus, o si volem regalar, reciclar o vendre el PC. Si escollim aquesta opció pot trigar hores però farà molt més difícil recuperar els arxius del disc dur amb fins fraudulents per part de terceres persones.

- Fes que el sistema no inicïi Windows de manera normal (Windows+L i clicar Inicio/Apagado – Reiniciar amb la tecla Shift polsada). Quan es reinici en mode de recuperació escull "Solucionar Problemas" i "Restablecer este equipo". Fes-ho fent una neteja dels arxius del disc dur. Què ha passat amb l'arxiu de text del escriptori?

Ja tenim un parell de mètodes que ens porten d'una manera més o menys "dràstica" a punts anteriors en la configuració del nostre sistema operatiu Windows. A més, hem vist que es poden accedir a les eines de recuperació a través d'un sistema en funcionament, o des de abans de que aquest s'inicïi. Tot i això, hi ha cops que no podem accedir ni tants sols a aquesta recuperació prèvia del sistema si abans no hem creat una **Unitat de recuperació**.

- Aconsegueix una unitat USB per tal de crear la teva pròpia Unitat de recuperació. Simplement cerca a la barra de tasques "Crear una unidad de recuperación" i segueix l'assistent.
- Després configura el menú boot de la teva BIOS per tal de que el sistema arranqui en primer lloc des de l'USB. Quines opcions trobes al arrancar l'ordinador des de la teva unitat de recuperació?

Systemback amb entorn gràfic

Realitzarem aquesta part de la pràctica amb la màquina virtual **VM_ud1804**.

Tot i que podríem utilitzar algunes comandes natives del sistema, en Ubuntu no hi ha d'entrada una eina de restauració/recuperació instal·lada com a part del sistema. N'hi ha diverses que podem utilitzar tot i que possiblement la més popular i que ofereix més opcions es Systemback. Així doncs, el primer de tot serà instal·lar-la:

- Obre un nou terminal i executa les següents comandes[27]:
  - `sudo apt-add-repository ppa:nemh/systemback` (afegeix el repositori)
  - `sudo apt update` (actualitza la llista de paquets disponibles)
  - `sudo apt install systemback` (instal·la el paquet systemback al nostre sistema)

Abans de posar-la en marxa hem de crear un lloc on guardar els punts de restauració del sistema, o d'altres opcions que ens ofereix l'eina. En aquest cas no podrem utilitzar un disc dur o pendrive extern en format NTFS o FAT (ja que no són natius de Linux), i per tant utilitzarem un disc dur auxiliar formatat en ext4:

- Apaga la màquina virtual **VM_ud1804** i afegeix-li un segon disc dur de 30GB. Anomena a aquest disc **disc_systemback**. Un cop afegit torna a posar en marxa la màquina. Reconeix el disc **disc_systemback**? Té format? Fes les accions necessàries per què sigui un disc dur practicable en format ext4.

Ara si és el moment de posar en marxa l'aplicació Systemback. Veurem a la dreta del programa ens ofereix diverses opcions:

- Restaurar sistema
- Copiar sistema
- Instal·lar sistema
- Crear sistema Live
- Reparar sistema
- I altres opcions

Començarem però com ho vam fer a Windows creant un **punt de restauració** després d'instal·lar alguna aplicació lleugera i crear algun document al escriptori:

- Documenta el procés per crear un punt de restauració al disc **disc_systemback**.
- Documenta el procés per restaurar el sistema des del punt de restauració creat al punt anterior. Què ha passat amb l'aplicació? I amb el document de l'escriptori?
- Com pots programar la creació de punts de restauració? Fes-ho per què creï un punt de restauració automàticament un cop per setmana.

Com has vist és una gestió fàcil tot i que pot portar una mica de temps. El següent pas serà provar d'utilitzar la opció **Crear sistema Live**, una opció interessant que ens permet crear una imatge ISO (de CD/DVD) de l'estat actual del nostre sistema, és a dir, ens permet crear un CD/DVD d'instal·lació on ja estiguin incloses les aplicacions, controladors de dispositius, configuracions i fins i tot, els arxius personals (opcional) que tenim al nostre ordinador:

- Selecciona primer el punt on crear la nostra ISO (al disc_systemback) i després la opció Crear sistema Live. Canvia el nom del sistema Live a **elmeuLive** i fes que s'incloguin els teus arxius de dades d'usuari. Fes clic en "Crear nuevo" i espera a que finalitzi el procés.
- En quin format s'ha creat la imatge del sistema **elmeuLive**?
- Ara tenim dos opcions: la primera es "Escribir en el destino" i "Convertir a ISO". Amb la primera cal tenir un USB connectat i aquest es convertiria directament en el nostre sistema Live a partir de **elmeuLive**. **Prova-ho**. La segona ens permetria fer la conversió a ISO per emmagatzemar-la al disc dur (ara ja podria ser qualsevol disc dur amb qualsevol sistema de fitxers) per més endavant copiar aquesta ISO en un USB o un CD/DVD.

[27] Si les comandes proposades no troben els repositoris per a l'última versió d'Ubuntu (18.04) descarrega els paquets necessaris i segueix el procés descrit en la pàgina web: https://francoconidi.it/systemback-1-9-3-per-debian-9-ubuntu-17-10-18-04/

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Crea una nova màquina virtual anomenada **VM_sbliveXX** (XX el teu número d'alumne). Aquesta ha d'estar preparada per instal·lar un Ubuntu Desktop 18.04, i per tant, has de respectar els requisits mínims per aquesta instal·lació.

- Posa en marxa la màquina tenint en compte de configurar al boot menú de la BIOS que ho ha de fer des d'un dispositiu USB i que has de tenir connectar el USB que conte **elmeuLive**. Fes un manual pas a pas d'aquest procés i fins que tinguis el sistema funcionant. Comprova com, per exemple, l'aplicació Systemback està instal·lada en la nova màquina virtual **VM_sbliveXX**.

Com veus, encara ens queden força eines de l'aplicació Systemback. No les provarem totes però fes una **petita descripció** (2 o 3 línies) de quines son aquestes aplicacions i per a que serveixen.

Systemback sense entorn gràfic

Realitzarem aquesta part de la pràctica amb la màquina virtual **VM_us1804**.

En aquest punt anem a veure com podem utilitzar Systemback en un entorn de treball que no disposa d'interfície gràfica:

- Primer de tot, instal·la l'aplicació Systemback a la màquina virtual **VM_us1804.**

Per llançar l'aplicació utilitzarem la comanda `sudo systemback-cli`. Segueix ara els següents passos per crear un punt de restauració del sistema:

- **Opció G** – Create new
- Quin format té el nom del punt de restauració creat? On s'ha guardat aquest punt de restauració? Això es segur?

Surt de l'apliació i executa `sudo apt install p7zip` i `sudo apt install p7zip-full`. Després fes `touch arxiuet` per crear un fitxer al teu home directory. Ara anem a recuperar el nostre punt de restauració. Torna a accedir a l'aplicació Systemback i explica pas a pas com restaures el sistema a partir del punt de restauració creat. Comenta especialment quines opcions apareixen i raona quines esculls.

RESULTATS

Arribat el final de la pràctica l'alumnat haurà de tenir molt clar la importància de tenir mètodes de recuperació per a diferents sistemes operatius, ha de saber generar aquests mètodes i aplicar-los en cas de necessitat. També haurà afegit una màquina virtual d'Ubuntu Desktop (**MV_sbliveXX**) al escenari de treball.

A més, haurà de tenir un document on s'hagin resolt les diferents preguntes plantejades a la pràctica. Cal lliurar aquesta documentació a través del **Moodle del curs** dins del **termini establert**.

Tot i el que hem aprés, a l'entorn virtual de l'aula tenim una avantatge, i és que les pròpies màquines virtuals creades amb VirtualBox et possibiliten **crear instantànies** (snapshots) de l'estat actual d'una màquina virtual de manera molt fàcil. Amb la màquina virtual apagada o encesa prems els botó en forma de càmera fotogràfica (o tecla control dret + T) i esculls un nom significatiu i una descripció. A partir d'aquell moment es crea un nou disc dur virtual des del qual s'executarà la màquina virtual i serà en ell on es facin totes les modificacions. Si més endavant cal tornar enrere podrem fer clic dret a la instantània creada anteriorment i escollir Restaurar instantània. Per tant, tenim un mecanisme de seguretat per poder guardar punts de restauració abans de provar noves configuracions, sense necessitat d'utilitzar els mètodes apresos anteriorment.

PT 3 | GESTORS D'ARRENCADA I ACTUALITZACIÓ DE SISTEMES OPERATIUS

En finalitzar aquesta pràctica sabrem com administrar l'arrencada d'una màquina dual amb dos sistemes operatius instal·lats a través de la configuració dels seus gestors d'arrancada. En segon lloc, aprendrem quins mètodes d'actualització ofereixen els sistemes operatius.

OBJECTIUS

- Instal·lar dos sistemes operatius dins d'una màquina virtual.
- Corregir problemes amb els gestors d'arrancada.
- Conèixer Windows Update.
- Conèixer el Gestor d'actualitzacions d'Ubuntu
- Buscar, analitzar i interpretar la documentació tècnica necessària.
- Realitzar manuals tècnics dels procediments realitzats.

Construcció de màquines virtuals amb arrencada dual

Quan anem a instal·lar una màquina virtual dual (Windows + Ubuntu) hauríem de tenir em compte que el millor ordre per fer les instal·lacions és: primer Windows i segon Ubuntu, ja que el GRUB (gestor d'arrencada) d'Ubuntu respecta les entrades al MBR (o GPT) d'altres sistemes com Windows. En canvi, el gestor d'arrencada de Windows, només reconeix les entrades d'altres sistemes Windows que hi pugues haver instal·lats en l'ordinador, però "destrueix" les entrades que fan referència a altres sistemes operatius d'altres famílies, per exemple, d'Ubuntu.

Començarem realitzant una instal·lació dual en l'ordre adequat. Primer prepararem una nova màquina virtual **VM_dualwuXX** (XX el teu número d'alumne). Fes-la preparant-la per instal·lar Windows 10 i utilitzant un disc dur de 60GB. A més, en l'apartat "Sistema" de la configuració de la màquina virtual marca l'opció "Habilitar EFI" per tal de que el gestor d'arrancada utilitzi UEFI BIOS. Un cop preparat escenari instal·la Windows 10.

Amb la màquina virtual **VM_dualwuXX** amb Windows 10 funcionant, anem a reservar un espai del nostre disc dur per fer la instal·lació d'Ubuntu Desktop 18.04. Accedeix al "Administrador de Discos" i redueix el volum de 60GB deixant 15GB com espai sense assignar. Adjunta una captura de pantalla d'aquesta configuració.

Ara apaga la màquina virtual **VM_dualwuXX** i introdueix la iso d'Ubuntu Desktop 18.04 al lector de CD/DVD. Inicia la màquina per instal·lar Ubuntu. Escull durant la instal·lació que vols instal·lar el teu sistema Ubuntu junt a Windows per tal de respectar les seves entrades a la UEFI BIOS.

- Ha funcionat correctament? Arranquen els 2 sistemes operatius? Adjunta una captura de pantalla del procés de boot on el GRUB-EFI d'Ubuntu deixa escollir iniciar Ubuntu Desktop 18.04 o Windows 10.

Ara intentarem una instal·lació més complicada, imaginant que ja tenim un Ubuntu Desktop 18.04 instal·lat, configurat i personalitzat, amb tots els nostres documents, etc., i per tant, no volem seguir l'ordre primer Windows i després Ubuntu ja que aquest últim el volem preservar tal i com està.

Primer de tot crearem una nova màquina virtual **MV_dualuwXX** (XX el teu número d'alumne). Aquesta estarà preparada per instal·lar Ubuntu Desktop 18.04 i utilitzarà un disc dur de 60GB. Marca a més, que utilitzarà UEFI BIOS en la seva instal·lació. Instal·la la màquina escollin fer particions al disc:

- Primer fes una partició de 3GB per instal·lar una partició EFI, per tal de que el sistema Ubuntu Desktop 18.04 pugui utilitzar UEFI BIOS.
- En segon lloc una partició de 12GB on instal·laràs l'arrel del teu sistema Ubuntu (punt de muntatge: /).
- Després assigna la resta d'espai (45GB) com una partició FAT32 (format que si reconeix Windows) i reserva l'espai per un sistema Windows (punt de muntatge: /windows).

  Adjunta una captura de pantalla de la teva configuració.

- Acaba el procés d'instal·lació i després apaga la màquina virtual **MV_dualuwXX**.

Anem a instal·lar ara Windows 10. Introdueix al lector de CD/DVD de la màquina virtual **MV_dualuwXX** la iso de Windows 10, posa-la en marxa i instal·la, al espai de 45GB reservat anteriorment, el sistema operatiu. En acabar, apaga el sistema i retira la iso de Windows 10 del lector de CD/DVD.

Torna a iniciar la màquina virtual **MV_dualuwXX**, algun problema?

- Per solucionar-lo prova en un primer pas des del mode de recuperació d'Ubuntu d'executar la comanda: `update-grub`. Detecta la partició de Windows? Reinicia (`systemctl reboot`) i prova d'iniciar Windows 10. Ha funcionat?

Sembla que ja tenim disponible el nostre sistema dual. Però, intenta iniciar Ubuntu Desktop 18.04 a la màquina virtual **MV_dualuwXX**. Accedeix, o continua entrant en el mode de recuperació?

Troba una solució a aquest problema editant el gestor d'arrancada GRUB per sistemes amb UEFI BIOS. Documenta pas a pas aquest procediment.

Gestors d'actualitzacions

Unes de les característiques desitjables d'un sistema operatiu és que es mantingui actualitzat d'una manera regular, incorporant suport per a nous controladors de dispositius, noves aplicacions i/o noves amenaces de seguretat que poden intentar "explotar" vulnerabilitats del propi sistema.

En el cas dels sistemes lliures, aquestes actualitzacions, arribaran al punt d'anar canviant el propi sistema operatiu per un de nou cada cert temps ja que optimitzarem al màxim el nucli del nostre sistema operatiu sense cap cost. En canvi, si treballem amb sistemes operatius propietaris (de pagament), sabem que tot i que es van actualitzant, tenen una "data de caducitat", ja que a partir d'un determinat moment, no es donarà suport tècnic (ni es crearan noves actualitzacions) per al nostre sistema, i per tant, tindrem que tornar a adquirir (pagar) un nou sistema operatiu.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

Un cop deixat això clar, veiem els mètodes que ofereixen Windows i Ubuntu per gestionar les actualitzacions regulars del sistema:

- Inicia la màquina virtual **MV_w10** i a través de "Configuración" i "Actualización y Seguridad" podràs accedir al gestor d'actualitzacions de Windows 10: **Windows Update**. S'ha fet ja alguna actualització?
- Fes una cerca inicial d'actualitzacions pel teu sistema operatiu. Ha trobat alguna? Has pogut escollir que fer amb les actualitzacions trobades? Què ha passat?
- Fes clic en "Opciones avanzadas" i explica quines opcions hi apareixen. Alguna permet que les actualitzacions no es descarreguin i/o instal·lin automàticament?

Ja veiem que Windows 10 no ens posarà tant fàcil el fet de deshabilitar la descarrega i/o instal·lació automàtica d'actualitzacions. Una opció dràstica seria la següent: deshabilitar el servei de Windows Update. Busca informació sobre la consola d'administració de serveis de Windows i digues com es pot accedir i deshabilitar un servei.

Òbviament, aquesta no és una opció gens recomanable ja que, en un temps, el nostre sistema podria començar a ser molt vulnerable per falta d'actualització. Llavors, com podem mantenint-nos actualitzats però escollint quan descarregar i/o instal·lar les actualitzacions? Segueix els següents passos:

- Accedirem a la consola[28] d'edició de les directives de grup local amb **gpedit.msc**. Per fer-ho només cal fer clic dret sobre el menú "Inicio" i "Ejecutar" i escriurem gpedit.msc. Com veuràs és un editor molt ampli on trobarem centenars de configuracions agrupades en dos grans blocs: Configuració de l'equip i Configuració d'usuari. Cadascuna d'aquestes té tres subcategories principals: Configuració de Software, Configuració de Windows i Plantilles administratives.
- En el nostre cas seguirem la següent ruta: Configuració de l'equip – Plantilles administratives – Components de Windows – Windows Update.
- Com pots fer que el sistema operatiu ens notifiqui que tenim descarregues disponibles, per poder escollir quan descarregar-les, i si les volem instal·lar o no un cop descarregades?

Anem ara a iniciar la màquina virtual **VM_w2016**. Tot i que en el nostre cas tenim una GUI instal·lada ens posarem al cas de que tenim el servidor només en mode comandes, i aprendrem a gestionar les actualitzacions en aquest cas:

- Executa una finestra de PowerShell amb privilegis d'administrador.
- El primer que farem serà instal·lar un complement per tal de gestionar Windows Update:
  - `Install-Module PSWindowsUpdate`
- Ara canviarem la política d'execució del PowerShell a "seguretat remota"[29]:
  - `Set-ExecutionPolicy RemoteSigned`

[28] En els sistemes Windows moltes de les opcions de configuració es poden fer a través de consoles (o complements) que allotgen i mostren eines administratives. Aquestes son conegudes com **Microsoft Management Console (MMC)** i s'accedeixen amb comandes tipus nomcomanda.msc

[29] La política d'execució remota (RemoteSigned) permet que les seqüencies de PowerShell descarregades des d'Internet s'executin a la nostra màquina sempre i que siguin signades per un editor de confiança.

- Ja podem importar el nou mòdul instal·lat:
  - `Import-Module PSWindowsUpdate`
- Per poder veure totes les opcions disponibles executarem la següent comanda:
  - `Get-Command -module PSWindowsUpdate`
- Com veus tenim bastants opcions. La primera que farem servir es llistar totes les actualitzacions disponibles als servidors de Microsoft Update:
  - `Get-WUList -MicrosoftUpdate`
- Per tal d'instal·lar manualment i amb conformitat cadascuna de les anteriors actualitzacions:
  - `Get-WUInstall -MicrosoftUpdate`
- Ara reinicia la màquina virtual **MV_w2016** torna a entrar al PowerShell i contesta les següents preguntes:
  - Com pots veure l'historial d'actualitzacions que ja s'han instal·lat al sistema?
  - Consulta l'ajuda de la comanda Get-WUInstall (`Help Get-WUInstall -full`). Amb quins paràmetres modificaries la instrucció d'instal·lació per què en comptes de preguntar i demanar conformitat una per una, s'acceptessin totes i a més, es reinicies la màquina automàticament en acabar de instal·lar-les?

Treballarem ara amb els sistemes de la família Ubuntu. Inicia la màquina **MV_uc18.04**.

Busca l'aplicació "**Software y actualizaciones**". Des d'aquí podrem configurar a la pestanya "Actualizaciones" quins tipus d'actualitzacions volem que es descarreguin i instal·lin al nostre sistema:

- Quins son aquests tipus d'actualitzacions?
- Programa el teu sistema per què busqui noves actualitzacions setmanalment i, si troba actualitzacions de seguretat, les descarregui automàticament, però que demani el teu consentiment per instal·lar-les. També volem que ens avisi de qualsevol nova versió del sistema operatiu que hi hagi disponible (sigui o no LTS).

També podem llançar manualment en qualsevol moment l'actualitzador de software buscant l'aplicació "**Actualización de software**" (que es basa en els paràmetres que es poden ajustar a "Software y actualizaciones").

Si no tenim entorn gràfic, o simplement volem utilitzar la línia de comandes, podem executar:

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

- Explica què fa cadascuna de les tres comandes de l'execució anterior?

RESULTATS

Arribat el final de la pràctica l'alumnat haurà de saber com fer instal·lacions de màquines duals respectant els gestors d'arrancada dels diferents sistemes operatius, i/o arreglant els possibles problemes que hi puguin sorgir. L'alumnat també sabrà mantenir actualitzats els seus sistemes operatius així com gestionar aquestes actualitzacions. També haurà afegit dues màquines virtuals (**MV_dualwuXX** i **MV_dualuwXX**) al escenari de treball.

A més, haurà de tenir un document on s'hagin resolt les diferents preguntes plantejades a la pràctica. Cal lliurar aquesta documentació a través del **Moodle del curs** dins del **termini establert**.

MP01 – UF 1 | INSTAL·LACIÓ, CONFIGURACIÓ I EXPLOTACIÓ DEL SISTEMA INFORMÀTIC

RA 2 | Configura el programari de base, atenent a les necessitats d'explotació del sistema informàtic

7. Administració d'usuaris i grups locals
   - ACT 15 | Comptes de correu per iniciar sessió a Windows
   - ACT 16 | Comptes d'usuaris locals i perfils amb Windows
   - ACT 17 | Usuaris i grups locals en l'entorn Ubuntu

8. Seguretat de comptes d'usuari
   - ACT 18 | Directives de bloqueig de comptes a Windows
   - ACT 19 | Política de contrasenyes a Ubuntu

PT4 | Configuració de xarxa i connectivitat de sistemes operatius
PT5 | Sistema de noms de dominis als diferents sistemes operatius

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

7. ADMINISTRACIÓ D'USUARIS I GRUPS LOCALS

La gestió d'usuaris i grups prem molta més importància quan estiguem treballant dins d'una organització i tinguem un controlador de domini des del qual gestionar molts comptes d'usuari que treballaran en diferents equips clients i amb diferents nivells d'accés.

A nivell d'una màquina local, com pot ser a un domicili, l'habitual és que hi hagi un sol usuari d'aquell equip, o com a molt, un parell o tres pels diferents membres d'una família. Tot i això, la base de gestió d'usuaris i grups locals serà un bon punt de partida per a la gestió d'usuaris de domini que veurem més endavant.

7.1. USUARIS I GRUPS LOCALS A WINDOWS

El fet de disposar de diferents usuaris ens permet que cadascun pugui iniciar sessió amb uns paràmetres i un aspecte determinat. A cada usuari se li associa un **compte** amb el seu login i contrasenya (o mètode d'accés) i les seves preferències s'emmagatzemaran al que denominem **perfil**. En aquest perfil, a més de les configuracions pròpies de l'usuari (com per exemple el seu fons d'escriptori), es guarden carpetes personals com "Mis Documentos", "Mis Imagenes", etc., i d'altres de creació pròpia. Només aquell usuari tindrà accés a les carpetes (a no ser que doni permisos a d'altres usuaris). L'administrador, o un usuari amb privilegis d'administrador, pot accedir a les carpetes individuals de cada usuari (per defecte).

Als sistemes operatius Windows existeixen quatre **tipus de comptes d'usurari**:

- **Usuari estàndard**: té accés als recursos que permeten treballar de manera habitual amb l'equip (navegar per Internet, obrir aplicacions ofimàtiques, jugar, imprimir, etc.), però no permeten accedir a arxius del sistema, instal·lar o desintal·lar programes, etc.
- **Usuari convidat**: té molt restringits els seus privilegis, i està pensada per un usuari esporàdic.
- **Usuari amb privilegis d'Administrador:** últimament Windows habilitat aquest tipus d'usuari com a mesura de seguretat ja que permet algunes funcions d'administració però no té un accés o control total sobre tots els arxius del sistema. El primer usuari que creem durant la instal·lació de Windows n'és un exemple.
- **Administrador local:** disposa d'accés total al sistema. Per seguretat, i per defecte, Windows 10 deixa desactivat[30] aquest perfil d'usuari (no pot iniciar sessió).

A més, cal dir que els sistemes actuals de Windows, a més de tenir l'opció d'arrancar amb un usuari local "clàssic", permet fer login a través d'un compte de correu electrònic Microsoft per tal de sincronitzar aquell usuari local amb el compte de correu i fer que les seves configuracions siguin visibles en diferents màquines en les que el nostre correu de Microsoft estigui introduït com un compte d'usuari vàlid a la secció "Configuración – Cuentas". Amb aquesta utilitat, també podrem agregar comptes d'usuari especificant que son familiars (adults o menors) i gestionar així configuracions de control parental.

[30] Per activar l'usuari Administrador cal anar al intèrpret de comandes (CMD) executant-lo amb privilegis d'administrador, i utilitzar la comanda `net user administrator /active:yes`

ACT 15 | **Comptes de correu per iniciar sessió a Windows**

Abans de continuar amb la configuració de comptes d'usuari en el mètode més "clàssic", anem a provar a iniciar sessió a una màquina virtual de Windows 10 amb un compte de correu electrònic de Microsoft.

a. Com inicies la sessió amb un compte de correu al teu equip Windows 10?
b. Configura algun paràmetre ben visible (per exemple, el tema d'escriptori) per al teu usuari de correu electrònic. Després marca totes les opcions de sincronització de comptes dins del menú "Configuración – Cuentas".
c. Com pots afegir un altre compte de correu com a vàlid per iniciar sessió a la teva màquina virtual de Windows 10? Afegeix el compte de correu d'un company. Fes que inicïi sessió. Té la seva configuració? Prova tu en la seva màquina virtual.

Tornant als usuaris locals "clàssics", veurem com crear comptes d'usuari local. Primer de tot accedirem a la consola "Administración de equipos" i concretament a "**Usuarios y grupos locales**". A partir d'aquí es molt fàcil crear un nou usuari. Només caldrà fer clic dret dintre de la carpeta "Usuarios", escollir crear un usuari nou i completar els camps que veiem a la Figura | 16.

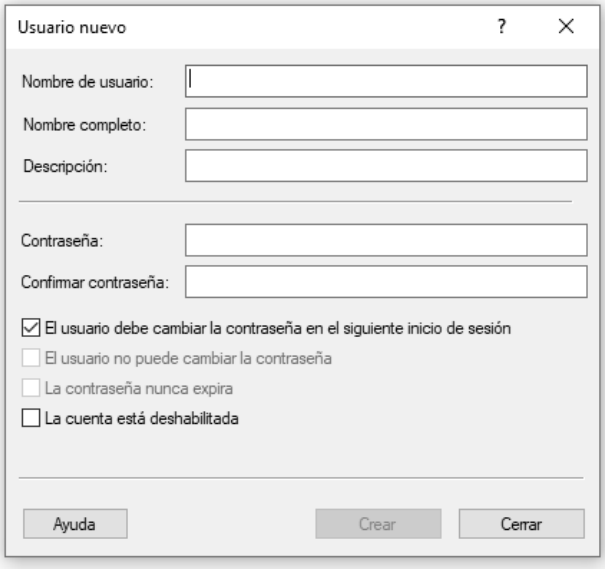


Figura 16 | Formulari per la creació d'un usuari local a Windows

Després hem d'escollir una contrasenya i repetir-la. Aquesta haurà de complir els requisits de complexitat, que aprendrem a modificar en el següent apartat d'aquest tema. A més, ens donarà diverses opcions, per indicar si cal canviar la contrasenya preestablerta en el primer inici de sessió, si l'usuari no podrà modificar-la, si la contrasenya no caduca (tot i que ho especifiquem així a les polítiques de seguretat) o, fins i tot, deshabilitar un compte d'usuari temporalment, sense necessitat d'eliminar-lo i perdre, per tant, les seves configuracions.

Un cop hem creat un usuari podem veure dins les seves propietats que s'inclou automàticament al grup local "Usuarios", però no al grup "Administradores" i per tant, serà un **usuari estàndard** del sistema operatiu. A més disposem de la fitxa "Perfil". Dins d'aquesta podríem assignar una ubicació especifica on crear el seu perfil d'usuari[31], o simplement una unitat de disc connectada on allotjar una carpeta particular (un espai a un disc dur) per aquell usuari.

[31] Per defecte els perfils dels usuaris de Windows es guarda a la carpeta C:\Usuarios amb una carpeta amb el seu login. Aquesta carpeta es crea en el primer inici de sessió de l'usuari al sistema i es basa en les configuracions de la carpeta "Default" de la mateixa ruta.

ACT 16 | **Comptes d'usuaris locals i perfils amb Windows**
Anem a treballar amb algun usuari local i el seu perfil:

a. Crea des de "Usuarios y grupos locales" un usuari anomenat *Usuari Prova* amb login *prova* i contrasenya *12345678* que haurà de canviar en el primer inici de sessió. Abans d'iniciar sessió amb *prova* contesta:
   - Pertany a algun grup local? Quin?
   - Té un perfil d'usuari creat a C:\Usuarios?

b. Inicia la sessió amb l'usuari *prova*. Comprova que triga ja que s'està generant el seu perfil. Canvia la contrasenya i modifica el seu fons d'escriptori. Torna a tancar la sessió, i a iniciar-la. Veuràs que va més ràpid i a més es conserva el nou fons d'escriptori.

c. Accedeix a l'equip amb l'usuari *nomXX* (que tindrà privilegis d'administrador) i busca la manera d'esborrar el perfil de l'usuari *prova*. Nota: hi ha un mètode recomanable que no és eliminar la carpeta C:\Usuarios\prova. Podrà iniciar sessió ara l'usuari *prova* sense perfil? Per què?

A continuació parlarem dels **grups locals**. En principi la idea de fer un grup d'usuari es aconseguir una gestió més eficaç en l'**assignació de permisos**. En un equip local d'una llar possiblement no tingui molta utilitat, ja que no tindrem un gran volum d'usuaris que utilitzin la màquina. Per tant, la gestió de grups serà molt més interessant en un àmbit de domini que no pas en l'àmbit local.

Tot i això, potser podem imaginar un equip per una botiga que tingui diversos venedors, encarregats, etc., i que han de tenir accés a diferents unitats o carpetes dins dels discs durs, i trobem útil fer algun grup en funció del "tipus" d'usuari i el permís, o no, que te sobre la unitat i/o carpeta concreta.

Dins de "Usuarios y grupos locales" tenim una carpeta "Grupos" on per defecte veurem una bona llista de grups locals per defecte en funció bàsicament de les diferents **tasques administratives** que poden o no desenvolupar. Estan acompanyats d'una descripció força explicativa. Per fer que un usuari pertanyi a un d'aquests grups només cal entrar a les seves propietats i agregar membres.

Si el que volem és crear un grup local propi (en l'exemple de la botiga el grup venedors i el grup encarregats), cal fer clic dret dins la carpeta "Grupos" i escollir crear un nou grup (Figura | 17).

Només cal assignar-li un nom, una descripció, i directament podem agregar els usuaris locals que volem que pertanyin al grup.

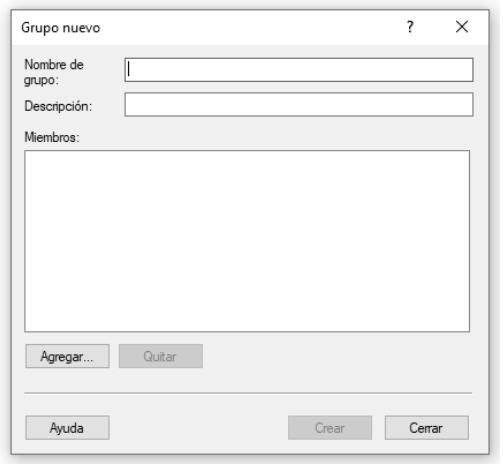


Figura 17 | Formulari per la creació d'un grup local a Windows

Per últim veurem com podem gestionar els comptes d'usuaris locals a través del CMD. Ho farem posant alguns exemples d'accions possibles a realitzar. Et recomano que facis proves de les comandes que veurem a continuació:

- Per a llistar els usuaris locals del sistema: `net user`
- Per crear un nou usuari local estàndard: `net user nomusuari /add`
- Per afegir una contrasenya a un usuari local: `net user nomusuari *` (també pot ser útil per esborrar la contrasenya a un usuari local contestant en blanc quan ens sol·licitin la nova).
- Podríem combinar les dues comandes anteriors: `net user nomusuari * /add` (més ràpid i a més, si un requisit de les polítiques de seguretat fots que no podem crear usuaris locals sense contrasenya, aquest seria l'únic mètode vàlid).
- Per esborrar un usuari local: `net user nomusuari /delete`
- Per a llistar els grups locals del sistema: `net localgroup`
- Per agregar un usuari local amb privilegis d'administrador: `net localgroup administradores nomusuari /add`
- Per eliminar els privilegis d'administració d'un usuari local: `net localgroup administradors nomusuari /delete`

7.2. USUARIS I GRUPS LOCALS A UBUNTU

Anem a estudiar la gestió d'usuaris i grups locals als sistemes operatius Ubuntu començant de "dins cap a fora", és a dir, aprendrem primer en quins fitxers guarda el sistema operatiu les configuracions dels comptes d'usuari i dels grups, per veure després amb quines comandes podem editar aquests fitxers, i deixant com una activitat final la utilització de les eines gràfiques que funcionen com a frontend del que hem aprés.

Ubuntu guarda un llistat de tots els seus usuaris locals dins d'un fitxer anomenat **passwd** ubicat dins del directori clàssic de les configuracions del sistema (/etc). És interessant veure com el nom del fitxer indica una característica particular dels sistemes Linux, i és que, tots els usuaris han de tenir obligatòriament una contrasenya, sinó no podran iniciar sessió a l'equip. El fitxer /etc/passwd conté una llista amb els usuaris locals (d'entrada ja força plena per què té usuaris "fantasmes", que no poden iniciar sessió, però que utilitzen diferents serveis del sistema per funcionar, per exemple, l'usuari mail). Cada línia del fitxer representa un usuari concret i té una estructura com la que veiem a la Figura | 18:

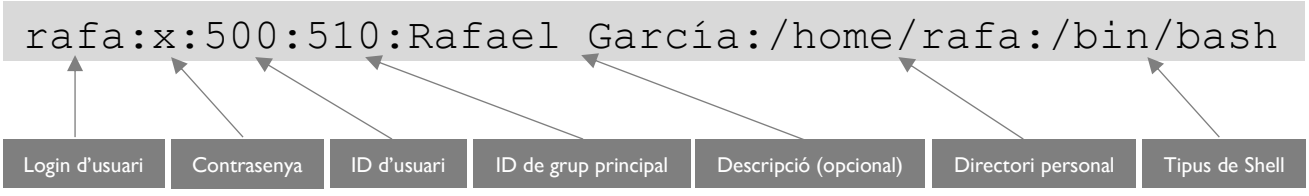


Figura 18 | Paràmetres dins del fitxer /etc/password

En aquest exemple veiem que el primer que trobem a cada línia del fitxer és el nom **únic** i identificatiu del usuari al sistema.

També tindrà com a paràmetre identificatiu el seu **número de ID** (en l'exemple el 500). És habitual que els números d'usuaris creats al sistema comencin a partir del 500 ja que els anteriors (del 0, que correspon sempre a l'usuari root, fins al 499) estan reservats per aquells usuaris especials per tasques administratives que comentàvem. El **ID de grup principal** (al exemple el 510) no ha de ser únic (òbviament pot haver més d'un usuari dins d'un grup i que aquest sigui el principal de tots), i també segueix la norma anterior del 0 = root i fins al 499 = grups reservats del sistema. Tots els usuaris han de pertànyer a un grup com a mínim (el grup principal), tot i que poden pertànyer a molts altres (tot i que això no ho podem veure en aquest fitxer). En crear un usuari, doncs, cal introduir-lo a un grup, si no ho fem manualment, automàticament es generarà un grup amb el mateix nom que l'usuari creat.

Ens havíem deixat enrere el paràmetre "**Contrasenya**" (al exemple una x). En principi hauríem de trobar una contrasenya xifrada en hash però com que el fitxer /etc/passwd té permisos de lectura per tothom, fa temps és va implementar un "sistema en l'ombra", on només el root podia veure el contingut de les claus encriptades. Per tant, si em comptes d'un llarg hash trobem una `x`, voldrà dir que la contrasenya d'aquest usuari estarà emmagatzemada al fitxer **/etc/shadow** (o fitxer a l'ombra). A més, es pot donar alguna altra circumstància especial en aquest paràmetre: si trobem un símbol `!` voldrà dir que aquell compte d'usuari està deshabilitat temporalment, si trobem `!!` vol dir que l'usuari no té contrasenya i per tant, no iniciarà sessió en Ubuntu, i per últim, si trobem `*` (molt típic en els usuaris del sistema) vol dir que son usuaris amb els que no podrem iniciar sessió però si que podran ser cridats per que realitzin tasques determinades.

Continuem avançant per la línia de l'usuari i després del seu ID i ID de grup principal, ens trobem un paràmetre (o paràmetres), la **descripció**, molts cops buit (ja que és opcional) però que pot contenir molta informació: el nom complert de l'usuari (com a l'exemple), el departament, el seu e-mail, telèfon, etc.

El següent paràmetre és el **directori personal** (o home directroy). Aquest serà l'espai reservat per cada usuari, on tindran permisos totals sobre els subdirectoris i fitxers que hi creïn, és la seva àrea de treball. A més, és en aquest directori on es guarden dos fitxers anomenats **.bashrc** i **.bash_profile**[32] (ocults, ja que tots els fitxers que comencen amb . a Ubuntu ho son) amb les configuracions personals de l'entorn de treball per aquell usuari, és a dir, el seu **perfil** (les configuracions per defecte estan configurades al fitxer /etc/login.defs). El més habitual és que estiguin ubicats al directori /home/nomusuari, tot i què es pot especificar un altra ubicació, o fer subdivisions (per exemple, a un institut tenir /home/profes/nomusuari per cada professor/a, i /home/alumnes/nomusuari per cada alumne/a)[33].

L'últim paràmetre que trobem és l'indicador de quin tipus d'**entorn d'intèrpret de comandes** (Shell) utilitzarem. Per un usuari habitual d'Ubuntu serà /bin/bash (versió extensa del /bin/sh). Veurem però que hi ha altres shells particulars com /bin/false o /sbin/nologin que poden aparèixer en aquells usuaris "fantasmes" amb tasques administratives i que reiteren el seu esperit de no ser usuaris amb drets no tant sols d'iniciar sessió a través de la GUI, sinó que tampoc es poden utilitzar per treballar des de l'entorn de la línia de comandes.

[32] Hi ha uns fitxers /etc/bashrc i /etc/profile generals per a tot l'equip només accessibles per l'usuari root que afecten a tots els usuaris del sistema, permetent una imposició de configuracions.

[33] És una pràctica habitual que en el moment de fer la instal·lació del sistema el directori /home tingui el seu punt de muntatge en una partició o disc diferent que el del sistema (/), protegint així les dades dels usuaris davant fallides del disc del sistema.

Autor | RAFAEL GARCÍA SUÁREZ
Contacte | rgarc259@xtec.cat

L'altre fitxer a tenir en compte quan parlem d'usuaris i grups locals a Ubuntu, és l'anomentat **group**. Òbviament és tracta del llitat de grups locals de l'equip i, com a fitxer de configuració, el trobem a /etc. Cada línia del fitxer correspondrà a un grup, i com en el cas dels usuaris, també trobarem ja bastants grups locals del sistema creats. Veiem la seva estructura (Figura | 19):

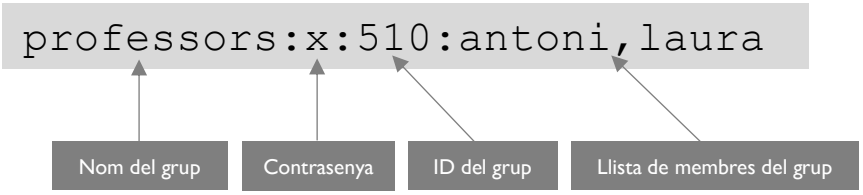


Figura 19 | Paràmetres dins del fitxer /etc/group

En aquest exemple veiem que el primer que trobem es el nom **únic** i identificatiu del grup al sistema. També el podem identificar pel seu **ID de grup** (a l'exemple, 510) que com en el cas dels usuaris tindrem el 0 per el grup root i fins al 499 reservats per a grups del sistema.

Abans del ID de grup ens trobarem amb el paràmetre **contrasenya** amb les mateixes condicions que en el cas dels usuaris, i per tant, podem trobar un hash o una x (si aquesta és troba a un fitxer a l'ombra, en aquest cas el **/etc/gshadow**). L'única diferencia és que en els cas dels grups la contrasenya **no** és obligatòria per tal de que el grup sigui funcional, això si, qualsevol usuari podrà unir-se al grup, o treballar temporalment sota els permisos d'aquest grup.

L'últim paràmetre és la llista de **membres del grup**, composta pels login dels diferents usuaris que son membres del grup separats per comes. Fem la següent reflexió, a la Figura | 18 veiem que el grup principal de l'usuari amb login rafa era precisament el grup amb ID=510. No hauria d'aparèixer, per tant, a la llista de membres del grup? La resposta és no, ja que només apareixeran com a membres del grup aquells que hi pertanyin però dels quals no sigui el seu grup principal. Dit d'un altra manera, per conèixer el grup principal d'un usuari ens dirigirem al fitxer /etc/passwd, i per conèixer els grups secundaris al fitxer /etc/group.[34]

Ara ja coneixem els dos fitxers principals on s'ubiquen els usuaris i els grups locals del sistema. Tot i que es possible, no és gens recomanable editar directament aquests fitxers per tal de generar i/o modificar un usuari i/o grup. Per fer-ho el sistema operatiu Ubuntu disposa de comandes que ens permetran gestionar usuaris i grups locals.

El primer que farem és aprendre a **crear un usuari**. Com es obvi només l'usuari root (o un usuari amb la capacitat de fer sudo, SuperUserDO[35]) tindran privilegis per fer-ho, així com per modificar o eliminar usuaris posteriorment.

[34] Disposem de diverses comandes per fer aquestes consultes més fàcilment: `id`, `groups` i `members`. Donen una informació semblant i son molt útils per no anar a fer cerques sobre els fitxers /etc/passwd i /etc/group.

[35] Existeix un grup local del sistema anomenat precisament sudo, i per tant podem fer que un usuari adquireixi privilegis administratius afegint-lo a aquest grup. El primer usuari que creem durant la instal·lació és membre del grup sudo (pots comprovar-lo executant: `members sudo`, o buscant la informació del grup al fitxer: `cat /etc/group | grep sudo`)

La comanda que utilitzarem és **useradd** tot i que fer `sudo useradd nomusuari` no serà de gran utilitat ja què cal una millor definició de l'usuari per què aquest pugui arribar a ser realment útil. Ens cal, llavors, estudiar les diferents opcions que ens proporciona la comanda:

- **Afegir home directory:** tot usuari requereix de tenir una carpeta personal per carregar les seves configuracions, i disposar d'un àrea de treball amb permisos de lectura/escriptura. Necessitem especificar dos opcions: **-m** (make home directory) i **-d *ruta*** (per especificar on s'ha de crear).
- **Afegir un intèrpret de comandes:** opció **-s /bin/bash** (típicament).

Amb aquestes tindríem gairebé creat un usuari funcional, només caldria posar-li una contrasenya. Ho podem fer a la línia de creació **-p *password*** tot i que es més recomanable fer-ho posteriorment amb la comanda **passwd *nomusuari***.

Si ho fem així és crearà un usuari funcional amb el nom especificat i amb grup principal un de nou amb el mateix nom. Si volem especificar durant la creació que el grup principal de l'usuari ha de ser un altre, ho farem amb la opció **-g *grup*** (ha d'existir el grup prèviament). Si el que volem es afegir-lo a un grup (o grups) complementari l'opció seria **-G *grup1,grup2,..,grupN***.

Altres opcions podrien especificar el seu UID (sinó agafa el següent disponible) amb l'opció **-u *UID***, o afegir una descripció: **-c *comentari***. Com sempre podeu consultar la llista complerta d'opcions al manual de la comanda (`man useradd`).

Podem crear un usuari també amb la comanda **adduser**. Aquesta comanda, però, és només un bash script a mode de frontend de adduser, que ens ajuda a crear l'usuari de forma interactiva a través de diverses preguntes, tot i que molt orientades a "descriure l'usuari": el seu departament, email, etc., i sense possibilitats de modificar camps com el grups (grups), home directory, UID, etc.

Un cop hem creat un usuari, no té perquè ser una entitat passiva i inamovible. Podem fer modificacions sobre aquest amb la comanda **usermod**, que a més, comparteix moltes opcions en comú amb usseradd, i per tant, ens resultarà molt similar canviar qualsevol paràmetre d'usuari amb opcions conegudes per la seva creació. Alguna opció particular de usermod, i que ens pot ser útil, és que ens permet, bloquejar un usuari temporalment sense eliminar-lo (opció **-L**, lock, /etc/passwd paramètre contrasenya igual a `!`). Podent desbloquejar-lo després (opció **-U**, unlock, elimina `!` del /etc/passwd).

Per eliminar un usuari, utilitzem la comanda **userdel**. Si ho fem així directament eliminarem el compte (l'entrada a /etc/passwd), però es conservaran els seus arxius i configuracions al seu home directory. Si no volem conservar-los, volem purgar realment tot el rastre de l'usuari al sistema, utilitzarem la opció **-r**.[36]

En aquest punt sabem crear, configurar, modificar i eliminar usuaris. Per canviar entre usuaris podrem iniciar diferents entorns gràfics, o dintre d'un terminal executar la comanda **su *nomusuari*** (select user).

Veurem que per treballar amb grups tindrem unes comandes similars:

[36] En principi no podem eliminar un usuari si aquest està logejat al sistema. Tot i això podem forçar-ho, tot i que no es recomanable, amb l'opció -f de userdel.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

La comanda **groupadd** ens permetrà crear un grup fàcilment. Si volem podrem especificar el seu GID (opció **-g**) o posar-li un password (opció **-p**, tot i que es millor, com en el cas dels usuaris, fer-ho a posteriori amb la comanda **gpasswd**).

Per modificar un grup utilitzarem **groupmod**, tenint en compte que només ens ha de servir per fer modificacions pròpies del grup (no pels usuaris que hi poden pertànyer). Podrem per tant canviar el nom del grup (opació **-n**) o el seu GID (opció **-g**).

Per tal de modificar usuaris dins del grup, sense recórrer a fer-ho usuari per usuari amb usermod, utilitzarem la comanda **gpasswd**. Típicament utilitzada per assignar contrasenyes als grups, també ens permet interesants opcions: **-M** llista els membres d'un grup, **-a *usuari*** afegeix a un usuari al grup (el tindrà com a grup secundari) o **-d *usuari*** eliminarà un usuari del grup.

Per tal de determinar el grup de treball d'un usuari que pertany a més d'un grup (el principal i algun o alguns secundari/s), hem de tenir em compte que en el seu inici de sessió cada document, directori, etc., que pugui crear, serà propietat seva i el grup de privilegis serà el del seu grup principal. Si volem canviar temporalment això, cal executar la comanda **newgrp *nomgrup***. Si l'usuari es membre del grup especificat treballarà directament amb ell fins fer **exit**. Si no pertany al grup, se'l demanarà la contrasenya del grup per poder treballar amb ell (a no ser que sigui un grup "obert" sense contrasenya).

Per acabar, podrem eliminar un grup utilitzant la comanda **groupdel** que òbviament no eliminarà els usuaris membres del grup, només la seva entrada com a grup en /etc/group.[37]

ACT 17 | **Usuaris i grups locals en l'entorn d'Ubuntu**

Ja hem vist des de quins fitxers emmagatzemen la informació d'usuaris i grups locals fins quines comandes podem utilitzar per la gestió d'aquests fitxers. Ens queda aprendre a utilitzar l'entron gràfic d'Ubuntu en aquest aspecte.

a. Busca l'aplicació "Usuarios" del teu sistema Ubuntu. Què és el primer que has de fer per poder afegir un usuari? Quins paràmetres et demanen? Pots canviar per exemple, el seu home directory d'ubicació? Crea un usuari, i busca la seva línia a /etc/passwd, comenta cada paràmetre d'aquesta.

b. Prova ara de buscar com aplicació "Usuarios y grupos". Com veuràs ni tant sols, hi ha instal·lat de forma predeterminada una aplicació per gestionar grups locals de forma gràfica. Igualment pots descarregar-la i instal·lar-la. Fes-ho i després prova de crear un nou grup, i afegir l'usuari anterior. Revisa els fitxer /etc/group per veure que ho has fet correctament.

c. Torna a fer els punts a i b per un nou usuari i grup, però ara utilitzan les comandes que hem vist abans. Quin mètode et dona més possibilitats de configuració? Quines diferencies veus en els fitxers entre els usuaris/grups creats per comandes i/o per entorn gràfic?

[37] La comanda groupdel pot generar un codi de error en la seva sortida si estem eliminant el grup principal de l'usuari.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

8. SEGURETAT DE COMPTES D'USUARIS

Ara que ja tenim coneixements sobre la gestió d'usuaris i grups, podem veure mètodes per intentar reduir, en mesura del possible, uns dels forats de seguretat més importants de tots els equips informàtics, les contrasenyes dels usuaris del sistema.

Aquestes contrasenyes, si no posem normes, son normalment massa "dèbils" i fàcils d'esbrinar a través d'un atac de diccionari[38]. A més, molts cops, son capturades en altres equips del usuari, o en altres aplicacions, i com que molts cops els usuaris les utilitzen per a tot, proporcionen un gran nivell d'accés.

Abans de començar, doncs, insistir que una bona conscienciació d'un ús responsable de credencials als nostres usuaris, serà la millor eina per aconseguir un entorn de treball més segur.

8.1. DIRECTIVES DE CONTRASENYA A WINDOWS

Les directives de contrasenya als equips amb sistemes operatius de la família Windows és controlen com una política de configuració del sistema. Recordeu que per tal d'accedir al panell de control de la consola de polítiques em d'executar **gpedit.msc**.

Dins d'aquest consola de Microsoft la configuració de les directives de seguretat estaran associades a la branca de configuració del equip. Dins d'aquesta accedirem a la **configuració de seguretat** on podrem trobar les configuracions relatives a les directives de comptes d'usuari.

A la Figura | 20 veiem les sis configuracions que podem editar per forçar l'ús de contrasenyes fortes:

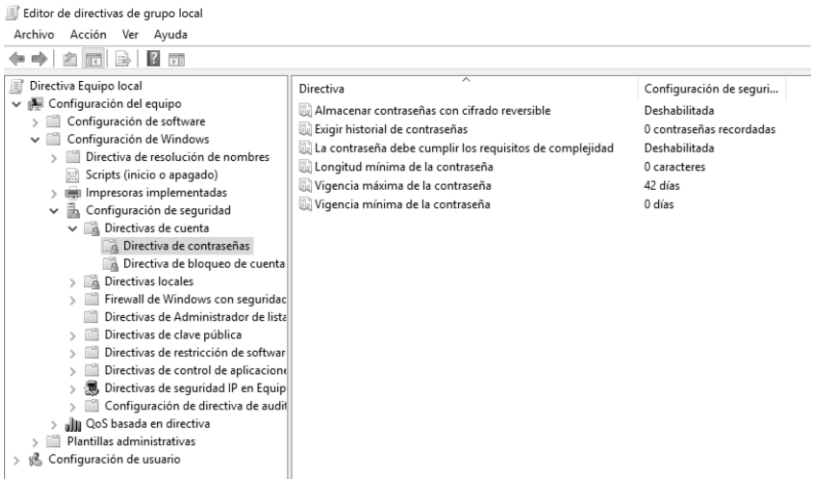


Figura 20 | Directives de contrasenya a Windows

[38] Un atac de diccionari és un mètode de cracking que consisteix en intentar esbrinar una contrasenya provant les paraules de diccionari. Aquest tipus d'atac sol ser més eficient que un atac de força bruta, ja que molts usuaris solen utilitzar una paraula existent en la seva lengua com a contrasenya per tal que la clau sigui fàcil de recordar, cosa que és una pràctica no recomanable. Els atacs de diccionari tenen poques possibilitats d'èxit amb sistemes que utilitzen **contrasenyes fortes** amb lletres en majúscules i minúscules barrejades amb números i amb qualsevol símbol.

Una de les primeres coses recomanables a habilitar la directiva anomenada **"La contraseña debe complir los requisitos de complejidad**". Amb això aconseguirem directament que l'usuari no pugui utilitzar contrasenyes febles ja que imposa els següents requisits:

- No pot contenir el nom d'usuari o parts del nom complert de l'usuari en més de dos caràcters consecutius.
- Ha de tenir una longitud mínima de 6 caràcters. És recomanable habilitar la directiva "**Longuitud mínima de la contraseña**" i augmentar aquest valor fins als 8 o 10 caràcters.
- Incloure al menys caràcters de 3 d'aquests 4 grups de caràcters:
  - Majúscules (A-Z)
  - Minúscules (a-z)
  - Dígits de base 10 (0-9)
  - Caràcters no alfanumèrics (#,$,%,@,etc.)

Cal tenir en compte que aquests requisits s'hauran de complir a partir d'ara quan creem qualsevol nova contrasenya o en qualsevol canvi que és realitzi, però que no afectarà a contrasenyes febles que ja puguin tenir els usuaris.

Amb l'acció d'exigir contrasenyes fortes haurem guanyat molt en seguretat, tot i això, podem anar un pas més enllà fent que les contrasenyes fortes escollides no siguin estàtiques i permanents, sinó que tinguin un caràcter temporal. Per aquest fi tenim les directives "**Vigencia màxima de la contraseña**" i "**Vigencia mínima de la contraseña**", que ens permetran establir un període de vigor de la contrasenya[39]. Així, per exemple, podrem imposar que una contrasenya introduïda per l'usuari s'hagi de canviar en un termini de 3 mesos, i al mateix temps, si volem, que no la pugui canviar durant el primer mes d'aquests 3 mesos.

Per últim, podem evitar que els usuaris estiguin reutilitzant antigues contrasenyes en cada canvi forçat per temps. A la directiva "**Exigir historial de contraseña**" podrem establir el número de contrasenyes que el sistema recordarà com utilitzades per un usuari i que no podrà reutilitzar fins que quedin alliberades.

ACT 18 | **Directiva de bloqueig de compte a Windows**
Un altre aspecte que pot millorar el nostre nivell de seguretat pel que fa a les contrasenyes del comptes d'usuari és aplicar directives per a bloquejar els usuaris que facin un número d'intents erronis en l'accés al equip.

Accedeix a les directives de comptes d'usuari i explica les 3 directives relacionades amb el bloqueig de comptes d'usuari. Fes algunes proves amb un usuari per veure els missatges que envia el sistema quan es bloqueja un usuari. Com es pot desbloquejar posteriorment?

[39] Recorda que en la configuració d'un usuari (Figura | 16) podem alliberar aquest període de vigència per un usuari concret marcant l'opció "La contraseña nunca expira".

8.2. DIRECTIVES DE CONTRASENYA A UBUNTU

Els sistemes operatius basats en Ubuntu permeten configurar una política de contrasenyes de forma fàcil i ràpida editant un document de text. Això si, per poder establir alguns dels paràmetres més avançats, relacionats amb la complexitat i/o evitar els atacs de diccionari, caldrà instal·lar alguna llibreria "extra" que ens faciliti la tasca.

Així doncs, el primer que farem serà executar `sudo apt install libpam-cracklib`. Un cop instal·lada la nova llibreria per a PAM[40], podrem configurar una política de contrasenyes que eviti l'ús de paraules del diccionari, la no reutilització de contrasenyes (historial), la complexitat d'aquesta, etc.

El fitxer per configurar la nostra política de contrasenyes s'anomena **common-password** i, com tots els fitxers de configuració del sistema, penja del directori /etc (/etc/pam.d/common-password). Dintre d'aquest fitxer haurem de trobar la línia **password required** i afegir just darrera que utilitzi la nova llibreria instal·lada (pam_cracklib.so). Només amb això aconseguirem que les contrasenyes no difereixin només d'un caràcter (per exemple de password a Password) o que no siguin al revés (de password a drowssap). També preveu contra atacs de diccionaris. A partir d'aquí podrem establir més opcions que considerem a la nostra política:

- **retry:** número d'intents de login abans de tornar un error.
- **minlen:** longitud mínima de la contrasenya.
- **difok:** nombre de caràcters que han de canviar entre una nova contrasenya i l'anterior.
- **ucredit**[41]**:** nombre de caràcters en majúscules que ha de contenir la contrasenya.
- **lcredit:** nombre de caràcters en minúscules que ha de contenir la contrasenya.
- **dcredit:** nombre de números que ha de contenir la contrasenya.
- **ocretid:** nombre de caràcters no alfanumèrics que ha de contenir la contrasenya.

Altres consideracions que hauríem de fer es si volem conserver un **historial de contrasenyes** o establir una **durada mínima i màxima** de cada canvi de contrasenya. Pel primer supòsit, la llibreria pam_cracklib consulta el historial a través del mòdul **pam_unix**. Per poder fer-ho primer hauríem de crear un fitxer anomenat **opasswd** per poder emmagatzemar les antigues contrasenyes dels usuaris. Per que sigui segur hauria de tenir uns privilegis iguals als de /etc/shadow (on es guarden les contrasenyes actuals), és a dir, amb permisos de lectura/escriptura només per al root[42].

---

[40] Linux Puggable Authentication Modules (PAM) proporciona uns mòduls per al support dinàmic de l'autenticació d'usuaris per a sistemes i aplicacions Linux. (www.linux-pam.org)

[41] Podem utilizar valors negatius i positius per establir la política de contrsenyes. Per exemple, ucredit=-3 indicaria que la contrasenya ha de tenir mínim 3 majúscules, en canvi, ucredit=+3 indicaria que la contrasenya pot tenir com a màxim 3 majúscules. Això, és extrapolable a lcredit, dcredit i ocredit.

[42] Creació d'un fitxer per emmagatzemar un historial de contrasenyes:

```
touch /etc/security/opasswd
chown root:root /etc/security/opasswd
chmod 600 /etc/security/opasswd
```

Un cop disposem d'un magatzem de contrasenyes cal indicar una nova línia de password required afegint ara darrera el mòdul pam_unix.so. A continuació indicarem opcions:

- **"tipus de xifrat":** si no s'especifica el fitxer contindrà contrasenya en text pla. Habitualment utilitzarem **md5** per indicar que es guardin amb un hash (xifrat).
- **rembember:** indicarà el nombre de contrasenyes a recordar.
- **use_authtok:** si afegim aquest forcem que es consulti l'historial al fer canvi de contrasenya. Paràmetre requerit, per tant.

Pel segon supòsit, establir una durada mínima i màxima per les contrasenyes, veurem que no és una funció actual de la nostra llibreria pam_cracklib, sinó que s'estableix com una condició a editar a **/etc/login.defs**[43]. Dintre d'aquest fitxer trobarem les variables del sistema PASS_MAX_DAY, PASS_MIN_DAY i PASS_WARN_AGE, que estabiran el màxims dies que pot durar una contrasenya, els mínims dies abans de poder tornar a canviar la contrasenya, i els dies abans que s'avisarà a l'usuari de que ha de canviar la contrasenya, respectivament. Aquestes configuracions només tindran efecte per als nous usuaris creats a traves de `useradd`. Per a usuaris que ja estan al sistema caldrà utilitzar un canvi de contrasenya a través de la comanda `passwd` amb els modificadors `-x#`,`-n#` i `-w#` (`#` serà el número que volem) per establir el màxim temps, mínim temps i avis abans que no caduqui, per la nova contrasenya del usuari.

ACT 19 | **Política de contrasenyes a Ubuntu**

Anem a treballar amb l'exposat anteriorment dissenyant una política de contrasenyes pel nostre sistema Ubuntu que compleixi les següents condicions:

- Ha d'utilitzar els paràmetres de seguretat que proporcional la llibreria pam_cracklib per defecte.
- Un usuari tindrà 3 opcions per ficar correctament la seva contrasenya.
- Aquesta tindrà una longitud mínima de 10 caràcters, dels quals només un ha de ser en majúscules i com a mínim 2 han de ser números.
- A més, s'ha de conservar un historial de les últimes 2 contrasenyes que no es podran reutilitzar.
- A més, la contrasenya caducarà cada mes, i s'avisarà 3 dies abans a l'usuari de que cal canviar-la.

Un cop fetes aquestes configuracions, crea un nou usuari i comprova que la teva política de contrasenyes funciona correctament. Afegim un punt extra per tal de que investiguis:

- Com puc aconseguir que en el meu sistema no estigués permesa específicament una contrasenya concreta, per exemple: *asWd345jku*, que tindria que ser vàlida segons la política de contrasenyes anteriors?

[43] Recorda que el fitxer /etc/login.defs inclou els paràmetres per defecte que adquireixen els perfils d'usuari en ser creats.

PT 4 | CONFIGURACIÓ DE XARXA I CONNECTIVITAT DE SISTEMES OPERATIUS

En finalitzar aquesta pràctica l'alumnat ha de ser capaç de configurar una targeta de xarxa en els entorns dels sistemes Windows i Ubuntu actuals, permetent la creació d'una xarxa LAN entre les seves màquines virtuals.

OBJECTIUS

- Configurar targetes de xarxa en mode gràfic en sistemes Windows i Ubuntu.
- Configurar targetes de xarxa per via de comandes en sistemes Windows i Ubuntu.
- Comprovar la visibilitat entre diferents màquines a una LAN a través de la seva IP.
- Buscar, analitzar i interpretar la documentació tècnica necessària.
- Realitzar manuals tècnics dels procediments realitzats.

Configuració de xarxa en entorns Windows

Per tal de configurar la xarxa en Windows el més habitual és accedir al "**Centro de redes y recursos compartidos**" del Panel de Control seleccionant "Cambiar configuración del adaptador". Aquí trobarem tots els adaptadors de xarxa disponibles per aquell equip i podrem accedir a les propietats de cadascun d'ells. Dins d'aquestes propietats es troba la configuració del protocol TCP/IPv4 on podrem establir si volem obtenir la nostra direcció IP de manera dinàmica (a través d'algun servidor DHCP) o si la volem establir nosaltres de manera manual.

Abans de posar en marxa la teva màquina virtual **VM_w10** estableix a la configuració de xarxa de la màquina virtual que treballarà en mode "Xarxa Interna". Quines màquines de la xarxa es podrien connectar amb la màquina virtual VM_w10 llavors?

Posa en marxa la màquina virtual **VM_w10** i estableix una IP estàtica amb els següents paràmetres:

- Direcció IP: 192.168.XX.100 (amb XX el teu número d'alumne).
- Màscara de xarxa: 255.255.255.0
- Porta d'enllaç: 192.168.XX.1

Quants bits de xarxa utilitzem? Quants host podrem arribar a connectar a aquesta LAN?

Ara configurarem la màquina virtual **VM_w2016** per treballar en "Xarxa Interna". La posarem em marxa i configurarem la seva IP estàtica, en aquest cas, a través del PowerShell. Per fer-ho accedirem a la consola del PowerShell amb privilegis d'administrador i executarem en la comanda: `Get-NetIPInterface`. Quin resultat obtenim? Localitza el número d'adaptador de xarxa que vols configurar a la columna ifIndex.

Autor | RAFAEL GARCÍA SUÁREZ
Contacte | rgarc259@xtec.cat

Ara ja sabem quins son els nostre adaptadors de xarxai quin volem configurar (Y), podrem configurar la nostra IP estàtica al adaptador corresponent executant:

```
New-NetIPAddress -InterfaceIndex Y -IPAddress 192.168.XX.101 -PrefixLength 24 -DefaultGateway 192.168.XX.1
```

Recorda substituir la Y pel número d'adaptador a configurar i XX pel teu número d'alumne.

Comprova la teva configuració anterior a través de la comanda ipconfig.

Un mètode alternatiu és utilitzar una eina interactiva del PowerShell anomenada sconfig. Executa-la i explica com canvies la teva IP a 192.168.XX.1/24.

Configuració de xarxa en entorns Ubuntu

En Ubuntu també podrem configurar la nostra IP de xarxa tant a través de l'entorn gràfic (si tenim) com a través de la línia de comandes, o fins i tot, editant directament el fitxers de configuració del sistema.

Començarem configurant la xarxa de la nostra màquina virtual **VM_ud18.04** per tal de treballar en "Xarxa Interna". Posarem en marxa la màquina virtual i ens dirigirem a la cantonada superior dreta per accedir fàcilment al panell "Configuración de red cableada". Comprova que estigui connectada i a través del botó de propietats (en forma de engranatge) accedeix a la configuració IPv4 i estableix de forma manual aquests paràmetres:

- Direcció IP: 192.168.XX.200 (amb XX el teu número d'alumne).
- Màscara de xarxa: 255.255.255.0
- Porta d'enllaç: 192.168.XX.2

Aplica els canvis, accedeix a un terminal i executa ifconfig. Tens la IP que has configurat? Reinicia el teu sistema i torna a comprovar-ho. A que es degut això? Com podríem actualitzar la configuració de xarxa sense reiniciar tot el sistema?

Ara configurarem la xarxa de la màquina virtual **VM_us18.04** per tal de que estigui en mode "Xarxa Interna". Posarem en marxa la màquina virtual i provarem de configurar la nostra xarxa a través de la edició del fitxer de configuració de xarxa del sistema[44].

[44] Potser algun de vosaltres està familiaritzat amb el fitxer /etc/network/interfaces, però aquest ha estat substituït des de la versió 17.10 i ja no és el mètode per defecte a la versió LTS actual. Si ho intentem visualitzar ens trobaríem amb el següent missatge:

```
user@ubuntu:~$ cat /etc/network/interfaces
# ifupdown has been replaced by netplan(5) on this system.  See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#    sudo apt install ifupdown
user@ubuntu:~$
```

Veiem que es pot rehabilitar com a mètode però està destinat a desaparèixer i per tant, no l'utilitzarem més.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

El fitxer de configuració de xarxa que utilitzarem està situat dintre de la carpeta **netplan** que penja de /etc. Aquest fitxer té una extensió .yaml i si no existeix es pot generar amb la comanda `netplan generate`.

Cerca i obre el teu fitxer .yaml amb l'editor nano i privilegis de root, i fes que tingui el següent aspecte:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.XX.2/24]
      gateway4: 192.168.XX.2
```

Guarda la nova configuració surt i executa ifconfig. Ha canviat la IP? Reinicia el servei de xarxa amb la comanda `sudo netplan apply` i torna a comprovar.

Connectivitat de xarxa

Un cop hem configurat unes IP estàtiques dins de la xarxa LAN interna 198.162.XX.0 anem a comprovar que tenim connectivitat entre les 4 màquines virtuals a través de les seves IP.

Començarem provant la connectivitat de les nostres màquines Ubuntu. Connecta les dues màquines virtuals **MV_ud18.04** i **MV_us18.04** i executa un terminal en cadascuna. Utilitza la comanda ping en cadascuna fins a la IP de l'altra màquina virtual i comprova que els paquets contesten a la petició d'eco.

Ara comprovarem la connectivitat de les màquines virtuals de Windows (**MV_w10** i **MV_w2016**) fent el mateix procés. Algun problema?

Si es perden paquets es degut a que el Firewall de Windows bloqueja les peticions de ping com a mesura de seguretat contra els atacs de ping massius ("ping flood") o contra atacs on s'envien paquets massa grans ("ping de la mort")[45]. Per això, i per tal de comprovar la connectivitat, podríem desactivar temporalment el Firewall de Windows però sembla, d'entrada, una mesura massa dràstica.

Accedeix a la configuració del Firewall i permet les regles d'entrada i sortida corresponents a l'entrada/sortida dels paquet ICMPv4 (els que enviaran els nostres ping). Torna a provar la connectivitat de les màquines virtuals.

Per últim pots comprovar connectivitats creuades d'alguna de les màquines d'Ubuntu a una de les màquines Windows i viceversa. No t'hauria de suposar cap problema ja que en enviar la petició d'eco el ping només necessita una IP i és indiferent de quin sistema operatiu i estigui darrera.

[45] Molts d'aquests tipus d'atacs son antics i molts sistemes implementen solucions per tal d'evitar-los. Tot i això, encara avui alguns dels atacs DoS i DDos ("denegació del servei") més populars es basen en d'inundació de paquets ICMP.

RESULTATS

Arribat el final de la pràctica l'alumnat haurà de saber configurar IP estàtiques a les seves màquines virtuals, així com conèixer els mètodes que permeten la comprovació de la connectivitat dins d'una xarxa.

El seu escenari de màquines virtuals haurà quedat amb les següents direccions IP:

- **MV_w10:** 192.168.XX.100/24
- **MV_W2016:** 192.168.XX.1/24
- **MV_ud18.04:** 192.168.XX.200/24
- **MV_us18.04:** 192.168.XX.2/24

A més, haurà de tenir un document on s'hagin resolt les diferents preguntes plantejades a la pràctica amb captures de pantalla dels resultats. Cal lliurar aquesta documentació a través del **Moodle del curs** dins del **termini establert**.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**

PT 5 | SISTEMA DE NOMS DE DOMINI ALS DIFERENTS SISTEMES OPERATIUS

En finalitzar aquesta pràctica l'alumnat haurà aprés els conceptes bàsics al voltant del sistema de noms de domini (DNS) i haurà posat en marxa aquest servei als sistemes operatius de Windows i Ubuntu en les seves versions per a equips servidors.

OBJECTIUS

- Estudiar els conceptes teòrics bàsics sobre el sistema de noms de domini.
- Configurar Windows Server 2016 per tal de que funcioni com a servidor DNS.
- Configurar Ubuntu Server 18.04 per tal de que funcioni com a servidor DNS.
- Comprovar la funcionalitat dels sistemes de noms de domini promocionats i configurats.
- Buscar, analitzar i interpretar la documentació tècnica necessària.
- Realitzar manuals tècnics dels procediments realitzats.

Conceptes teòrics del sistema de noms de domini

El **sistema de noms de domini** (DNS, del anglès Domain Name System) és un sistema de nomenclatura jeràrquic descentralitzat per a dispositius connectats a xarxes IP (ja sigui Internet o una LAN privada). Aquest sistema associa informació variada amb el nom de domini assignat a cadascun dels participants.

La seva funció més important es "traduir" noms intel·ligibles per les persones composats per identificadors binaris que s'associen als components connectats a la xarxa, amb el propòsit de poder-los localitzar i adreçar de manera més fàcil i global.

Un equip que funcioni com a servidor DNS utilitzarà una base de dades distribuïda i jeràrquica que emmagatzema informació associada a noms de dominis en xarxes com Internet. Com a base de dades el DNS es capaç d'associar diferents tipus d'informació a cada nom, però l'ús més comú es l'assignació de noms de dominis a adreces IP i la localització dels servidors de correu electrònic de cada domini.

Així doncs, si et parlo de l'adreça 216.58.210.163 possiblement no et dirà res en especial, tot i que accedeixes diàriament a ella (Google). Òbviament, és més fàcil de recordar el nom, i a més, l'adreça IP podria canviar en qualsevol moment per qualsevol motiu, sense tenir que canviar el nom associat, proporcionant un mètode més fiable d'accés. Per poder operar amb el sistema DNS s'utilitzen tres **components** principals:

- Els **clients fase 1**: un programa client DNS es el que s'executa en un equip d'un usuari quan es genera una petició DNS, per exemple, al escriure una pàgina web al navegador es sol·licita la traducció DNS d'aquell domini.
- Els **servidors DNS**: son els encarregats de respondre a les peticions dels clients. Poden fer-ho per si mateixos, o en alguns casos, demanar a altres servidors DNS l'adreça sol·licitada.
- Les **zones d'autoritat**: és una part de l'espai de noms de domini sobre la que és responsable un servidor DNS concret. Un servidor DNS pot tenir autoritat sobre varies zones.

Autor | RAFAEL GARCÍA SUÁREZ
Contacte | rgarc259@xtec.cat

Un **nom de domini** usualment consta de dos o més parts (o "etiquetes"), separades per punts quan les escrivim en forma de text. Per exemple, *equip1.empresa.tipus.com*. (Figura | 21).

A l'etiqueta ubicada més a la dreta (a l'exemple *com*) és anomenada **domini de nivell superior** (top level domain). Cada etiqueta a l'esquerra del domini de nivell superior especifica una subdivisió o **subdomini** (a l'exemple *tipus*). Veiem que de la mateixa forma *empresa* seria un subdomini del subdomini *tipus*, establint així l'organització jeràrquica del sistema DNS.

Finalment, la part més a l'esquerra del domini (*equip1*) expressa normalment el **nom de la màquina** (hostname) tot i que potser només especifica una manera de crear una ruta lògica a la informació requerida i no es refereix a una màquina física en particular.

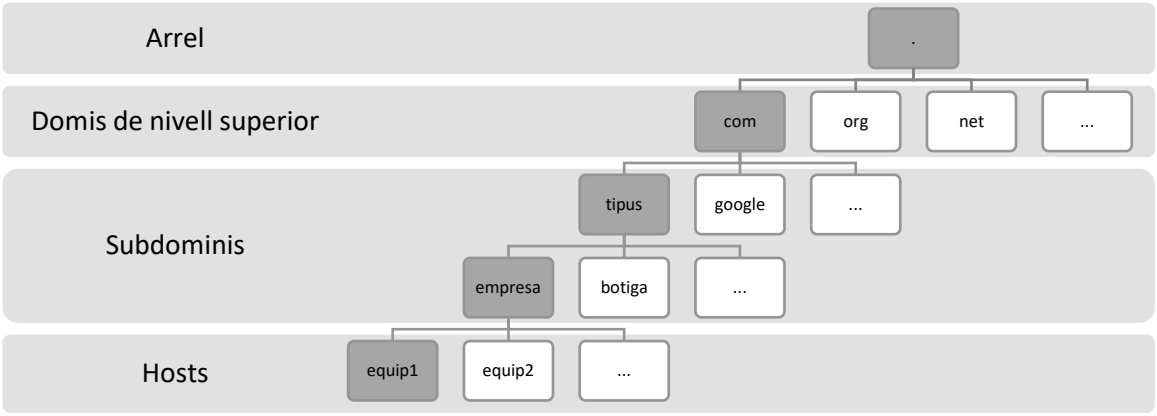


Figura 21 | Exemple de l'organització jeràrquica del sistema DNS

Per resoldre aquests nom de domini existeixen dos tipus de consultes: **resolució iterativa** i **resolució recursiva**.

Cerca informació relativa a cadascun d'aquests tipus de consulta i realitza un esquema de funcionament.

A l'hora de configurar un servidor DNS (indiferentment de quin sigui el sistema operatiu que el suporta) cal tenir en compte la nomenclatura que reben els diferents **tipus de registres** de la base de dades DNS per tal de poder referenciar-se als diferents tipus d'elements del sistema:

- **A = adreça:** s'utilitza per traduir noms d'equips a adreces IPv4
- **AAAA = adreça:** és equivalent a l'anterior però treballa amb adreces IPv6
- **CNAME = nom canònic:** s'utilitza per a noms addicionals o alies, per exemple, si un mateix servidor te diversos serveis (FTP i servidor Web) i una mateixa IP, o en un servidor HTTP amb diferents noms per un mateix host.
- **NS = servidor de noms:** defineix l'associació que existeix entre un nom de domini i els servidors de noms que emmagatzemen la informació d'aquell domini.
- **MX = intercanvi de correu:** associa el nom de domini a una llista de servidors de correu.
- **PTR = punter:** també conegut com a registre invers, funciona a la inversa que els registres del tipus A (o AAAA), tradueix IPs en noms de domini.
- **SOA = autoritat de zona:** proporciona informació sobre el servidor DNS primari de la zona.

Per últim, mencionar alguns temes vinculats a la **seguretat del sistema DNS**. Originalment, com en molts altres protocols de xarxa, les preocupacions de seguretat no van ser considerades importants ja que no es concebia la emergent xarxa d'Internet tal i com la veiem avui dia on cal implementar bones mesures de seguretat per protegir la integritat de les dades i l'autenticació d'usuaris.

Així doncs, es van començar a descobrir i explotar vulnerabilitats per par d'usuaris maliciosos. Per exemple, els **atacs d'enverinament de "caché" DNS**, en el que les dades son distribuïdes als resolvedors de "caché" (en català memòria cau) fent-se passar per un servidor d'autoritat d'origen, contaminant la memòria dels servidors amb informació potencialment falsa i amb llargs temps d'expiració, aconseguint d'aquesta manera que les sol·licituds d'aplicacions legitimes puguin ser redirigides a equips de xarxa amb continguts maliciosos.

Això es degut a que les respostes DNS tradicionalment no estaven firmades criptogràficament, permetent moltes possibilitats d'atac. Les **extensions de seguretat DNS** (DNSSEC) modifiquen el DNS per afegir la possibilitat de tenir respostes signades criptogràficament. Altres alternatives plantejades son **DNSCurve** o les extensions **TSIG**.

Altres vulnerabilitats que s'han explotat son atacs del tipus **phising**[46] intentant introduir a la resolució de noms entrades amb noms de serveis similars i enganyosos, per exemple, paypal.com i paypa1.com podrien induir a confusió i més segons el tipus de lletra utilitzat (`paypal.com paypa1.com`). Alguna tècnica per intentar reduir l'impacte d'aquests atacs es utilitzar el **FDNS invers de confirmació avançada** (FCrDNS).

Cerca informació més detallada sobre els sistemes DNSSEC, DNSCurve i FCrDNS per tal d'entendre com ens ajuden a millorar la seguretat dels nostres sistemes de noms de domini.

Configuració de Windows Server 2016 com a servidor DNS

Actualment la nostra màquina virtual **VM_w2016** és només un equip que corre el sistema operatiu Windows Server 2016 però que no te cap rol (o funció) de servidor assignada. Posa en marxa l'equip i comprova que tens fetes les següents configuracions:

- Nom de l'equip: wserverXX (amb XX el teu numero d'alumne)
- IP estàtica: 192.168.XX.1/24

Fetes aquestes comprovacions anem a indicar que el servidor DNS d'aquest equip serà ell mateix assignant-li la IP de localhost (127.0.0.1) al servidor DNS primari. Fes-ho a través de l'entorn gràfic.

Anem ara a afegir el rol de servidor DNS al nostre equip wserverXX. Ves a "Administrador del servidor" i cerca a la part superior la opció "Administrar" i "Agregar roles y características". Un cop aquí s'obrirà un assistent. Escollirem el tipus d'instal·lació anomenada "Instalación basada en caractrísticas o reles".

Genera a partir d'aquí un manual pas a pas, amb captures de pantalla, de com afegeixes el sistema DNS com a rol del servidor. Caldrà reiniciar l'equip al finalitzar l'assistent (o pot fer de forma automàtica).

[46] Els atacs de Phishing son coneguts també com atacs de **suplantació d'identitat** i estan basats en la enginyeria social intentant aconseguir informació confidencial (contrasenyes, targetes de crèdit, etc.) fent-se passar per una empresa o persona que aparenti una confiança a l'usuari.

En aquest moment dins del panell de "Administrador del servidor" ja veurem que ha aparegut un apartat dedicat al servidor de noms de domini, i si funciona correctament, estarà de color verd.

Anem a configurar el nostre DNS. Ves des de "Administrador del servidor" a "Herramientas" i "DNS". S'obrirà una finestra on veurem el nom del nostre servidor (wserverXX) i sota els paràmetres configurables per aquest.

Començarem per l'apartat de "Zonas de búsqueda directa" que ens ha de permetre crear la nostra zona de cerca principal. Fes clic dret i escull "Zona nueva" per llançar l'assistent. Documenta aquest procés de creació de la zona directa principal tenint en compte que la zona es dirà **wserverXX.sis** (XX el teu numero d'alumne) i que no admetrem actualitzacions dinàmiques ja que es tractarà d'un sistema DNS per una xarxa privada.

Anem ara a crear una nova zona de cerca en aquest cas inversa basada en IPv4. Documenta el procés tenint en compte la xarxa on treballes (192.168.XX.0) i el no admetre les actualitzacions dinàmiques per l'exposat anteriorment.

Amb les dues zones creades (directa i inversa) anem a fer algunes configuracions. Crea a la zona directa un nou registre tipus A amb nom *servidor* amb la IP 192.168.XX.1 (no has de crear el PTR associat, o farem manualment). Després crea un nou registre tipus CNAME per tal de que el nostre servidor respongui també a *alias.wserverXX.sis*.

A la zona inversa hauràs de crear un nou registre del tipus PTR per tal de vincular la adreça 1.XX.162.198.in-addr.arpa al nostre primer registre tipus A (*servidor*).

En aquest moment tindrem una zona directa (*wserverXX.sis*) amb un registre tipus A (*servidor*) i un registre tipus CNAME (*alias*). A més d'un punter de cerca inversa (1.XX.168.192.in-addr.arpa). Anem a comprovar la seva funcionalitat des de les màquines virtuals **VM_w10** i **VM_ud18.04**.

Posa en marxa la màquina virtual **VM_w10** i configura el seu DNS primari amb la IP del nostre nou servidor DNS (198.162.XX.1). Fes-ho a través del PowerShell (recorda la comanda sconfig de la PT 3).

Ara executarem la comanda la comanda **nslookup** sense paràmetres. En el prompt[47] de la comanda has d'indicar quina sortida proporciona per els següents arguments:

- servidor.wserverXX.sis (XX el teu numero d'alumne)
- alias.wserverXX.sis
- 198.162.XX.1

Funciona tot com esperaves?

Torna a realitzar aquest procés de comprovació des de la màquina virtual **VM_ud18.04**, configurant el seu DNS primari amb la IP 192.168.XX.1 (paràmetre `nameservers` al fitxer .yaml) i comprova que obtens els mateixos resultats amb la comanda nslookup.

[47] Prompt fa referència al caràcter o caràcters que es mostren a una línia de comandes per indicar que està a l'espera d'ordres.

Configuració d'Ubuntu Server 18.04 com a servidor DNS

Per poder convertir el nostre equip anomenat userverXX (XX el teu número d'alumne) instal·lat a la màquina virtual **VM_us18.04** el primer que ens caldrà és instal·lar el paquet DNS per Ubuntu, anomenat **bind9.** Posa en marxa la màquina i comprova que té la IP estàtica 192.168.XX.2. Amb aquesta IP no podrem descarregar ni instal·lar cap paquet (ja que es una xarxa interna privada), i per tant, cal modificar els paràmetres de xarxa de la màquina virtual per treballar en una xarxa NAT i posteriorment editar el fitxer .yaml per tal d'obtenir una adreça IP automàtica a través de DHCP [48].

Un cop tenim de nou connexió amb l'exterior a la nostra màquina virtual **VM_us18.04** podrem instal·lar els paquets necessaris per treballar amb el sistema de noms de domini al nostre servidor Ubuntu:

```
sudo apt install -y bind9 bind9utils bind9-utils dnsutils
```

Un cop instal·lats els paquets, haurem de retornar a la nostra configuració amb IP estàtica (192.168.XX.2) per tal de que el servidor sigui localitzable (un servidor DNS no pot tenir una IP dinàmica). Aprofita per afegir l'adreça de local host 127.0.0.1 com servidor primari DNS (ell mateix).

Ara si estem preparats per configurar el sistema de noms de domini a Ubuntu (bind9). Els fitxers de configuració, com sempre, penjaran de /etc, concretament /etc/bind/. Dintre trobarem els fitxers de configuració i els fitxers de cerca de zones. El fitxer de configuració global es diu **named.conf** tot i que nosaltres utilitzarem un anomenat **named.conf.local** per la nostra xarxa DNS local.

Obre amb un editor, i amb permisos de root, el fitxer /etc/bind/named.conf.local i escriu el següent per configurar una zona de cerca directa anomenada userverXX.sis (XX el teu número d'alumne):

```
zone "userverXX.sis" IN {                          #especifica el nom del domini
        type master;                               #especifica que es un DNS primari
        file "/etc/bind/directa.userverXX.sis.db   #futur fitxer de cerca directa
        allow-update { none; }                     #no cal ja que es el DNS primari
};
```

Al mateix temps podem crear una zona de cerca inversa, a continuació del fitxer, i amb un format molt similar:

```
zone "XX.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/inversa.userverXX.sis.db
        allow-update { none; }
};
```

[48] Afegeix al fitxer .yaml els paràmetres `dhcp4: yes` i `dhcp6: yes` sota l'etiqueta `ethernets:`. A més comenta les línies (#) de configuració de paràmetres de IP estàtica (millor això que borrar-les i haver de tornar a escriure-les més endavant). Recorda executar `sudo netplan apply` per reiniciar el servei de xarxa amb els nous paràmetres.

Ara ja tenim definides les nostres zones de cerca directa i cerca inversa, i hem indicat que farem la configuració d'aquestes dues zones als fitxers *directa.userverXX.sis.db* i *inversa.userverXX.sis.db* respectivament.

Partint del fitxer /etc/bind/db.local com a exemple, farem una primera copia per crear el fitxer de configuració de cerca directa:

```
sudo cp /etc/bind/db.local /etc/bind/directa.userverXX.sis.db.
```

Editarem el fitxer resultant de la copia fent les següents modificacions:

- El registre SOA ha d'indicar "userverXX.sis." com a domini i no "localhost.".
- El número "; Serial" s'ha de modificar per un número més gran.
- El registre NS cal tornar a substituir "localhost." per "userverXX.sis.".
- El registre A ha de ser la nostra IP estàtica (192.168.XX.2).
- No cal especificar cap registre AAAA ni MX.
- Afegirem un registre tipus CNAME anomenat "alias" (`alias IN CNAME userverXX.sis`).

Un cop modificat, i abans de configurar la zona de cerca inversa, anem a comprovar el que hem fet fins ara. El primer de tot es verificar la sintaxis dels fitxers editats:

- Primer executem: `sudo named-chekconf` per comprovar la sintaxi dels fitxers named.conf *.
- Si no retorna errors continuem comprovant el fitxer de configuració de zona de cerca directa: `sudo named-chekzone userverXX.sis /etc/bind/directa.userverXX.sis.db.`
- Si ens retorna una sortida amb el nom de la zona, el número de Serial que hem modificat i un OK és que ho hem fet correctament.

Ara que sabem que ho tenim correcte, reiniciem el servei de noms de domini per carregar els canvis: `sudo systemctl restart bind9`. Després aprofitem per habilitar el servei cada cop que iniciem l'equip: `sudo systemctl enable bind9`. Per últim veiem el seu estat actual: `sudo systemctl status bind9` (comprova que està en mode *active (running)*).

Tot està configurat i en marxa. Arranca la màquina virtual **VM_ud18.04** per verificar que funciona tal i com desitgem. El primer es canviar el servidor primari DNS de l'equip uclientXX (actualment està configurat de l'apartat anterior com 192.168.XX.1) fent que correspongui amb la IP 192.168.XX.2.

Ara utilitzarem la comanda `dig userverXX.sis` [49] que ens hauria de retornar en alguna línia de la seva sortida una vinculació entre nom de domini i la seva IP. Prova també amb `dig alias.userverXX.sis`.

Ara és el torn d'investigar una mica i veure com has de configurar el fitxer *inversa.userverXX.sis.db* per configurar la zona de cerca inversa. Comença creant el fitxer a partir d'una copia del fitxer /etc/bind/db.local, tal com hem fet abans, recorda de comprovar la seva sintaxis després de modificar-lo (named-checkzone), de reiniciar el servei bind9 i finalment comprovar els resultats des de l'equip uclientXX en aquest cas amb la comanda: `dig -x 192.168.XX.2`.

[49] Si la sortida del la comanda indica "command not found" et caldrà instal·lar el paquet **bind-utils** (recorda que hauràs de canviar la xarxa a NAT i modificar el fitxer .yaml per fer-ho, i desfer aquests canvis per tornar a la IP estàtica privada de la xarxa interna 192.168.XX.0 per continuar després amb la pràctica).

RESULTATS

Arribat el final de la pràctica l'alumnat haurà après a configurar dins de la seva targeta de xarxa el seu DNS primari. A més sabrà com convertir equips amb sistemes servidors de les famílies de Windows i Ubuntu en servidors de noms de domini (DNS).

Al seu escenari de màquines virtuals, les màquines **VM_w2016** i **VM_us18.04** seran servidors DNS dels noms wserverXX.sis i userverXX.sis respectivament. Les màquines **VM_w10** i **VM_ud18.04** tindran establerts els servidors DNS primaris en els anteriors, respectivament.

A més, haurà de tenir un document on s'hagin resolt les diferents preguntes plantejades a la pràctica amb captures de pantalla dels resultats. Cal lliurar aquesta documentació a través del **Moodle del curs** dins del **termini establert**.

Autor | **RAFAEL GARCÍA SUÁREZ**
Contacte | **rgarc259@xtec.cat**