



GUIA DE BENVINGUDA PER ALMUNES EN PRÀCTIQUES D'UN CFGS D'ASIX

FONAMENTS DE MAQUINARI

MANAR NEKHAICH EL WIHRANI

OCTUBRE 2024



ÍNDEX

1.	INTRODUCCIÓ.....	2
2.	DIFERÈNCIES	3
2.1	ANTIVIRUS	3
2.1.1	Què és un antivirus ?	3
2.1.2	Per a què serveixen els antivirus informàtics	3
2.1.3	Tipus d'antivirus informàtics	4
2.2	FIREWALL	4
2.2.1	Què és un Firewall ?	4
2.2.2	Per a què serveixen els Firewall	5
2.2.3	Tipus de Firewall.....	5
2.3	SPYWARE	7
2.3.1	Què és un "Spyware"	7
2.3.2	Tipus de "Spyware"	7
2.3.3	Com es poden eliminar els "Spyware"	8
3.	IMPORTÀNCIA DE LES COPIES DE SEURETAT	10
3.1	TIPUS PRINCIPALS.....	10
4.	GESTIÓ DE DISCOS	12
4.1	Definició de Partició i Tipus de Particions.....	12
4.2	Principals Sistemes d'Arxius	12
4.3	Eines de Gestió de Discs Durs	13



1. INTRODUCCIÓ

En aquest projecte simularem l'arribada d'un nou alumne al nostre centre escolar, que s'ha inscrit concretament al cicle formatiu de grau superior d'Administració en sistemes i xarxes, en perfil de ciberseguretat (ASIX).

Després d'haver tingut una reunió amb el director del centre i rebre la notícia del nou alumne hem de preparar la seva arribada. El nostre objectiu es crear un document que serà lliurat al nou alumne. Aquest document consta d'un conjunt de conceptes bàsics que cal que integri en els seus coneixements per tal de poder iniciar i treballar en les seves tasques. Conceptes com “*antivirus, Firewall, spyware*”, la importància de les còpies de seguretat i els seus tipus principals, a més a més de com és gestionen els discos.

Per tant, la base d'aquest projecte és poder crear un informe que contingui definicions i termes necessaris per a que el nostre nou alumne sigui capaç de treballar i desenvolupar noves habilitats en aquest camp d'informàtica, concretament en l'administració en sistemes i xarxes. D'aquest mode, cara al futur, podrà augmentar el seu coneixement i desenvolupar el seu coeficient intel·lectual per poder aportar noves tècniques o eines a la societat actual.



2. DIFERÈNCIES

2.1 ANTIVIRUS

2.1.1 Què és un antivirus ?

Un antivirus és una mena de programari que serveix per evitar, cercar, detectar, prevenir i eliminar d'un sistema computat els virus informàtics.


Els programes de protecció contra virus ajuden a protegir els teus arxius i maquinari de (malware), com cucs, troians i programes espia, i a més poden oferir protecció addicional, com barreres de protecció (firewall) personalitzaves i bloquejos de llocs web. Aquests programes analitzen arxius i aplicacions per identificar i eliminar codi nociu. Exemples comuns d'antivirus inclouen; “**McAfee Total Protection**”, “**Norton Antivirus**”, entre d'altres. Un cop instal·lats, la majoria dels programaris antivirus s'executen automàticament en segon pla per brindar protecció en temps real contra atacs de virus.

En resum , es tracta d'un programa que busca solucions als danys causats per aquestes formes invasives de programari, la presència del qual al sistema no sol ser detectable sinó fins que se n'evidencien els símptomes.

2.1.2 Per a què serveixen els antivirus informàtics

En l'actualitat, els antivirus serveixen per a més que simplement escanejar i desinfectar una màquina que ha contret un virus informàtic . En general ofereixen serveis de monitorització actiu, per impedir l'accés total d'un document infectat al sistema, bloquejar pàgines web insegures i eliminar fitxers riscosos un cop ingressin al computador . Això rep el nom de protecció activa.

D'altra banda, els antivirus informàtics lidien també amb altres eines de programari, com el “*spyware*”, “*malware*” o “*rootkits*”, i fins i tot d'intents de hackeig. Per això té



un *talla focs*; programari de bloqueig de connexions remotes; i una base de dades que es basa en una base de definicions de virus, que és una mena d'enciclopèdia dels virus més comuns.

2.1.3 Tipus d'antivirus informàtics


Cal destacar els següents tipus d'antivirus informàtic, d'acord amb el funcionament:

- **Antivirus d'identificació.** Són aquells que rastregen seqüències actives associades a determinats virus, però no són gaire efectius a l'hora de lidiar amb el programari indesitjat. Tenen la virtut de ser molt lleugers, alguns s'executen des de la xarxa .
- **Antivirus descontaminadors.** Normalment venen instal·lats al sistema com qualsevol altre programari d'aplicació , aquests programes poden activar-se amb la finalitat de revisar el contingut complet de l'ordinador a la recerca de virus. Si n'hi ha, aleshores, es procedeix a la desinfecció i, si no és possible, a la quarantena o l'esborrat.
- **Antivirus de protecció a temps real.** Són aquells que requereixen protecció constant al sistema, sense necessitat de dur a terme una revisió exhaustiva, sinó revisant tots els fitxers i connexions entrants i sortints. Aquests antivirus solen estar combinats amb funcions descontaminadores.

2.2 FIREWALL

2.2.1 Què és un Firewall ?

Els firewalls són considerats com fronteres o portes que administren el flux de l'activitat web que es permet o prohibeix en una xarxa privada. El terme prové del concepte de parets físiques que actuen com a barreres per alentir la propagació del foc fins que els serveis d'emergència el poden extingir. Tenen com a objectiu evitar l'accés no autoritzat, tant a la xarxa com a les aplicacions. Els firewalls poden ser de programari, com el **Firewall de Windows**, o de maquinari, com els que es troben en routers.



Els *firewalls* creen “colls d'ampolla” per canalitzar el trànsit web. En aquests punts, es fa una revisió d'un conjunt de paràmetres programats i s'actua en conseqüència. Alguns tallafocs també fan un seguiment del trànsit i les connexions als registres d'auditoria per consultar el que s'ha permès o bloquejat.

Normalment, els *firewalls* s'utilitzen per delimitar les fronteres d'una xarxa privada o els dispositius host. Per tant, són una eina de seguretat que s'inclou a l'àmplia categoria del control d'accés dels usuaris. Aquestes barreres en general es troben en dues ubicacions: en ordinadors específics a la xarxa o als ordinadors de l'usuari i en altres punts de connexió (hosts).

2.2.2 Per a què serveixen els Firewall


El funcionament del *firewall* es basa en regles de seguretat que defineixen quin tipus de trànsit pot passar i quin tipus de trànsit ha de ser bloquejat. El firewall actua com una barrera entre la xarxa de l'empresa i el món exterior, avaluant cada paquet de dades que ingressa o surt de la xarxa, determinant si és segur o no i bloquejant-lo si és necessari.

2.2.3 Tipus de Firewall

Els firewalls es poden classificar en diverses categories segons els seu funcionament i característiques. Trobem els firewalls de xarxes, d'aplicacions, els de pròxima generació, basats en hosts, al núvol i els de hardware i software. A més a més, cal destacar que els més comuns són el Firewall de xarxa i el Firewall de host.

1. Firewalls de xarxes

- **Firewalls de filtratge de paquets:** cal analitzar tots els paquets de dades interaccionen amb la xarxa, acceptant o bloquejant el tràfic segons els paràmetres predefinits.

- 
- **Firewalls d'estat:** aquest mantenen un registre sobre l'estat de les connexions i s'encarreguen de prendre decisions sobre el filtratge basat en l'estat de la connexió.

2. Firewalls d'aplicacions

- **Firewalls Proxy:** fan com d'intermediaris entre els usuaris i els servidors. S'ocupen d'analitzar el tràfic a nivell d'aplicacions i poden oferir funcions addicionals com la caché.
- **Firewalls de filtratge a nivell d'aplicació:** es centren en protocols concrets de l'aplicació, a més a més tenen la capacitat de bloquejar atacs com la injecció SQL.

3. Firewalls de pròxima generació (NFW)

El que fan es combinar funcions en un Firewall tradicional que té capacitats avançades com detecció d'intrusions, prevenció d'intrusions (IPS) i anàlisis de les aplicacions.

4. Firewalls basats en hosts

Acostumen a trobar-se instal·lats en computadores o servidors i controlen el tràfic que entra i surt d'aquests dispositius.

5. Firewalls als núvols

S'encarreguen de protegir els recursos que estan als núvols i oferir certs caràcters específics per a entorns virtuals, normalment amb la finalitat de tenir una solució àmplia de seguretat en el núvol.

6. Firewalls de hardware i software

- **Hardware:** dispositius físics que es posen entre la xarxa interna i l'accés a internet
- **Software:** programes instal·lats en servidors o dispositius individuals que actuen com Firewall.



2.3 SPYWARE

2.3.1 Què és un "*Spyware*"


Podem definir com a *spyware* un del atacs informàtics més comuns que un usuari d'internet pot patir. Acostumen a aparèixer com tipus de programari que s'instal·la a l'ordinador i aquests acostumen a ser ignorats, però, aquests programes comporten riscos greus i poden posar en risc la informació personal de l'usuari.

Quan el *spyware* està dins del dispositiu, recopila informació que després envia a tercers. Aquesta sol ser de caràcter personal: des de l'història de cerques fins a contrasenyes i comptes de correu electrònic, vulnerant la privadesa de l'usuari. El dany que pot causar varia segons el tipus de *spyware*: de vegades pot ser només una molèstia, però, en els casos més greus, pot fins i tot portar al robatori d'identitat.

Es molt complicat poder detectar-lo, ja que el programari es pot instal·lar al nostre dispositiu sense que nosaltres tinguem consciència. Normalment, solen estar incorporats a programes o fitxers que es descarreguen de la xarxa o fins i tot en fitxers adjunts de correu electrònic. És possible descobrir-ho, però, parant atenció a algun dels senyals que poden indicar la presència de *spyware*. Són senyals sobre problemes, com ara que l'ordinador funcioni excessivament lent, que apareguin icones desconegudes a les barres d'eines, que les cerques es redirigeixin o es facin mitjançant un cercador desconegut.

2.3.2 Tipus de "*Spyware*"

El *spyware* pot canviar i adaptar-se per poder afrontar les mesures de seguretat que venen integrades als sistemes operatius. Aquest fet fa que es compliqui establir una tipologia completa d'aquest tipus de programari. Entre els diferents tipus de *spyware* cal destacar els següents:


- 
- **Keyloggers** : el *keylogger*; un dels més perillosos; registra les tecles que prem l'usuari des del seu ordinador. El risc més gran és que les contrasenyes també poden quedar registrades quan s'introdueixen, com ara, quan es fa una compra amb una targeta de crèdit.
 - **Adware** : és el més comú i fa que apareguin constantment anuncis publicitaris a finestres emergents (els coneguts pop-ups). No només és molest, sinó que es podrà guardar i transmetre qualsevol informació que l'usuari ofereix sense la seva autorització només quan accedeixi a algun d'aquests llocs.
 - **Infostealers** : com el *keylogger*, opera sense que l'usuari s'adoni que està recopilant i transmetent la informació de l'ordinador. En aquest cas, emmagatzema totes les dades que s'introdueixen a l'ordinador: des del contingut multimèdia a l'historial de cerca, incloent-hi contrasenyes i comptes de correu electrònic.

2.3.3 Com es poden eliminar els "*Spyware*"

Encara que eliminar el spyware és complicat, cal prevenir el problema abans de que succeeixi. Podem evitar l'instal·lació d'aquest codi maliciós al nostre dispositiu, per això, cal mantenir el sistema operatiu i els navegadors actualitzats, evitar llocs web de descàrregues poc viables i realitzar anàlisis periòdicament.

A més a més, sabent que és difícil de detectar, es pot evitar la instal·lació a l'ordinador. Les millors alternatives són:

- **Utilitzar una eina antispymware** : aquestes eines analitzen l'ordinador per localitzar qualsevol tipus de spyware. Un cop es conclou l'anàlisi, es procedeix a eliminar-la. Aquests programes solen ser els més efectius per solucionar el problema.
- **Eliminació manual** : és més complicada a causa de l'esmentada capacitat que té aquest programari espia per amagar-se. Tot i això, si s'aconsegueix detectar, eliminar-lo farà que l'amenaça desaparegui.
- **Reinstal·lar el sistema operatiu** : si el programa antispymware no aconsegueix eliminar el problema, aleshores es pot formatar l'ordinador. Per tant, és important,



que abans de començar el procés, es faci la còpia de seguretat de totes les dades, ja que aquestes seran eliminades.



3. IMPORTÀNCIA DE LES COPIES DE SEURETAT

Les còpies de seguretat s'han de fer de manera continua, sobre tot d'aquells fitxers més importants per tal d'assegurar que les dades estan sempre protegides i accessibles en cas d'algun problema.

Una còpia de seguretat és la clonació de certa informació a la qual es pot accedir en cas de pèrdua de la original. Les còpies de seguretat són imprescindibles si es tracta d'informació sensible. A més a més, solen ser el mecanisme més útil amb que pot comptar una empresa. Això és degut a que aquestes poden patir un robatori de les seves dades i si estan emmagatzemades, és a dir, que tenen una còpia de seguretat no tindran problema a l'hora de recuperar aquestes.

Així mateix, la realització d'una còpia de seguretat del disc complet garanteix la protecció completa de totes les dades i la capacitat de restaurar el sistema totalment en cas d'una fallada greu. A Per tant, fer una còpia de seguretat ben planificada i executada és fonamental per a la seguretat de la informació.


3.1 TIPUS PRINCIPALS

Entre els diferents tipus de còpies de seguretat cal destacar els següents:

- **Còpia de seguretat completa:** s'encarrega de copiar totes les dades i informació en un altre suport; com ara cintes, dvd, discs durs, etc...per poder ser recuperats quan faci falta. Aquest procés es el més lent i ocupa molt espai.

Per tant, l'inconvenient que presenta aquest l'espai que ocupa i la despesa d'afegir- hi més suports, i l'altre es el temps que triga a fer les còpies de seguretat.

Per això es recomanable fer aquest tipus de còpia de manera puntual.

- 
- **Còpia de seguretat incremental:** consisteix a copiar totes les dades noves o modificades des de l'última còpia completa, a més a més redueix el temps i l'espai de còpia tot i que la recuperació pot significar un procés bastant lent.
 - **Còpia de seguretat diferencial:** de tots els tipus de còpies aquesta és l'opció més recomanada. Això es degut a que aquesta només realitza la còpia dels fitxers que hagin estat modificats des de la última còpia, sigui completa o diferencial.

L'avantatge d'aquest tipus de còpia és que es pot fer tantes vegades possibles degut a que l'augment d'emmagatzematge ens permet estalviar espai i ofereix major rapidesa.

Per realitzar aquest tipus de còpia de seguretat el programari compara les dates de modificació dels fitxers i només copia els fitxers amb data més recent .



4. GESTIÓ DE DISCOS

4.1 Definició de Partició i Tipus de Particions

Definim partició com al nom que rep una divisió lògica d'un disc dur. Aquesta permet separar l'espai d'emmagatzematge en parts diferents. És a dir, tenir diverses particions és com tenir diversos discs durs en un sol disc dur físic, cadascuna amb els seus sistemes de fitxers.


Les particions es poden utilitzar per a diverses finalitats. Pots tenir una dedicada a guardar dades sensibles amb mesures de seguretat que no interfereixin a la resta del sistema, així com còpies de seguretat. En alguns d'ells, com els basats en GNU/Linux, també es pot estructurar el disc en particions per als diferents tipus de fitxers que usa el sistema operatiu.

Hi ha dos tipus de particions, les primàries i les lògiques.

- **Partició primària:** són les divisions primàries del disc que depenen d'una taula de particions, i són les que detecta l'ordinador en arrencar, per la qual cosa és on s'instal·len els sistemes operatius. Hi pot haver un màxim de quatre, i pràcticament qualsevol sistema operatiu les detectarà i assignarà una unitat sempre que utilitzin un sistema de fitxer compatible.
- **Partició lògica :** són les particions que es fan dins d'una partició estesa. L'únic que es necessita és assignar-li una mida, un tipus de sistema de fitxers (FAT32, NTFS, ext2,...), i ja estarà a punt per ser utilitzada. Funcionen com si fossin dispositius independents, i pots utilitzar-la per emmagatzemar qualsevol fitxer.

4.2 Principals Sistemes d'Arxius

Entre els diferents sistemes d'arxius cal destacar els següents:

- 
- **NTFS (New Technology File System):** tracta del Sistema **d'arxius** que Microsoft utilitza en els seus sistemes Finestres **Windows des** d'èpoques remotes. Ofereix suport per a grans arxius, permisos de seguretat i recuperacions d'aquest en cas de pèrdues.
 - **FAT32 (File Allocation Table 32):** FAT32 és la versió de 32 bits del sistema d'arxius FAT (File Allocation Table). Un sistema d'arxius especifica el protocol per emmagatzemar i organitzar dades en un disc dur, incloent noms de fitxers i certs permisos. Tot i ser un sistema més antic és usat en unitats USB o targetes de memòria.
 - **EXT4 (Fourth Extended File System):** és el sistema de fitxers Linux natiu fet per superar els problemes de l'Ext3. El sistema de fitxers es va llançar per primera vegada com extensions d'Ext3, que eren compatibles amb versions anteriors. A més a més, és eficient i suporta grans volums i arxius.
 - **APFS (Apple File System):** Es utilitza en macOS i iOS, és capaç d'emmagatzemar en estat sòlid, amb característiques com xifrat i instantànies
 - **XFS:** És un sistema d'arxius de rendiment elevat, és perfecte per a servidor i grans capacitats de dades
 - **Btrfs (B-tree File System):** El B-tree Files System es modern i flexible, a més a més ofereix característiques com snapshot i la gestió de volums.

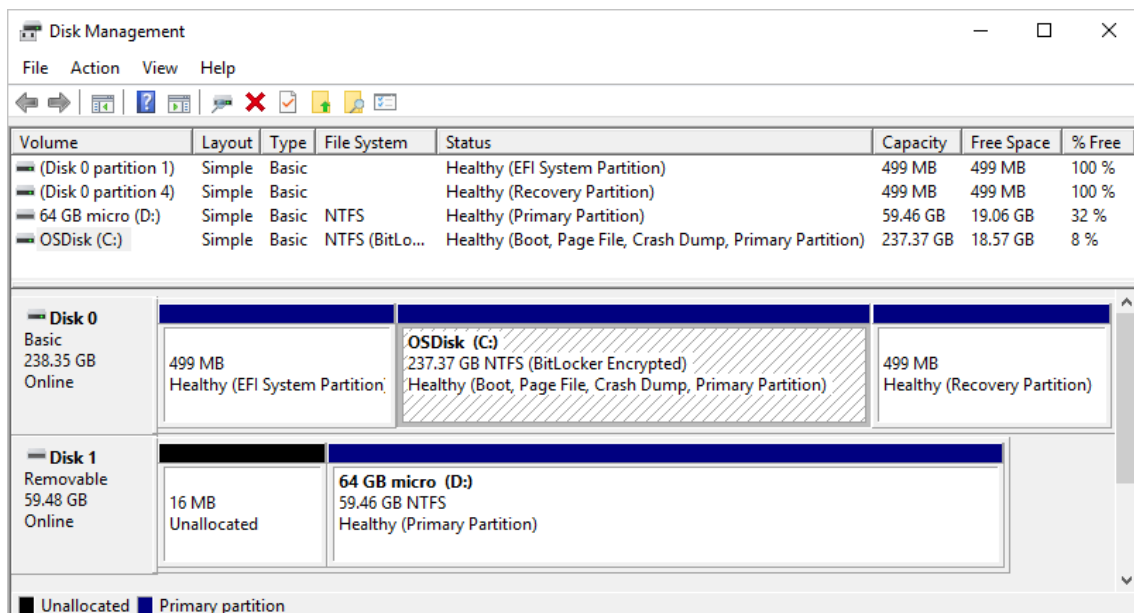
4.3 Eines de Gestió de Discs Durs

Windows: Disk Management

La gestió de discs és una utilitat de sistema en Windows per a operacions avançades d'emmagatzematge. A continuació podem veure tasques que es poden completar amb la gestió dels discs durs .

Disk Management mostra els detalls de cada unitat en el seu PC i totes les particions per a cada unitat. Els detalls inclouen estadístiques sobre les particions, incloent la quantitat d'espai assignat o utilitzat.

La següent imatge mostra la visió general de la gestió de discs per a diversos impulsos. El disc 0 té tres particions, i el disc 1 té dues particions. En el disc 0, la C: unitat per a Windows utilitza l'espai més disc. Dues altres particions per a les operacions del sistema i la recuperació utilitzen una menor quantitat d'espai de disc.



The screenshot shows the Windows Disk Management console. At the top, a table lists the volumes. Below this, a graphical view shows the layout of Disk 0 and Disk 1. Disk 0 is a 238.35 GB Basic disk, and Disk 1 is a 59.48 GB Removable disk. The graphical view shows the partitions for each disk, including their sizes and file systems.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)	499 MB	499 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (Recovery Partition)	499 MB	499 MB	100 %
64 GB micro (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	59.46 GB	19.06 GB	32 %
OSDisk (C:)	Simple	Basic	NTFS (BitLo...	Healthy (Boot, Page File, Crash Dump, Primary Partition)	237.37 GB	18.57 GB	8 %

Disk	Layout	Type	File System	Status	Capacity	Free Space	% Free
Disk 0	Simple	Basic		Healthy (EFI System Partition)	499 MB	499 MB	100 %
Disk 0	Simple	Basic		Healthy (Recovery Partition)	499 MB	499 MB	100 %
Disk 0	Simple	Basic	NTFS (BitLocker Encrypted)	Healthy (Boot, Page File, Crash Dump, Primary Partition)	237.37 GB	18.57 GB	8 %
Disk 1	Simple	Basic	NTFS	Healthy (Primary Partition)	59.46 GB	19.06 GB	32 %

Windows normalment inclou tres particions en la seva unitat principal (C:\normalment la unitat C:\). Aquestes particions inclouen la partició del sistema EFI, la partició del Dissipat Local (C:) i una partició de recuperació.

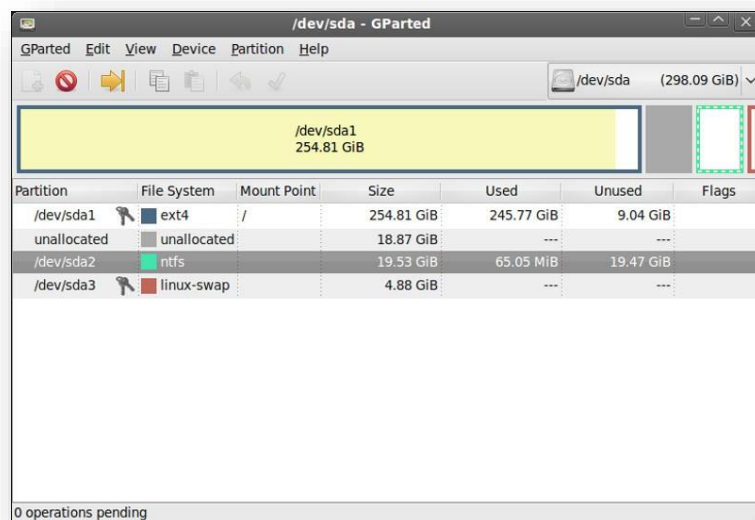
- El sistema operatiu Windows està instal·lat en la partició de Disc Local (C:). Aquesta partició és la ubicació d'emmagatzematge comú per a les altres aplicacions i arxius.

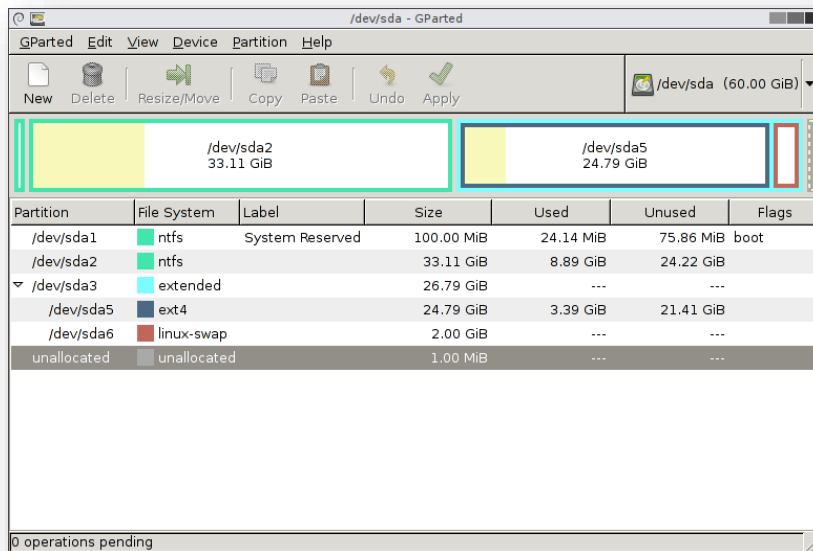
- Els PC moderns utilitzen *la partició del sistema EFI* per començar (bota) el seu PC i el seu sistema operatiu.
- *La Partició de Recuperació* emmagatzema eines especials per ajudar-te a recuperar Windows, en cas que hi hagi un problema per iniciar el PC o altres problemes seriosos.

Troblem eines de gestió de discs durs que permet formatar i gestionar particions en Windows: *EaseUS Partition Master*, *MiniTool Partition Wizard*, *MiniTool Partition Wizard*, *AOMEI Partition Assistant*.

LINUX: GParted

GParted és una eina gràfica d'escriptori que permet crear, eliminar, redimensionar, moure, validar i copiar particions - tot des d'una interfície gràfica simple i intuïtiva. El seu objectiu principal és mantenir la interfície el més simple possible però sense prendre la potència de l'usuari per realitzar operacions associades amb els sistemes de fitxers.





Per crear una partició cal:

- Seleccionar l'espai per a la partició
- Feu clic a la dreta sobre aquest espai i seleccioneu la nova opció
- Ajustar la mida i el tipus de partició
- Aplicar els canvis

Trobem eines de gestió de discs durs que permet formatar i gestionar particions en Linux: *GParted*, *KDE Partition Manager*, *Disks (GNOME Disks)*, *fdisk*, i *Parted*.