

FONAMENTS DEL MAQUINARI

PRACTICA 2

Octubre, 2024

Víctor Benjumea Gutiérrez

ÍNDEX

1. Introducció.....	3
2. Diferència entre antivirus, firewall i spyware.....	4
2.1 Antivirus.....	4
2.2 Firewall.....	4
3. Importància de les còpies de seguretat i tipus principals.....	5
3.1 Còpia de seguretat completa.....	5
3.2 Còpia de seguretat incremental.....	6
3.3 Còpia de seguretat diferencial.....	6
3.4 Principals diferències.....	7
3.5 Exemples pràctics.....	7
4. Gestió de discos.....	8
4.1 Particions Primàries.....	8
4.2 Particions Lògiques.....	8
5. Eines de gestió de disc.....	9
6. Conclusió.....	10

1. Introducció

El director t'informa que, en un futur pròxim, s'incorporarà a l'equip un alumne en pràctiques procedent d'un CFGS d'Administració de Sistemes Informàtics i Xarxes (ASIX). Queda a la nostra responsabilitat elaborar un document destinat a aquest alumne, on es detallin els aspectes fonamentals que haurà de conèixer per tal d'iniciar el seu període de pràctiques de manera eficient.

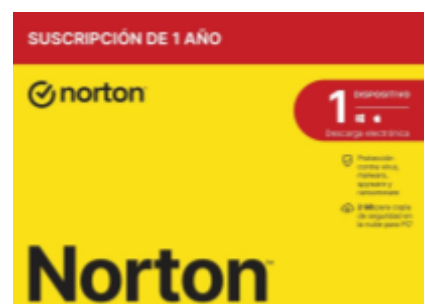
A aquest document hem d'incloure una sèrie de pautes i instruccions que permetin a l'alumne familiaritzar-se amb les seves funcions. A les indicacions hem de ser clars, ja que és important que l'alumne pugui entendre fàcilment i ràpidament els conceptes.

Haurem d'explicar-li la diferència entre antivirus, firewall i spyware, la importància de les còpies de seguretat i tipus principals. La gestió de discos com definir què és una partició i per a què serveixen les particions primàries i les lògiques. Explicar els principals sistemes d'arxius i explicar les eines de gestió de discs durs per les particions sigui per Linux o Windows.

2. Diferència entre antivirus, firewall i spyware.

2.1 Antivirus

Els **antivirus** és un tipus de software o programari que permet analitzar la memòria, les



unitats de disc i altres elements de l'ordinador per detectar la presència de virus. En cas de trobar-ne, el software ens notificarà que ha trobat un virus, i preguntarà a l'usuari si vol netejar l'arxiu o altres vegades l'esborrarà ell mateix.

La seva funció principal és escanejar fitxers i programes per detectar comportaments sospitosos o patrons de codi que coincideixin amb malware conegut, a aquest procés se l'anomena *mètode heurístic*.

El propòsit està clar, protegir el sistema contra programes maliciosos que ja hagin entrat o intentin entrar.

Al mercat hi existeixen una gran quantitat d'antivirus, però quasi tots són de pagament, tot i que algun fabricant ofereix la versió de prova com per exemple [McAfee](#) o [Norton](#).

2.2 Firewall

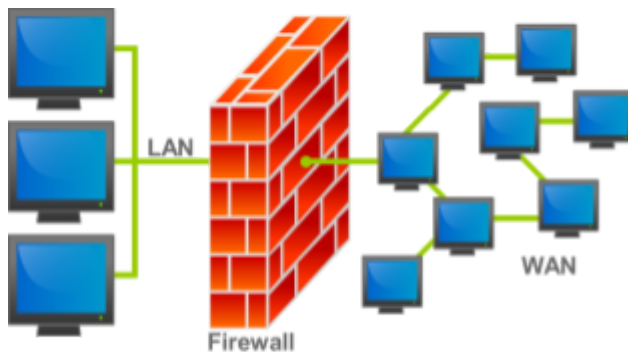


Fig.2: Esquema de com actua el firewall, entre una xarxa local i una externa

Un **firewall** o tallafocs és un sistema de seguretat de xarxa (pot ser un dispositiu físic, programari o una combinació dels dos) que actua com a barrera entre una xarxa de confiança (com la xarxa interna d'una empresa o un ordinador personal) i xarxes externes no confiablés, com internet.

El firewall controla el trànsit basant-se en un conjunt de regles de seguretat, permetent o bloquejant

connexions segons el que s'estableixi.

L'objectiu és controlar i filtrar el trànsit de xarxa per evitar els accessos no autoritzats a un sistema monitorant els accessos a la xarxa.

A Windows podem trobar els següents tallafocs: L'integrat de Windows, [ZoneAlarm](#) o Sygate SPFi i per a Linux trobem el GFW, Netfilter/iptables, Firestarter o el [Guarddog](#).

2.3 Spyware

El **spyware** és un tipus de programari maliciós dissenyat per infiltrar-se en un sistema de manera oculta o conscient amb la funció de recopilar informació de l'usuari sense el seu coneixement o consentiment.

Generalment, aquest tipus de malware està destinat a espiar les activitats de l'usuari, com la navegació per internet, les pulsacions del teclat ([keyloggers](#)) o el robatori de credencials i dades sensibles (com contrasenyes o informació financera).

Per detectar aquest tipus d'espionament, hi ha una sèrie de senyals que permeten identificar-los com per exemple s'obren finestres emergents, la navegació va lenta o les pàgines del navegador o d'inici canvien.

3. Importància de les còpies de seguretat i tipus principals

Les **còpies de seguretat** són essencials per protegir la informació si hi ha la pèrdua de dades, ja sigui per atacs d'un extern, fallida de la màquina o per culpa.

Sigui la raó que sigui, és vital tenir una còpia de seguretat que permeti garantir la integritat de la nostra informació. Existeixen diferents tipus de còpies de seguretat:

3.1 Còpia de seguretat completa

Aquest tipus de còpia de seguretat implica guardar tots els fitxers i dades, independentment de si han estat modificats o no des de l'última còpia. Això vol dir que cada còpia conté totes les dades del nostre equip.

Els avantatges que té és que, en ser una còpia única de totes les dades, això ajuda a la recuperació i fa que sigui més fàcil i ràpid

D'altra banda, aquest tipus de còpia presenta problemes, ja que, al ser una còpia íntegra de totes les dades implica que requereix molt espai d'emmagatzematge i a la vegada el procés de copiar les dades serà molt lent.

3.2 Còpia de seguretat incremental

En aquest cas, només es copien els fitxers que han estat modificats o creats des de l'última còpia, sigui completa o incremental. Això permet optimitzar l'espai i el temps necessari per a cada còpia.

Aquesta còpia, pel que fa a espai, millora a la còpia completa, ja que només es copien els fitxers de l'última còpia, i, per tant, és molt més ràpida de fer.

Encara els avantatges, el procés de restauració pot ser complex, ja que per restaurar el sistema, necessites la còpia completa original i totes les còpies incrementals fins a l'últim punt de restauració

3.3 Còpia de seguretat diferencial

Aquesta còpia de seguretat guarda tots els fitxers que han canviat des de l'última còpia **completa**. A mesura que es fan còpies diferencials successives, aquestes inclouen tots els canvis acumulats des de la darrera còpia completa.

Aquest tipus de còpia fa que la restauració sigui més senzilla que amb les còpies incrementals, ja que només necessites la còpia completa i l'última còpia diferencial, fent més de pressa el procés.

En canvi, aquesta còpia fa que a mesura que es fan més còpies diferencials, aquestes ocupen més espai, ja que acumulen tots els canvis des de l'última còpia completa.



Fig.3: Còpia de seguretat

3.4 Principals diferències

Còpia Completa: Cada còpia inclou tots els fitxers. És fàcil de restaurar i no depèn d'altres còpies, però ocupa molt espai i requereix molt temps en fer-se, ja que es copien tots els fitxers cada vegada.

Còpia Incremental: Cada còpia només inclou els fitxers nous o modificats des de l'última còpia. És la més eficient en termes d'espai i temps de còpia, però la restauració és més lenta i complicada, ja que necessites la còpia completa original i totes les còpies incrementals fins al punt de restauració.

Còpia Diferencial: Cada còpia inclou els fitxers nous o modificats des de l'última còpia completa. Utilitza més espai que la còpia incremental, ja que acumula tots els canvis des de l'última còpia completa, però la restauració és més senzilla, ja que només es necessiten la còpia completa i l'última còpia diferencial.

3.5 Exemples pràctics

Còpia Completa:

Imagina que fas una còpia de seguretat completa de tots els teus arxius avui. Aquesta còpia inclou tot el que tens al teu ordinador, des de documents, fotos, programes, etc. Si demà vols restaurar alguna cosa, només necessites la còpia que vas fer, ja que conté **tots** els fitxers.

Còpia Incremental

Fas una còpia completa el dilluns, i una còpia incremental cada dia de la setmana. El dimarts només es copien els arxius modificats o nous des de dilluns. El dimecres, es copien els canvis des de dimarts, i així successivament. Si vols restaurar el sistema el divendres, necessaries la còpia completa de dilluns i totes les còpies incrementals (dimarts, dimecres, dijous i divendres).

Còpia Diferencial

Fas una còpia completa el dilluns i còpies diferencials cada dia de la setmana. Dimarts es copien tots els canvis des de dilluns. Dimecres, es copien els canvis des de dilluns fins dimecres... Si vols restaurar el sistema el dijous, només necessites la còpia completa de dilluns i la còpia diferencial de dijous, que conté tots els canvis des de l'última còpia completa.

Aquestes diferències entre les tres, determinaran quin tipus de còpia és més adequada segons les necessitats d'emmagatzematge, temps de còpia, i facilitat de restauració.

4. Gestió de discos

Quan parlem de la gestió de discos hem de parlar de les particions, ja que aquestes juguen un paper molt important en aquesta gestió

Una partició és una divisió d'un disc dur o un altre dispositiu d'emmagatzematge en seccions més petites que funcionen de manera independent. Cada partició es pot formatar amb un sistema de fitxers i actuar com una unitat lògica separada dins d'un disc físic. Les particions permeten organitzar millor les dades, instal·lar diferents sistemes operatius o gestionar diferents volums d'informació de manera més eficient.

4.1 Particions Primàries

Són les **particions bàsiques** del disc, i un disc pot tenir fins a quatre particions primàries.

Normalment, s'utilitzen per allotjar sistemes operatius o per emmagatzemar dades. Com que el sistema de gestió de particions tradicionals només permet quatre particions primàries, si necessites més particions, hauràs de crear **particions lògiques** dins d'una partició estesa.

4.2 Particions Lògiques

Són particions que es creen dins d'una **partició estesa**. No tenen la mateixa limitació de quatre particions com les primàries.

Són útils quan necessites més de quatre particions al mateix disc. Les particions lògiques es poden utilitzar per emmagatzemar dades o per a diferents sistemes operatius, com les primàries, però estan contingudes dins d'una partició estesa, permetent una major flexibilitat en la gestió de l'espai del disc, però no poden arrencar un sistema operatiu.

4.3 Principals sistemes d'arxius

Els sistemes d'arxius s'utilitzen per gestionar com s'emmagatzemen, organitzen i recuperen les dades en dispositius com discos durs, SSDs o unitats USB. A continuació esmentaré els principals:

NTFS (New Technology File System)

És el sistema d'arxius per defecte en Windows. Suporta permisos avançats, xifratge i la compressió de fitxers.

Suporta fitxers de gran mida, és segur i fiable gràcies al [journaling](#).

FAT32 (File Allocation Table 32)

És un sistema d'arxius molt compatible amb qualsevol dispositiu i sistema operatiu, però no suporta fitxers més grans de 4 GB ni particions superiors a 8 TB.

exFAT (Extended File Allocation Table)

Dissenyat per a dispositius d'emmagatzematge portàtils. No té les limitacions de mida de fitxer de FAT32, ja que suporta fitxers més grans de 4 GB i és més modern i compatible amb altres sistemes.

ext4 (Fourth Extended File System)

Aquest sistema d'arxius, per defecte en la majoria de distribucions de Linux, ofereix el journaling i fa una gestió eficient d'espai i a més a més suporta grans volums i fitxers.

Un contra és que té una compatibilitat limitada amb Windows.

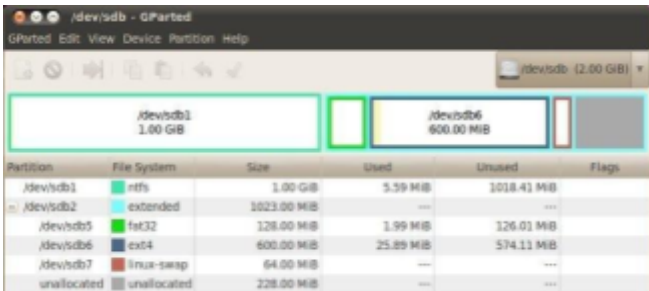
Btrfs (B-tree File System)

Aquest sistema d'arxius és més modern que ext4, i està dissenyat per gestionar millor les grans quantitats de dades i suportar funcions avançades com la compressió. A diferència del ext4, aquest no és tan estable.

5. Eines de gestió de disc

Tant a Linux com a Windows existeixen eines per a la gestió de disc, és a dir, per a formatar i gestionar les particions abans esmentades. A continuació esmentaré un de Windows i un de Linux:

LINUX:



Partition	File System	Size	Used	Unused	Flags
/dev/sdb1	ntfs	1.00 GB	5.59 MB	1018.41 MB	---
/dev/sdb2	extended	1023.00 MB	---	---	---
/dev/sdb3	fat32	128.00 MB	1.99 MB	126.01 MB	---
/dev/sdb6	ext4	600.00 MB	25.89 MB	574.11 MB	---
/dev/sdb7	linux-swsp	64.00 MB	---	---	---
unallocated	unallocated	228.00 MB	---	---	---

GParted: Aquesta és una eina de gestió molt utilitzada als sistemes Linux, ja que permet crear, esborrar modificar particions. És molt fàcil d'instal·lar i amb una simple comanda podrem utilitzar-la.

WINDOWS:

Disk Management: A Windows ve integrat aquesta eina de gestió que permet fer el mateix que GParted, crear i modificar particions.

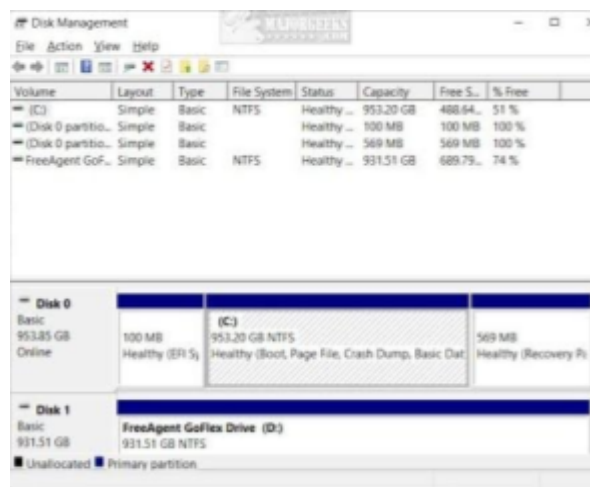


Fig.5:Captura Disk Management

6. Conclusió

En conclusió, aquest treball servirà com a guia clara i estructurada a l'alumne en pràctiques del CFGS d'Administració de Sistemes Informàtics i Xarxes (ASIX), amb l'objectiu d'ajudar-lo a integrar-se de manera eficient en les seves funcions.

S'han detallat aspectes sobre la seguretat informàtica, com la diferència entre antivirus, tallafocs i spyware, i s'ha ressaltat la importància de les còpies de seguretat, presentant els seus tipus principals (completa, incremental i diferencial) i les seves aplicacions pràctiques.

També s'ha introduït la gestió de discos, amb una explicació clara de les particions primàries i lògiques, i com aquestes permeten una millor organització i gestió de les dades.

Així mateix, s'han analitzat els sistemes d'arxius més rellevants, tant per a Windows (NTFS, FAT32, exFAT) com per a Linux (ext4, Btrfs), per tal que l'alumne entengui quines opcions són més adequades en els diferents entorns que es trobarà en el seu període de pràctiques.

Finalment, s'han presentat eines de gestió de discs tant per a Linux (com GParted) com per a Windows (com Disk Management), ja que aquestes eines li proporcionaran a l'alumne els recursos necessaris per gestionar particions.

En general, aquest document li servirà com a base perquè pugui començar les seves pràctiques amb una mica de context.