

FONAMENT DE MAQUINARI

PRÀCTICA 2

Octubre 16, 2024

Oussama el Kaddouri El Morabiti

ÍNDEX

1. Introducció.....	3
2. Diferències entre Antivirus, Firewall i Spyware.....	4
2.1. Antivirus.....	4
2.2. Firewall.....	4
2.3. Spyware.....	4
3. Importància de les còpies de seguretat i tipus principals.....	6
4. Gestió de discos.....	8
4.1. Particions - Lògiques i Primàries.....	8
4.2. Principals Sistemes d'Arxius.....	9
4.3. Eines de Gestió de disc dur.....	10
5. Conclusió.....	11
6. Bibliografia.....	11

1. Introducció

Aquest treball servirà com una guia bàsica per a un/a alumne/a en pràctiques del Cicle Formatiu de Grau Superior (CFGS) en Administració de Sistemes Informàtics en Xarxa (ASIX). L'objectiu principal d'aquest treball és bàsicament proporcionar unes instruccions perquè l'estudiant que estigui realitzant les pràctiques pugui iniciar les tasques que realitzem diàriament en l'empresa, d'una forma clara i ordenada, per evitar que l'alumne es perdi i que no necessiti més ajuda externa a part d'aquest document. A més a més, en aquest document també s'inclouran aspectes essencials com quines seran les tasques que haurà de realitzar, quins recursos tindrà al seu abast per poder complir les diferents tasques, les normes que ha de seguir per no tenir cap problema amb l'empresa i quines són les persones de referència a dins de l'organització.

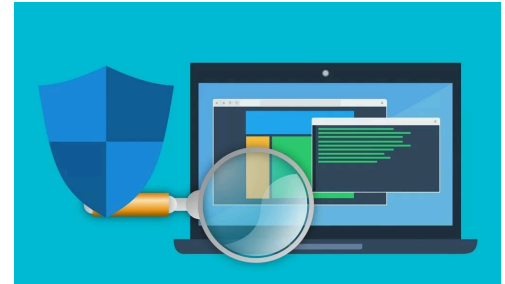
D'aquesta manera, podrem assegurar que per part de l'estudiant en pràctiques no tindrem cap problema, i podrà tenir una ràpida i efectiva integració en l'entorn laboral, garantint d'aquella forma una experiència enriquidora tant per a l'estudiant com per a l'empresa.

2. Diferències entre Antivirus, Firewall i Spyware

Abans de començar amb les diferències, faré una breu introducció de què és cada concepte, per poder-nos fer una idea.

2.1. Antivirus

Un antivirus és un programa que té com a finalitat detectar, prevenir i eliminar programes que ens puguin afectar de manera negativa al nostre sistema operatiu, com per exemple, virus, troians, etc. L'antivirus s'executa en segon pla, és a dir, que mentre nosaltres estem en l'ordinador ell està treballant pel seu compte, analitzant i escanejant els nostres programes a la recerca d'alguna cosa sospitosa que pugui danyar el nostre sistema operatiu.



2.2. Firewall

Un firewall és bàsicament una eina que s'encarrega de posar un sistema de seguretat entre la nostra xarxa i internet, per aquesta forma poder tenir un control de totes les dades i informació que passen per la nostra xarxa, per tant, actua com una barrera que si veu que una de les connexions pot tenir un efecte negatiu per al nostre dispositiu, aquest va ràpidament a bloquejar-les.



2.3. Spyware

Un spyware és un programa que va ser dissenyat amb un únic propòsit, el qual és el d'espionar un usuari i tot el que està realitzant en el seu dispositiu sense el seu consentiment. Aquests tipus de programes a part d'utilitzar-se com a programa espia, també s'utilitza per robar informació important de la víctima com per exemple informació personal, contrasenyes, informació bancària, entre moltíssimes altres coses. Tot això amb la finalitat de vendre aquesta informació de forma il·legal.



A continuació et mostraré les principals diferències entre un antivirus, un firewall i un spyware:

Per començar, un antivirus com hem dit anteriorment té com a finalitat protegir el nostre dispositiu de programes maliciosos, més coneguts com a “malware”. Aquest per poder detectar aquests programes maliciosos s'executa en segon pla i s'encarrega d'anar analitzant programa per programa per veure si tots són segurs pel seu funcionament, en resum, el seu principal objectiu és el de mantenir el sistema net i lliure d'amenaçes.

Per altra banda, un firewall no s'encarrega de detectar i eliminar programes que siguin maliciosos pel nostre dispositiu, sinó que aquest s'encarrega de controlar tot el trànsit de dades que passa entre la nostra xarxa i la de l'internet. Per exemple, si tenim a un atacant que vol accedir al nostre sistema aquest s'encarrega de tallar aquesta connexió, evitant d'aquesta forma que pugui accedir al nostre dispositiu. És com un vigilant que filtra les connexions, només deixa que funcionin les que siguin més segures. Per això, no té res a veure amb un antivirus, ja que, no s'encarrega d'eliminar i analitzar els diferents programes en busca d'un programa maliciós.

Per últim, un spyware no té res a veure amb els 2 últims conceptes, ja que aquest és un tipus específic de “malware” que no té com a objectiu danyar d'una forma directa ni visible el sistema, sinó que se centra més a recopilar informació de la víctima, com ara, les pàgines web que visita, les contrasenyes que utilitza, informació personal o dades bancàries. L'objectiu d'aquest programa és de recopilar tota aquesta informació, per aquesta forma poder ser venuda a altres de forma il·lícita.

En resum, un antivirus i un firewall, tenen la funció de controlar i vigilar al nostre dispositiu, mentre un ho fa revisant els programes en cerca de malware, l'altre ho fa controlant les diferents connexions que té el nostre dispositiu per la xarxa. El spyware, en canvi, fa tot el contrari, intenta robar informació i espionar a l'usuari.

3. Importància de les còpies de seguretat i tipus principals

Una còpia de seguretat és un mètode de seguretat que s'encarrega de duplicar tota la informació que nosaltres considerem important, tot això amb la finalitat que si algun dia passa alguna cosa o bé per la nostra culpa esborrem aquestes dades importants o bé per error del sistema o per infeccions per malware o altres coses, i aquesta informació desapareix que puguem tenir aquesta mesura de seguretat per poder recuperar la informació. Per aquest motiu, les còpies de seguretat són tan importants, ja que la pèrdua de dades pot ser un gran problema i pot portar



conseqüències molt greus, especialment en entorns més professionals com les empreses, per exemple, si una empresa perd tots els seus arxius financers o les dades dels seus clients, si no té una còpia de seguretat, tota aquella informació ja s'ha perdut per sempre, i això en una empresa no només pot comportar perdre diners, sinó tota la teva reputació.

Per aquest motiu, fer còpies de seguretat és tan important, perquè si algun dia passa algun error, encara tenim l'oportunitat de recuperar la informació. Dintre de les còpies de seguretat existeixen diversos tipus, que anomenarem a continuació:

- ★ **Còpia de seguretat completa:** Com bé ens indica en el nom, aquest fa una còpia d'absolutament totes les dades que hi ha en el sistema. És el tipus de còpia de seguretat més segur que existeix, ja que, si perdem qualsevol cosa, podem recuperar absolutament tota la informació. Tot i això, és el tipus de còpia més lent i que ocupa més espai, ja que, com bé he dit anteriorment fa una còpia de seguretat d'absolutament tot el sistema, fins i tot, d'informació totalment irrellevant.
- ★ **Còpia de seguretat incremental:** Aquest tipus de còpia de seguretat, només duplica els fitxers que han estat modificats en l'última còpia de seguretat. D'aquesta forma, podem reduir moltíssim el temps i l'espai necessari per realitzar la còpia, ja que, només realitza còpia a informació que hem estat obrint i modificant recentment, per tant, informació la qual ha de ser important.

- ★ **Còpia de seguretat diferencial:** Aquest tipus de còpia de seguretat, també és un tipus de còpia que només duplica fitxers i dades que han set recentment modificats, però només amb l'última còpia de seguretat de tipus completa, és a dir, que amb qualsevol altra tipus de còpia de seguretat realitzaria també una còpia de seguretat d'absolutament tot el sistema.

- ★ **Còpia de seguretat en núvol:** Aquest tipus de còpia es realitza a través d'internet, enviant totes les dades a un servei de núvol com pot ser Google Drive o Dropbox. Aquest té un avantatge que tots els altres no tenen i és que la nostra informació, està guardada fora del nostre dispositiu, la qual cosa fa que estigui més segura i protegida davant de robatoris o incendis. L'únic problema és que depèn molt de la nostra velocitat de connexió a internet, si aquesta és lenta, la informació tardarà més a pujar al núvol.

- ★ **Còpia de seguretat local:** Aquest a diferència de l'anterior ja no es realitza virtualment, sinó tot al contrari, es fa físicament, per aquest tipus de còpia de seguretat necessitem un dispositiu físic com per exemple disc durs externs, memòries USB, etc. Aquest solen ser els més ràpids, però com que són físics estan més exposats a robatoris, pèrdues, etc.



4. Gestió de discos

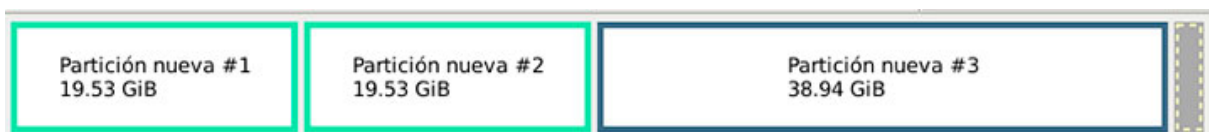
La gestió de discos és un dels processos on el qual tenim el poder per a poder controlar i organitzar d'on guardem la nostra informació dins de l'ordinador o del dispositiu. Els discos són els llocs on es guarden tots els nostres fitxers, programes i sistemes operatius. Gestionar aquests discos et dona molts avantatges, com per exemple, poder dividir el disc en parts més petites els quals reben el nom de "Particions", poder formatar el disc, és a dir, esborrar tot el que contingui, per poder tornar-lo a reutilitzar i per últim poder assignar la quantitat d'espai que necessites per a poder instal·lar-te noves aplicacions. En resum, gestionar els discos és com si estiguéssim guardant tota la nostra informació i arxius en una prestatgeria, el qual som nosaltres els encarregats d'escollir l'espai i la ubicació de cada arxiu.

4.1. Particions - Lògiques i Primàries

Una partició, com bé indica el seu propi nom és bàsicament com si estiguéssim dividint el disc dur de l'ordinador en diversos compartiments on en cada un d'ells tinguéssim la finalitat de classificar la informació i els arxius del nostre dispositiu, a part de classificar informació una partició també serveix per a tenir la possibilitat de poder instal·lar-se diferents sistemes operatius dins del nostre ordinador o dispositiu. En resum, una partició serveix per a poder dividir la memòria del nostre disc dur en diverses parts el qual cada un d'aquestes parts podrem emmagatzemar o descarregar qualsevol informació o sistema operatiu que nosaltres vulguem. N'hi ha de 2 tipus, aquestes són:

- **Particions Primàries:** Aquests tipus de particions, com bé indica el seu nom són les principals del disc dur, i per tant són les més importants. Un disc dur pot tenir fins a quatre particions primàries, aquestes solen ser utilitzades per guardar la informació més important i són els únics tipus de Particions que són arrencables, és a dir, on es poden iniciar diferents sistemes operatius, per això, normalment les Particions Primàries solen ser utilitzades per a la utilització de Sistemes Operatius.

→ **Particions Lògiques:** Aquest tipus de particions, se solen utilitzar quan l'usuari necessita més de 4 particions en el disc, per a poder realitzar això només hem de crear una partició primària especial el qual obtindrà el nom de partició estesa i dins d'aquesta partició estesa tindrem la possibilitat de poder crear moltes particions lògiques, les quals podrem guardar moltíssima informació i arxius addicionals, la diferència que té aquest tipus de partició amb l'altre és que no són arrencables, és a dir, que no es poden iniciar Sistemes Operatius en ells.



4.2. Principals Sistemes d'Arxius

Dins d'un dispositiu com és lògic, hi ha moltíssima informació, i molta d'aquesta informació no té res a veure amb l'altre, és a dir, que a dins d'un dispositiu existeix moltíssima diversitat d'informació, i per tant hi ha diverses maneres de guardar aquesta informació, els encarregats de classificar els diferents tipus d'informació i d'arxius són els sistemes d'arxiu, a continuació et descriuré els tipus més coneguts i utilitzats dins del món de la informàtica:

- **FAT32:** És un dels sistemes d'arxius més antic que existeix, i per això, és compatible amb gairebé tots els dispositius que existeixen (ordinadors, consoles, càmeres, etc.). El problema d'aquest sistema d'arxius, és que només té una capacitat de 4 GB com a màxim per a poder utilitzar, i això és un gran desavantatge actualment.
- **NTFS:** És el sistema d'arxius que utilitza actualment els dispositius que tenen Windows, a diferència de l'anterior, és més actual, per tant, té funcions més avançades i té una capacitat major a 4 GB, per tant, es poden guardar arxius més pesats.

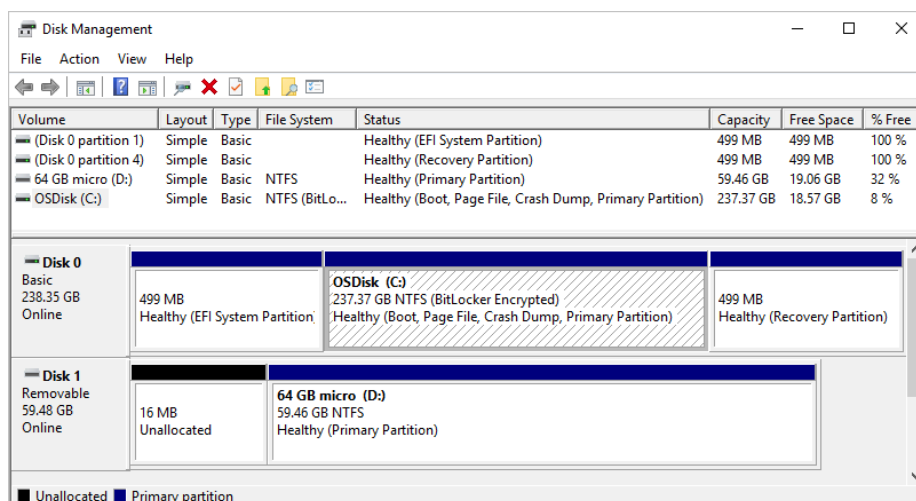
- **exFAT:** Aquest sistema d'arxius és una versió més moderna i avançada del FAT32, a diferència del FAT32, No està limitat només a 4 GB, funcions més modernes, compatible amb Windows i macOS.
- **ext4:** És el sistema d'arxiu per excel·lència a sistemes operatius Linux, és ràpid, segur i té moltíssima capacitat per guardar arxius grans. Els desavantatges és que si vols utilitzar aquest sistema d'arxius en Windows o en macOS t'hauràs de descarregar programes perquè aquest sigui compatible amb aquests.

4.3. Eines de Gestió de disc dur

Per a poder gestionar el disc dur del nostre dispositiu existeixen diverses eines tant en Windows com en Linux que ens permeten poder executar aquesta tasca d'una forma ràpida i senzilla, aquestes eines són les següents:

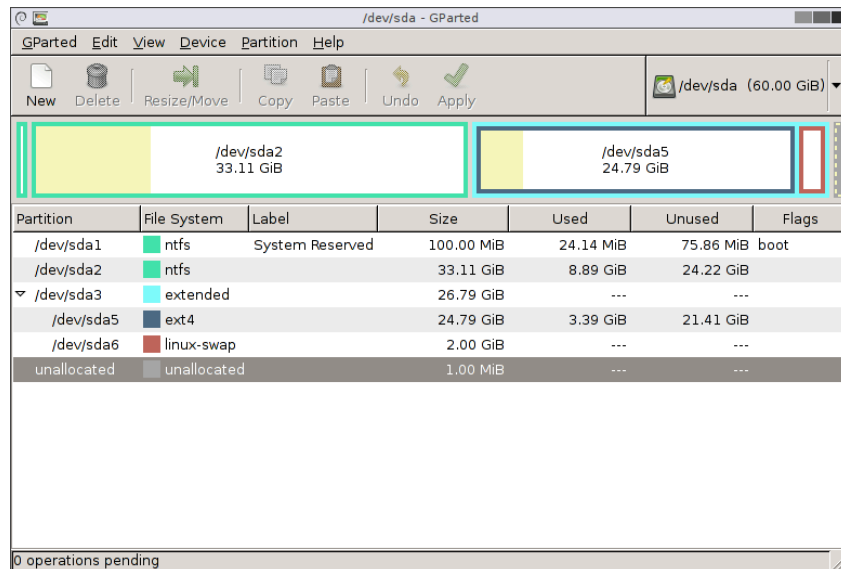
Eines per a Windows:

- **Gestió de Discos (Disk Management):** Aquesta aplicació ja ve inclosa amb el Sistema Operatiu de Windows, aquesta eina ens permet poder crear, eliminar i modificar les particions del disc d'una forma visual i fàcil.



Eines per a Linux:

- **GParted:** Eina més utilitzada en Linux, ens permet crear, eliminar, modificar i formatar particions d'una forma superfàcil i visual.



5. Conclusió

En aquest treball hem pogut observar la importància i les principals diferències entre Antivirus, Firewall i Spyware, a més a més, també hem pogut observar la gran importància que té realitzar constantment còpies de seguretat, per aquesta forma evitar perdre de forma permanent els nostres arxius i dades més importants i per últim també hem pogut veure la importància que té el fet de tenir una bona gestió del sistema i el de tenir tots els tipus d'arxius ben classificats en els diferents sistemes d'arxius, tot això per aquesta forma poder tenir un millor control i organització de les nostres dades i arxius de l'ordinador o dispositiu en qüestió.

6. Bibliografía

<https://es.wikipedia.org/wiki/Antivirus>

https://latam.kaspersky.com/resource-center/definitions/firewall?srsId=AfmBOop-lox5K9SJggDr_8P3XnMDGUrWpZJSWjQWrHV3kKd5BmJO5A38

<https://www.avast.com/es-es/c-spyware>

https://ca.wikipedia.org/wiki/C%C3%B2pia_de_seguretat

<https://informaticos.co/4-tipos-de-copias-de-seguridad/>

https://es.wikipedia.org/wiki/Partici%C3%B3n_de_disco

<https://es.easeus.com/partition-manager-tips/programa-para-hacer-particiones-de-disco-duro.html>

<https://geekflare.com/es/best-linux-partition-managers/>