

Tema 1: Característiques de seguretat en la publicació de pàgines web

Introducció

Qualsevol desenvolupador web ha de ser conscient del material amb el qual treballa i fer-se una sèrie de preguntes abans de publicar un lloc web:

- Les dades que manipulo són sensibles i han de complir amb la Llei orgànica de Protecció de Dades?
- Tinc mesures de protecció per al meu equip antimalware i antivirus?
- És necessari accedir a l'ordinador o sistema mitjançant credencials d'accés (usuari i clau)?
- La meua zona de treball està protegida per a impedir l'accés d'altres usuaris de l'equip de treball?
- El servidor destí o de producció compleix amb les regles esmentades prèviament?
- El servidor disposa del programari actualitzat i adequat?

Les respostes podem trobar-les reflexionant sobre les següents premisses:

- El desenvolupador ha de contemplar la seguretat en els equips en els quals es desenvolupi el producte i el lloc on, finalment, s'instal·li el producte final del lloc web.
- En els equips locals ha d'assegurar el seu sistema amb programari de seguretat com antimalware, antivirus, així com també un control de seguretat d'accés a l'equip (login) a través d'accés amb credencials: nom d'usuari i clau.
- Quant a l'equip de producció o hosting ha de complir i exigir unes mesures de seguretat: primer d'accés, a través de l'usuari i clau, i després a través d'actualització de programari, antivirus del servidor, així com una configuració adequada del servidor.

Més informació sobre la LOPD (Llei orgànica de Protecció de Dades) per la qual han de registrar-se tot sistema web que s'implementi dins del territori europeu.

<https://www.aepd.es/es/documento/reglamento-ue-2016-679-consolidado.pdf>

1.1. Seguretat en diferents sistemes d'arxius

Què és un sistema d'arxius? Un sistema d'arxius consisteix en un mètode i una estructura de dades el qual un sistema operatiu o sistema base utilitza per a organitzar els diferents arxius d'un sistema d'emmagatzematge massiu i/o partició d'aquest.

També sol referir-se a la mena de mètode o organització d'aquest sistema d'arxius. Com, per exemple, FAT, EXT4, NTFS, etc.

En definitiva, els sistemes d'arxius formen part integral dels sistemes operatius (Windows, UNIX, GNU/Linux, Mac OS, etc.). No obstant això, en l'actualitat on tots els dispositius estan

interconnectats, el sistema operatiu pot integrar elements aliens al propi maquinari i integrar-los en el propi sistema d'arxius per a tractar-los com a propis.

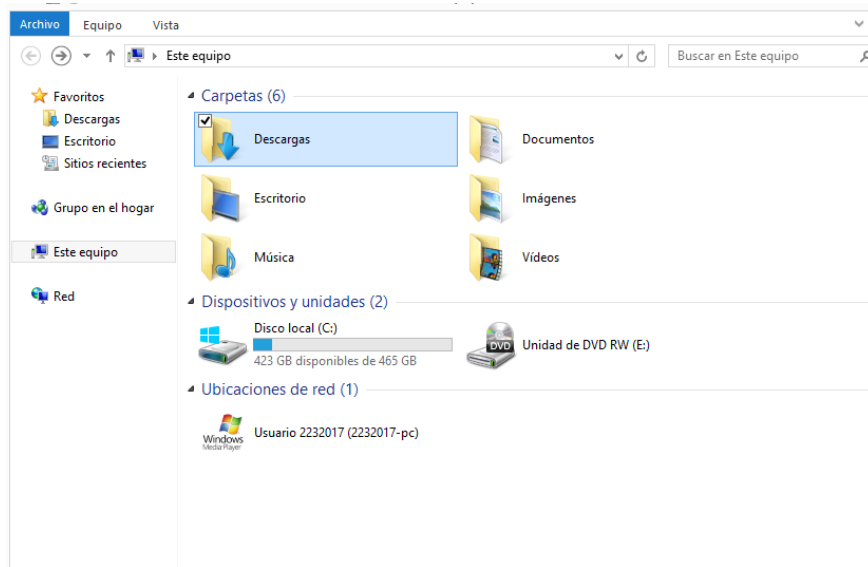


Figura 1.1.

En la imatge 1.1 podem observar els dispositius d'emmagatzematge corresponents a un disc dur, així com també una unitat DVD de lectura-escritura i una unitat de xarxa. Aquesta unitat fa referència a zones d'emmagatzematge d'un altre dispositiu connectat a la xarxa local.

Una vegada feta aquesta petita introducció als sistemes d'arxius hem de comprendre que igual que protegim documents en suport paper també hem de protegir els arxius o dades amb els quals treballem. Més si cap si existeixen dades sobre persones o entitats.

En general, la forma que tenim per a protegir els nostres arxius serà: Mitjançant les eines del propi SO i mitjançant programari de tercers.

Podem esmentar com a eines del SOTA la capacitat d'aquest per a discernir a un usuari i a un altre a través de credencials. A més, l'administrador de l'equip podrà seleccionar el perfil adequat que permeti limitar els privilegis de tots i cadascun dels usuaris. Per exemple, un usuari no hauria de poder accedir a la zona d'un altre usuari sense tenir privilegis majors que els d'un usuari del sistema. Si l'usuari en qüestió, s'autentica a través d'una xarxa contra un servidor, els nivells de seguretat seran majors.

Si s'ha de compartir informació s'ha d'indicar qui pot accedir i amb quins privilegis. Per exemple, imaginem que compartim una carpeta o directori, però hem d'indicar quins usuaris poden: llegir, escriure i/o modificar.

El programari de tercers que podem utilitzar per a protegir el nostre equip pot ser: tallafocs, antivirus, antimalware, antispyware, etc.

Hem de tenir en compte el desenvolupament en paral·lel dels sistemes distribuïts i xarxes de dades, comentat anteriorment, que ha donat lloc a l'aparició de nous riscos de seguretat

relatiu a la distribució de la informació entre els sistemes informàtics i a la necessitat de reforçar i adaptar al nou entorn els controls de seguretat dels sistemes individuals.

En l'era actual, tots els ordinadors estan interconnectats generalment, i la propagació de virus és molt més ràpida gràcies també a la facilitat a l'accés i distribució de la informació.

Donada aquesta situació es fa necessari integrar en les arquitectures de comunicacions existents les funcionalitats pròpies de la seguretat. Aquest procés d'integració necessàriament implicarà la implementació de mecanismes i serveis amb funcions de seguretat que es recolzaran en molts casos en serveis, mecanismes i funcions ja implementats en la pròpia arquitectura de comunicacions. El resultat final serà l'**Arquitectura de seguretat**.

L'estàndard ISO 7498-2 defineix un servei de seguretat com el servei proporcionat per un nivell d'un sistema obert que garanteix la seguretat dels sistemes oberts o a les transferències de dades en aquests sistemes. Aquests serveis estan dividits en cinc categories i 14 serveis específics. Les categories són:

- **Autenticació:** Assegura que les entitats que es comuniquen són els qui diuen que són. L'estàndard ISO 7498-2 defineix dos serveis d'autenticació específics: Autenticació de l'origen de les dades i Autenticació d'entitats pareixes.
- **Control d'accés:** el servei de control d'accés evita l'ús fraudulent dels recursos del sistema. Amb aquest servei es controla qui pot accedir als recursos en general i en quines condicions tindrà aquest accés. A més, podrà limitar-se unes certes condicions a aquests recursos (horari d'accés, privilegis sobre el recurs, etc.).
- **Confidencialitat:** El servei de confidencialitat assegura que la informació no serà divulgada o revelada ni estarà disponible per: individus, entitats o organitzacions, processos o programari no autoritzat.
- **Integritat:** El servei d'integritat assegura que les dades rebudes són exactament a com han estat enviats per una entitat autoritzada. És a dir, sense duplicacions o repeticions, retransmissions tallades o continuades de manera atípica, insercions o modificacions.
- **No repudi:** el servei de no repudi evita que les entitats pareixes que es comuniquen entre si puguin denegar una o totes dues en haver participat en la comunicació.

Si volem un sistema d'arxius segur hem d'implementar sistemes, mètodes i procediments que així ho permetin. Podem esmentar diversos mètodes dels més utilitzats per a mantenir-ho segur: tindrem l'assignació de permisos d'accés discrecionals segons perfils d'usuaris, utilització de tallafocs, antivirus, còpies de seguretat, xifrat d'informació i encriptació d'arxius i carpetes.

1.1.1. Sistema operatiu Linux

Centrant-nos en el sistema operatiu Linux devem, primer, indicar que no és un sistema operatiu propietari. Trobarem que hi ha distribucions de pagament (Xarxa Hat, Suse, Mandriva) i distribucions sota llicència GNU (Ubuntu, Fedora, Centos, OpenSuse, Debian). GNU significa (GNU is Not Unix).

Linux pot implementar diverses solucions de sistemes d'arxius com EXT3, EXT4, ReiserFS, XFS. Tots ells amb un sistema de logs o journaling consistents a dur a terme un registre de diari en el qual s'emmagatzema la informació necessària. Amb aquest sistema s'aconsegueix restablir les dades afectades per la transacció en cas que aquesta falli. Per exemple, quan el sistema cau per falta de corrent elèctric.

Algunes de les característiques bàsiques d'aquests sistemes operatius són les següents:

- **Lliure:** qualsevol ho pot usar, distribuir i modificar.
- Tenim distribucions gratis podent emprar tantes llicències com es desitgi.
- Desenvolupat per milers de voluntaris en el món. Qualsevol pot participar i pertànyer a la comunitat.
- Codi font obert a tots.
- Alta estabilitat, per la qual cosa és difícil que es quedi penjat.
- Extremadament segur ja que té diversos sistemes de protecció. El seu tallafocs està incrustat en el propi nucli del sistema.
- Facilitat d'ús en moltes tasques.
- Llegeix i escriu en sistemes d'arxius de Windows i Macintosh.
- Es comunica amb qualsevol altre sistema de xarxa.
- Les distribucions tenen diversos escriptoris com **Unity**, **Gnome**, **KDE**, **XFCE**, **LXDE**.
- Necessita baixos requeriments Maquinari per a poder executar-se.
- Ocupa poca memòria a causa de la senzillesa d'UNIX.

En el procés d'instal·lació, distribucions Linux com Debian sol·liciten clau per a un usuari, anomenat root, que serà l'administrador del sistema. A més, haurem d'indicar les credencials d'un usuari (nom d'usuari i clau) que tindrà l'accés restringit al sistema. És a dir, si volem fer tasques normals d'usuari utilitzarem l'usuari introduït. No obstant això, si volem fer tasques pròpies d'un administrador d'equip, com a instal·lacions o paquets, aquestes hauran de realitzar-se a través de l'usuari **root**.

Una dels avantatges del SO Linux és que qualsevol usuari pot fer tasques com a administrador. Però hi ha una dificultat, sempre necessitarà les credencials de root.

Encara que és un sistema amb una fama de segur no està lliure d'accessos indesitjats, virus, spyware, etc. Amb la qual cosa haurem d'implementar mecanismes de defensa activa.

```
(base) javier@javier-VirtualBox:/etc$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
all -- anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
```

Figura 1.2.

El que fa al tallafocs com s'ha comentat prèviament. Aquest és part integrant del nucli (kernel) de Linux. Cal assenyalar les línies DROP, amb aquest paràmetre aconseguim que les peticions

procedents de les màquines que les seves IPs coincideixen amb les marcades no rebim resposta. És a dir, de cara a elles el nostre ordinador està apagat i fora de cobertura. El valor ALL indica que les comunicacions per qualsevol port estan negades.

És tal la potència de IPTABLES que ens pot ajudar a “enrutar” tots els paquets d'una xarxa filtrant l'origen de les dades i donant pas segons quin port i a on es dirigeixen.

Netfilter és un framework disponible en el kernel de Linux que permet interceptar i manipular paquets de xarxa.

El problema de configurar un tallafocs en manera comando és la necessitat d'aprendre no sols el comando sinó també tots els paràmetres i valors possibles. Per a una major rapidesa en el procés seria convenient una aplicació gràfica que ens proporcioni una vista molt més intuïtiva del procés. En Linux tenim exemples com són: Guarddog, Firestarter, KMyFirewall, FWbuilder i altres.

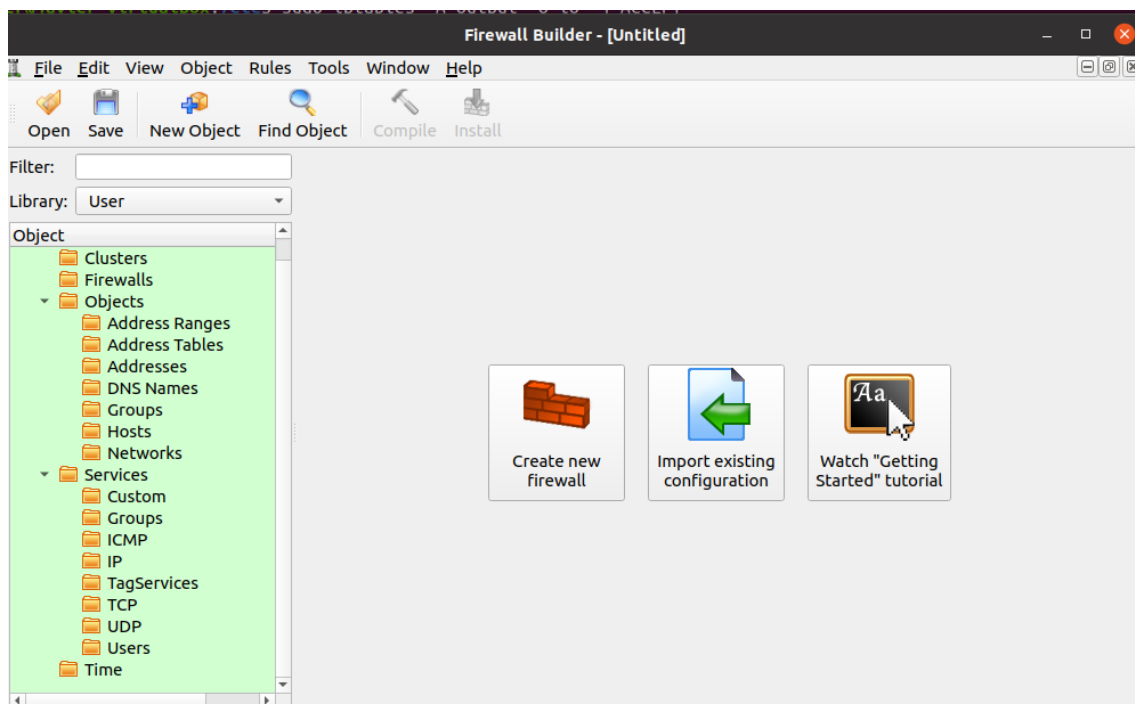


Figura 1.3.

En la figura 1.3 observem la pantalla del paquet FWBuilder, una de les aplicacions gràfiques més conegudes. Hem de tenir en compte que no és un tallafocs sinó una eina que ens permet generar un arxiu amb les regles que nosaltres volem implementar per a protegir el nostre equip d'atacs externs o de sortides de dades internes cap a l'exterior. És a dir, compleix part de les funcions que es poden establir amb IPTABLES, si volem emprar l'arxiu haurem d'usar IPTABLES per a indicar que aplicació les regles que hem generat amb aquesta eina.

Una eina molt útil relacionada amb IPTABLES és FAIL2BAN. Aquesta eina ens permet indicar quin programari ha de ser protegit contra atacs per “força bruta” indesitjats. Com funciona? En el seu arxiu de configuració de regles, /etc/fail2ban/*jail.conf, indicarem el programari que volem protegir i com ha d'actuar. En el següent exemple observem una porció de la

configuració de l'arxiu esmentat prèviament i correspon a com protegir el programari d'accés remot SSH per mitjà del port 23.

```
[ssh]
enabled=true
port = ssh
filter = sshd
action = iptables[name=SSH, port=23, protocol=tcp]
logpath=/var/log/auth.log
maxretry=6
```

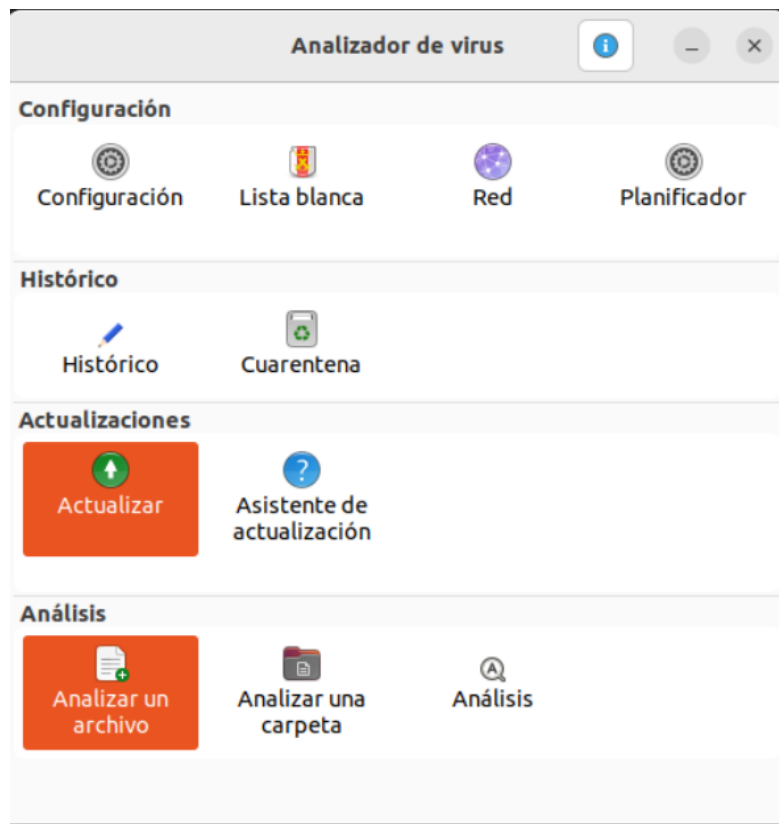


Figura 1.4.

Encara que existeixen antivirus suficients per a triar el que considerem més adequat, en aquest cas s'utilitzarà un antivirus lliure i gratuït denominat CLAMAV. En la figura 1.5 observem com s'està treballant amb l'aplicació gràfica ClamTK. Quant a malware i cucs és molt complicat infectar un sistema Linux a causa dels seus nivells de seguretat. Però cal recordar que el fet que aquests sistemes siguin segurs no garanteix plena seguretat en aquests.

1.1.2. Sistema operatiu Windows

En Windows generalment, el primer usuari que es crea té privilegis d'administrador i és integrant del grup d'administradors.

És aconsellable que hi hagi més d'un usuari amb perfil d'administrador i, si pot ser, no utilitzar-lo més que en casos d'administració del SO.

Convé generalment tenir dos usuaris administradors (almenys en Windows) ja que aquests sistemes són centre de molt malware i atacs. S'aconsegueix que el centre de l'atac sigui l'usuari de treball estant l'usuari administrador (el que seleccionem com a tal), aparentment, fora de perill. En cas d'atac es pot arrencar el sistema "a prova d'errors", accedir com a administrador i fer les tasques de manteniment que s'estimin necessàries per a arreglar el problema.

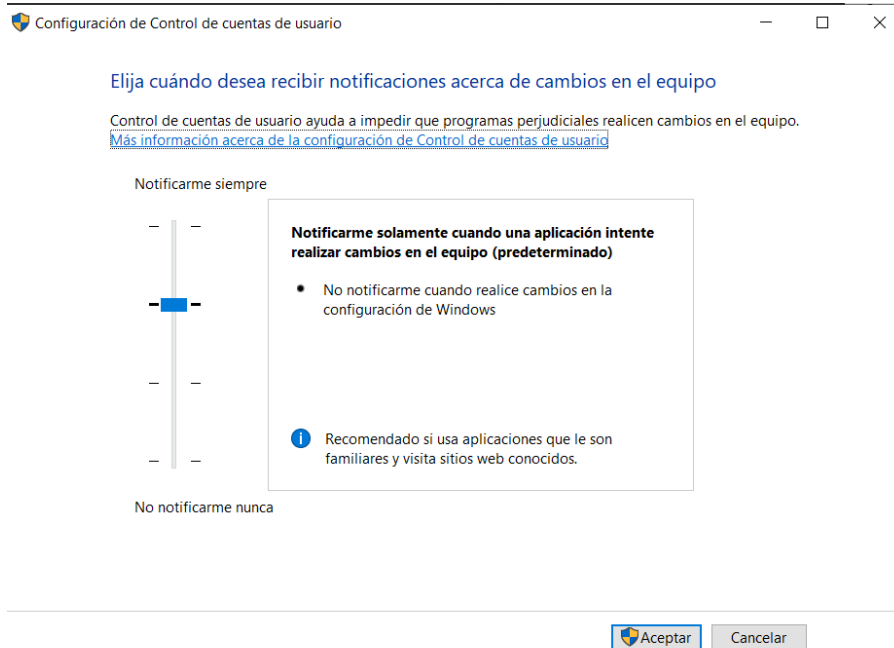


Figura 1.5.

El sistema operatiu Windows té un sistema de control d'usuaris però, a diferència de Linux, podem manipular el nivell de seguretat que s'aplicarà a aquests usuaris.

En el moment que creuem un usuari li indiquem al sistema en quin grup estarà integrat. És important definir-ho perquè determinarà el perfil de l'usuari. Els grups poden ser: usuari estàndard o administrador. No és aconsellable que tots els usuaris siguin administradors. L'habitual és que hi hagi un o dos usuaris administradors i la resta dels usuaris, usuaris estàndard.

En la figura 1.5 observem el UAC (User Access Control) de Windows que obre el panell per a la gestió. Podrem accedir en Windows escrivint **Canviar configuració de Control de comptes d'usuari**, aquesta característica forma part del panell de control.

El control consisteix a indicar-li el nivell d'avís de canvis en el sistema per part d'una aplicació o servei. L'avís espera la reacció de l'usuari autoritzant o no la realització d'aquests canvis. Aquest avís no informa de l'abast dels canvis.

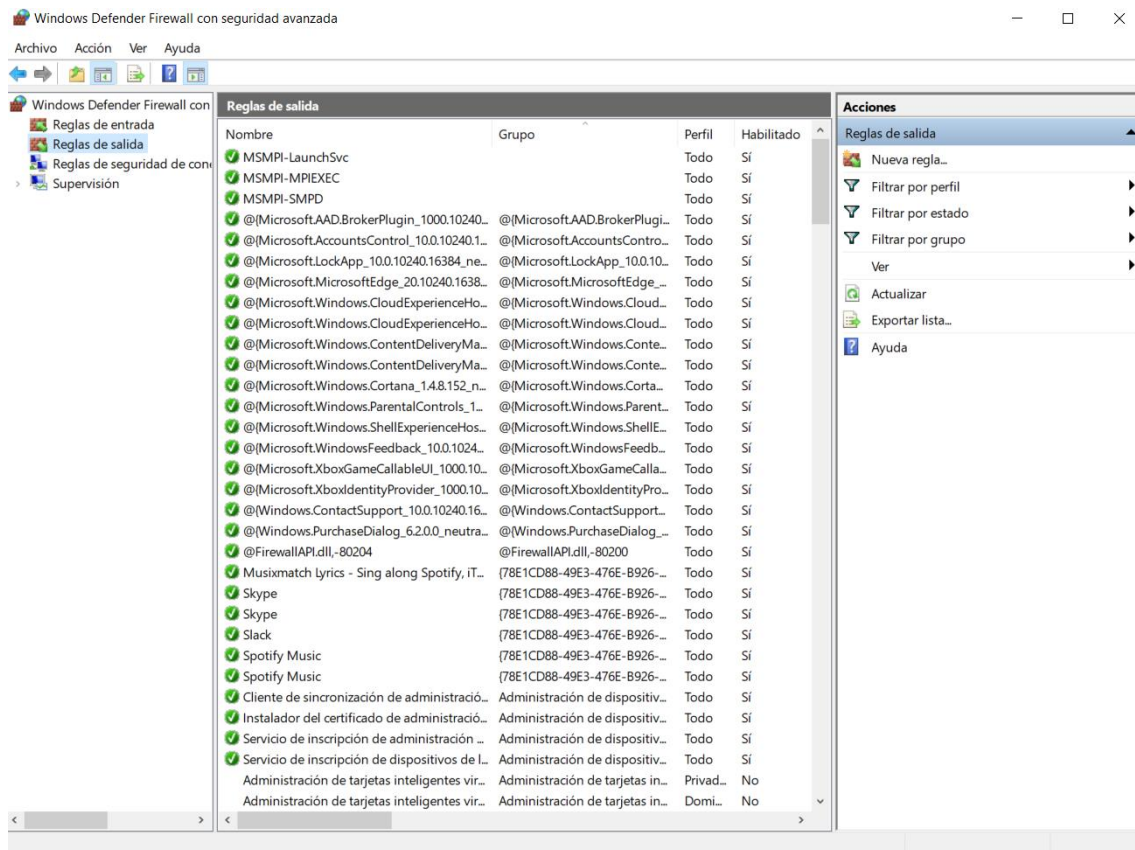


Figura 1.6.

En la figura 1.6 tenim un panell de configuració avançada del tallafocs de Windows 10.

En l'apartat de tallafocs, des de la versió de Windows Vista, disposa d'un tallafocs integrat en el sistema, però no està integrat en el seu nucli (kernel) a diferència de Linux, la qual cosa fa d'un sistema Windows un sistema més vulnerable.

Quant a antimalware i antivirus de Microsoft ofereix, un antivirus propi i gratuït: Microsoft Security Essentials. La seva potència i fiabilitat és bastant qüestionable, encara que garanteix nivells bàsics de seguretat. En Windows és millor usar programari de tercers per a protegir de malware: com Kaspersky, Colla, Avast...

1.1.3. Altres sistemes operatius

Entre altres sistemes operatius diferents a Windows i Linux, trobem el més conegut MacOS, així com també uns altres de gran ús com FreeBSD i SunOS.

A més, si parlem de dispositius mòbils (telèfons intel·ligents), generalment cadascun dels mateixos ja integren persé sistemes operatius propis com poden arribar a ser Android, iOS, Ubuntu Touch, Windows Phone, Kindle...

1.2. Permisos d'accés

Un dels nivells de seguretat esmentats és, sens dubte, el control d'accés. I quina mesura de seguretat no ho és quan el primer que et demanen és identificar-te? Això és el que ocorre en la majoria de SSOO que s'executen en els ordinadors però no en altres dispositius com a telèfons intel·ligents en els quals la part de la seguretat del telèfon ve gestionada tant per la targeta SIM com pel sistema operatiu que integri.

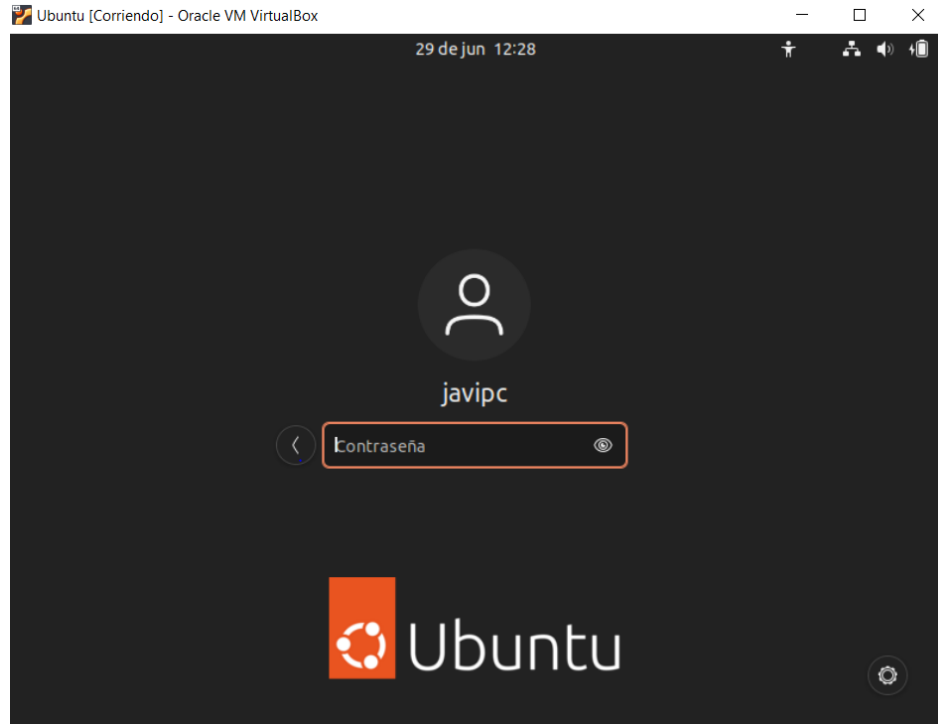


Figura 1.8

En la figura 1.8 observem el control d'accés d'un SO com Ubuntu Desktop 22.04 LTS (versió estable).

Amb el control d'accés no sols ens estem identificant davant el SO sinó que a més, estem indicant el nostre perfil d'accés que té aparellat nivells de seguretat dins del SO. És a dir, des que accedim al sistema tenim limitats segons quines accions i responsabilitats.

Habitualment, en els sistemes operatius, els usuaris estan agrupats en un grup com a mínim, però podent ser membre d'uns altres.

Els permisos sobre les carpetes poden ser gestionats tenint com referència no sols els usuaris sinó agrupar-los per grups i els membres d'aquests heretaran els permisos. No sols es gestionen els permisos sinó la denegació sobre recursos.

Podem seguir els principis següents:

- Si un recurs és denegat a un grup o usuari preval sobre la resta dels drets.
- Si a un recurs se li dona drets o privilegis per a un grup, tots els usuaris hereten aquests privilegis.

- Si a un usuari se li donen privilegis sobre un recurs, però no al grup, sollo l'usuari tindrà els privilegis.
- Herència de privilegis. Quan un usuari té privilegis sobre una carpeta, l'usuari heretarà els mateixos privilegis sobre les carpetes filles, Sempre que no se li denegui.

1.2.1. Tipus de accés

Depenent de la mena d'àrees en el qual es treballi, hi ha 3 tipus de control d'accés:

- **Control d'accés obligatori:** Es tracta d'una eina de control d'accés multinivell. Es defineix per a això una jerarquia de nivells de seguretat. És a dir, una política de rols que garanteixi la seguretat en l'accés de la informació.
- **Control d'accés discrecional:** Aquí tots els objectes tenen un propietari. És el propietari el que permet atorgar l'accés als diferents recursos (informació) a grups i/o usuaris
- **Control d'accés basat en rols:** Hi ha entorns en els quals és difícil detectar qui és el propietari dels recursos. En els sistemes basats en rols, els usuaris tens assignats rols basats en les seves funcions en el sistema. Aquests sistemes estan centralment administrats. És a dir, no tenen accés discrecional.

Sistemes Windows

Aquests sistemes contenen components de control i seguretat com els següents:

- Monitor de referència de seguretat que fa complir les polítiques de seguretat en l'equip local. Protegeix els recursos del sistema, audita i protegeix en temps d'execució els diferents objectes.
- L'administrador de recursos esborra, crea i administra objectes executius i tipus de dades abstractes que són utilitzats per a representar recursos del SO com a processos, fils i diversos objectes de sincronització.
- El procés del servidor d'autenticació de seguretat local en realitat realitza peticions d'autenticació.

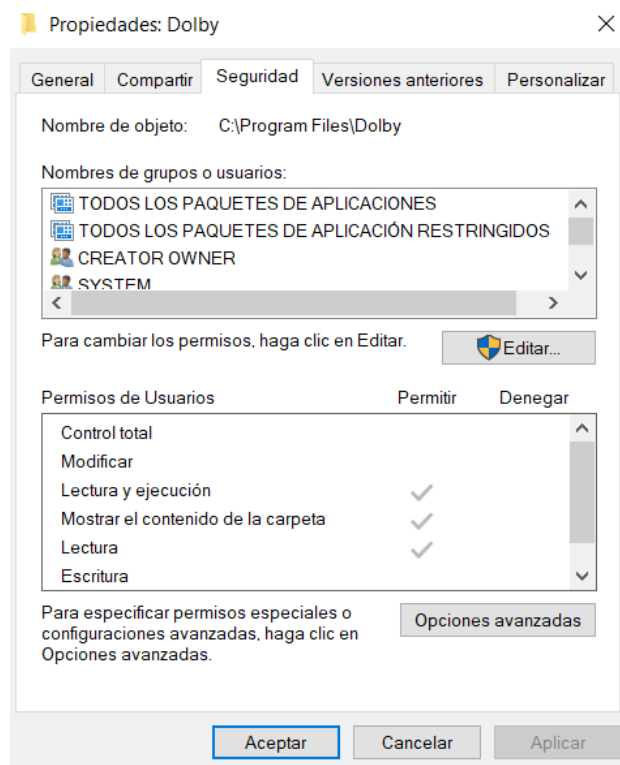


Figura 1.9.

Els sistemes Windows defineixen 13 permisos per a fitxers i directoris o carpetes. I proporciona fins i tot més opcions podent decidir si el permís serà “accés permès” o “accés denegat”:

- Recórrer carpeta/Executable.
- Lectura d'atributs.
- Lectura estesa d'atributs.
- Crear arxius/Escriure dades.
- Crear carpetes/Afegir dades.
- Escriure atributs
- Escriure atributs estesos.
- Eliminar subcarpetes i arxius.
- Esborrat.
- Lectura de permisos.
- Canvi de permisos.
- Prendre possessió..

I també es predefineixen permisos bàsics que són més intuïtius i hauria de ser suficient per a la majoria de les tasques comunes.

- Mostrar contingut de la carpeta
- Control total
- Modificar
- Lectura
- Escripura

- Llegir i executar

En la figura 1.9 observem usuaris i permisos per a l'usuari o grup sobre una carpeta. Aquests elements de permisos són els últims comentats. No obstant això, si pressionem en “Opcions avançades” podem desglossar de manera més especificada el nivell de permisos que es vol atorgar.

Sistemes Linux

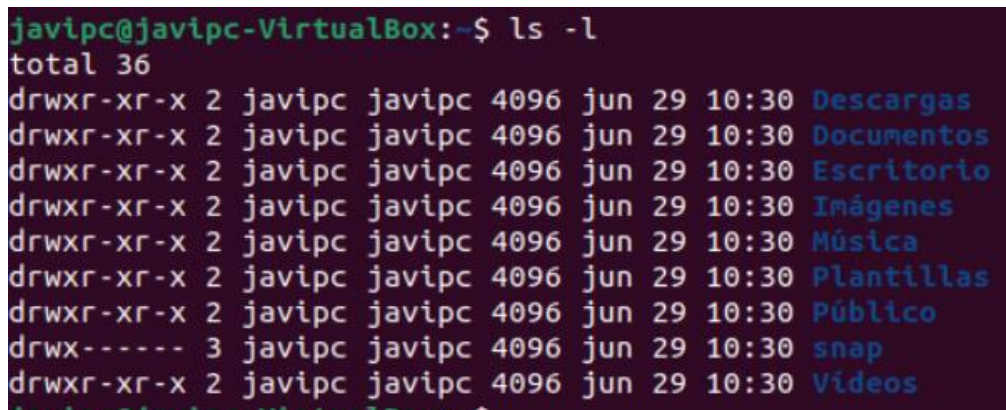
Normalment els SOs Unix i Linux implementen una protecció de control d'accés per als arxius que és bàsica a tres nivells. Els permisos es poden garantir a 3 nivells:

- **Usuari (u):** Especifica a l'usuari, probablement l'amo de l'arxiu o directori.
- **Grup (g):** Especifica els usuaris que pertanyen al mateix grup com l'indicat en l'arxiu o directori.
- **Altres (o):** Representa a la resta d'usuaris.

Per a cada classe podem seleccionar 3 tipus de permisos: **Lectura, Escriptura i Execució**.

Aquests bits de permisos es comproven en el següent ordre:

- Si el UID (User Identifier) de l'arxiu és el mateix que el UID del procés, només s'apliquen permisos de propietari; el grup i altres permisos no es comproven.
- Si els UID no coincideixen, però el GID (Group Identifier) de l'arxiu coincideix amb un dels GID del procés, s'apliquen només als permisos de grup; el propietari i altres permisos no es comproven.
- Només si el UID i GID del procés no coincideixen amb els de l'arxiu només es comproven els permisos per a “uns altres”. Si aquests permisos no permeten l'operació sol·licitada, es produirà un error.



```
javipc@javipc-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Descargas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Documentos
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Escritorio
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Imágenes
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Música
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Plantillas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Público
drwx----- 3 javipc javipc 4096 jun 29 10:30 snap
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Vídeos
```

Figura 1.10.

Unix/Linux defineix tres atributs addicionals:

- **SUID (Set User ID):** Després d'executar un arxiu, el procés creat en general té el seu ID d'usuari igual a l'ID de l'usuari que executa el programa. No obstant això, si el bit SUID es troba en un executable, el procés creat obté l'ID del propietari de l'arxiu.
 - Activació
 - **chmod u+s arxiu**

- Desactivació
 - **chmod u-s arxiu**
- **SGID (Set Group ID):** Un procés que normalment té l'ID de grup igual al grup de processos. No obstant això, si el bit SGID es troba en l'executable, se li assigna el procés que el seu ANEU de grup és el corresponent al grup d'arxius
 - Activació
 - **chmod g+s arxiu**
 - Desactivació
 - **chmod g-s arxiu**
- **Sticky Bit (bit pegadizo).**

En la **figura 1.10.** observem, en manera terminal, els drets i privilegis sobre dos arxius. S'observa el nom del propietari i el grup (el de l'esquerra és el propietari i el següent el grup). A la seva esquerra estan les propietats dels arxius o directoris i la seva representació és la següent:

- Si el primer bit és **d** és que es tracta d'un directori o carpeta.
- Els següents nou caràcters es divideixen en grups de 3:
 - Els primers 3 corresponen als atributs del fitxer o directori respecte al propietari indicat.
 - Els següents corresponen als atributs del fitxer o directori respecte al grup indicat.
 - I els últims 3 corresponen a la resta d'usuaris..

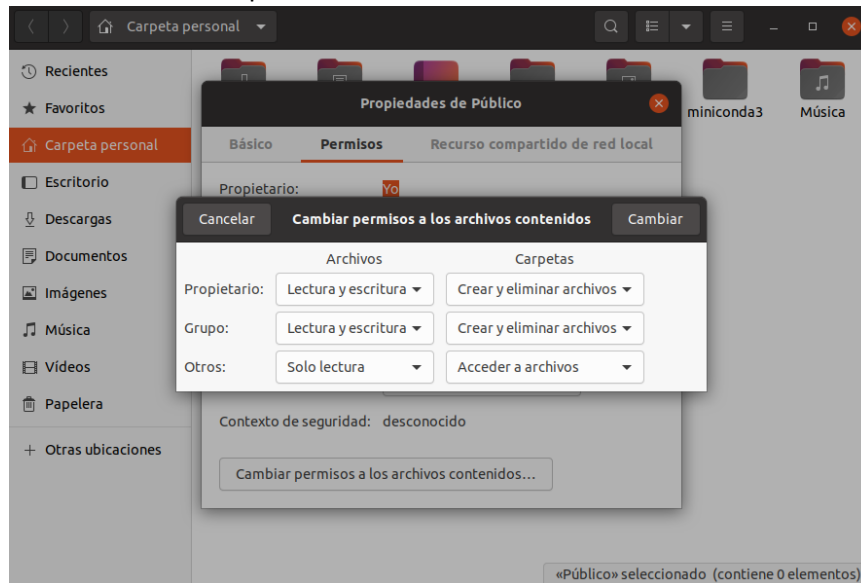


Figura 1.11.

En la **figura 1.11.** observem una finestra (també dita quadre de diàleg) del SO Ubuntu Desktop. Sota l'escriptori Unity.

S'observen els 3 elements diferenciadors: propietari, grup i altres. Amb dues columnes: arxius i carpetes. També podem observar els permisos concrets que s'estableixen en cada cas per al directori seleccionat.

1.2.2. Elecció de la mena d' accés

Prendrem com a referència els SSOO Linux i Windows per ser els més emprats. Hem de conèixer que Mac OS X és un SOTA de tipus Unix. Pel fet que Mac és compatible amb POSIX, la gran majoria de paquets escrits per a BSD o Linux poden ser recompilats per a ser executats en Mac.

Però, quin és el tipus d'accés que hem de triar?

Gairebé tots els SSOO, en manera local, permeten l'ús de l'ordinador a diversos usuaris. Segurament, aquests SSOO no necessiten d'un servidor per a comunicar-se entre si. És el cas de Mac OS X, Windows i Linux.

I què implica? Que en una xarxa local poden comunicar-se els ordinadors entre si en una arquitectura d'igual a igual. Això fa pensar que un usuari del nostre equip pot accedir des d'un altre ordinador o dispositiu mitjançant unes credencials si és que està lliure l'accés.

Aquests sistemes generen, a cada usuari, una zona “privativa” que podem compartir tota o part, de lectura i/o escriptura amb altres usuaris (o a tots). Hem de recordar que l'usuari administrador o l'usuari que tingui perfil d'administrador podran recórrer qualsevol part del nostre equip.

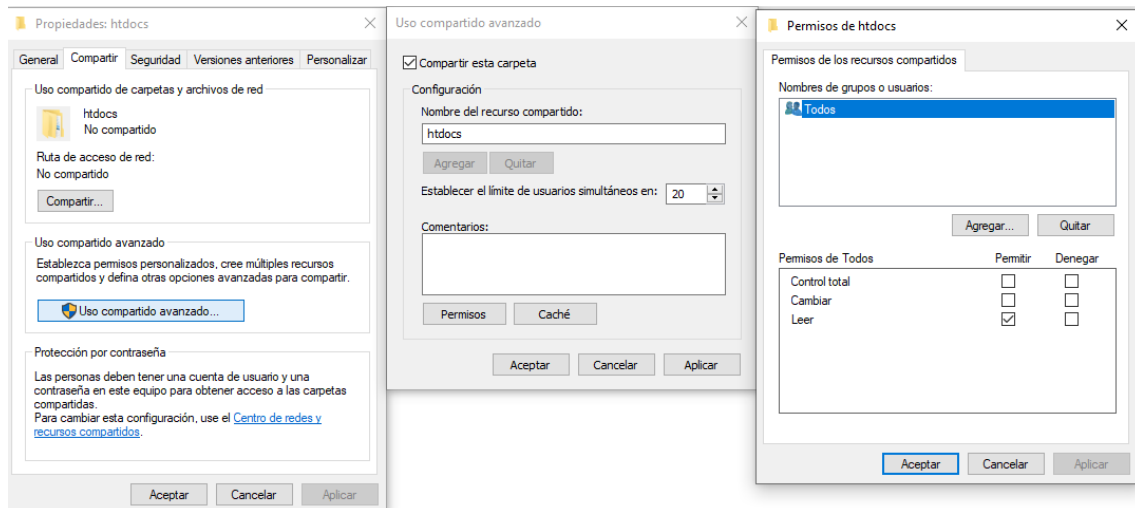


Figura 1.12.

Posant com a exemple la imatge de la **figura 1.12**. Intentem compartir una carpeta o directori. Com? Seleccionem la carpeta que volem compartir i, amb el menú contextual, seleccionem propietats i, aquí, seleccionarem la pestanya compartir i podrem configurar la compartició. No oblidem que estem configurant l'accés i hem de configurar la pestanya “Seguretat” per a no crear conflictes de permisos.

Una forma més ràpida és, seleccionant la carpeta objecte de compartició, amb el menú contextual, seleccionar l'opció “compartir amb” on podrem seleccionar els usuaris amb aquells que volem compartir la carpeta o directori.

Per descomptat, el millor sistema de compartició de recursos és a través d'un servidor. Tots els aspectes de compartició i gestió de recursos queden en mans d'un SOTA (Servidor) la fi del qual és aquest mateix.

1.2.3. Implementació d' accessos

S'ha esmentat en l'anterior punt que hem d'adequar els permisos de la pestanya "seguretat" amb els permisos de compartició.

També s'ha comentat que els usuaris administrador i aquells que tinguin perfil del grup administradors no tindran cap problema en el mateix moment d'accedir a uns recursos del sistema. Però no ocorre el mateix amb aquells usuaris que tenen perfil de "usuari estàndard". És per això que hem de "afinar" els permisos tant per als grups, si estan agrupats, com per als usuaris si volem que puguin fer les tasques ja definides sobre el recurs.

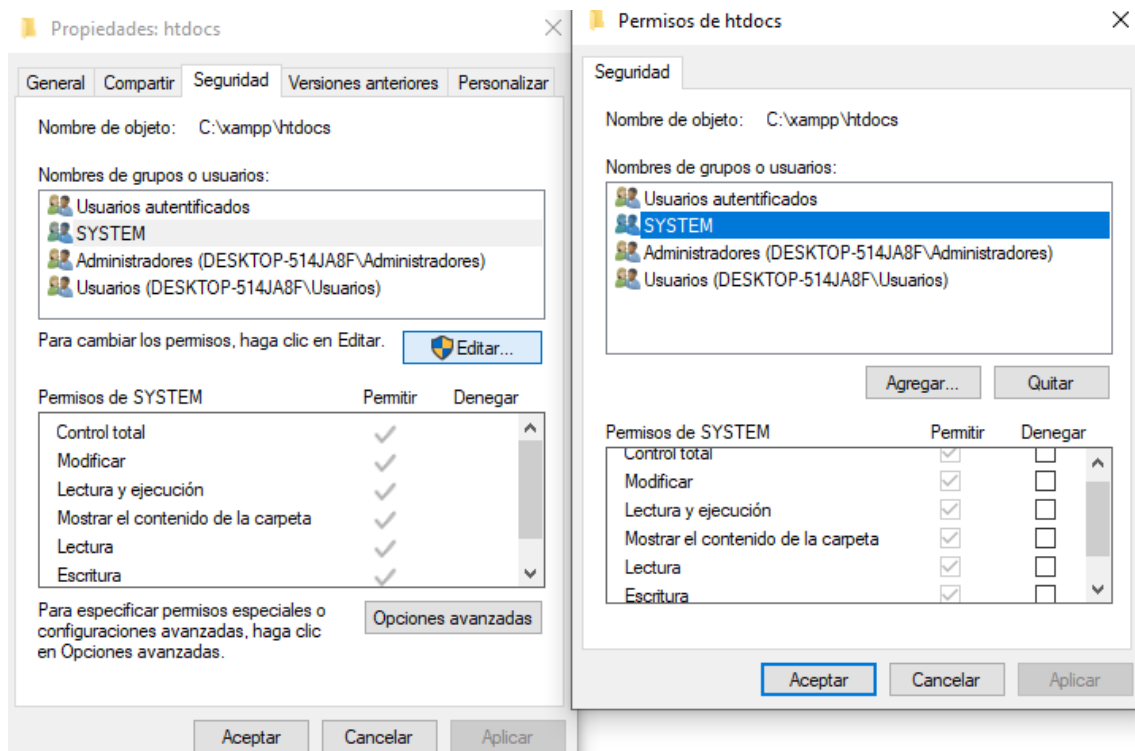


Figura 1.13.

En la **figura 1.13.** observem, en la part esquerra de la imatge, com estan els permisos per al grup **SYSTEM**. Si desitgem conèixer els permisos d'un altre component, n'hi ha prou amb seleccionar-lo perquè apareguin els permisos actuals que tenen assignats. Si es volen modificar els permisos o afegir un usuari o grup premerem el botó "Opciones avanzadas". Ens portarà a una finestra (quadre de diàleg) que està a la dreta de la imatge. En aquesta finestra podrem agregar nous permisos i modificar els actuals que té assignat el grup SYSTEM.

1.3. Ordres de creació, modificació i esborrat.

En el cas de voler realitzar un projecte serà una bona idea crear una carpeta on es guardi, organitzadament, cadascun dels arxius que tenen referència al projecte. Si parlem d'un projecte web aquest constatarà d'arxius HTML, CSS, JavaScript, imatges i documentació relacionada amb el projecte.

Quan l'autor indica “organitzadament” es refereix a separar els diferents tipus d'arxius en carpetes. És a dir, dins de l'arrel de la carpeta “projecte” crear una carpeta que es cridi “CSS”, una altra “imatges”, etc. Només s'esmenta com a orientació.

1.3.1. Descripció d' ordres en diferents sistemes

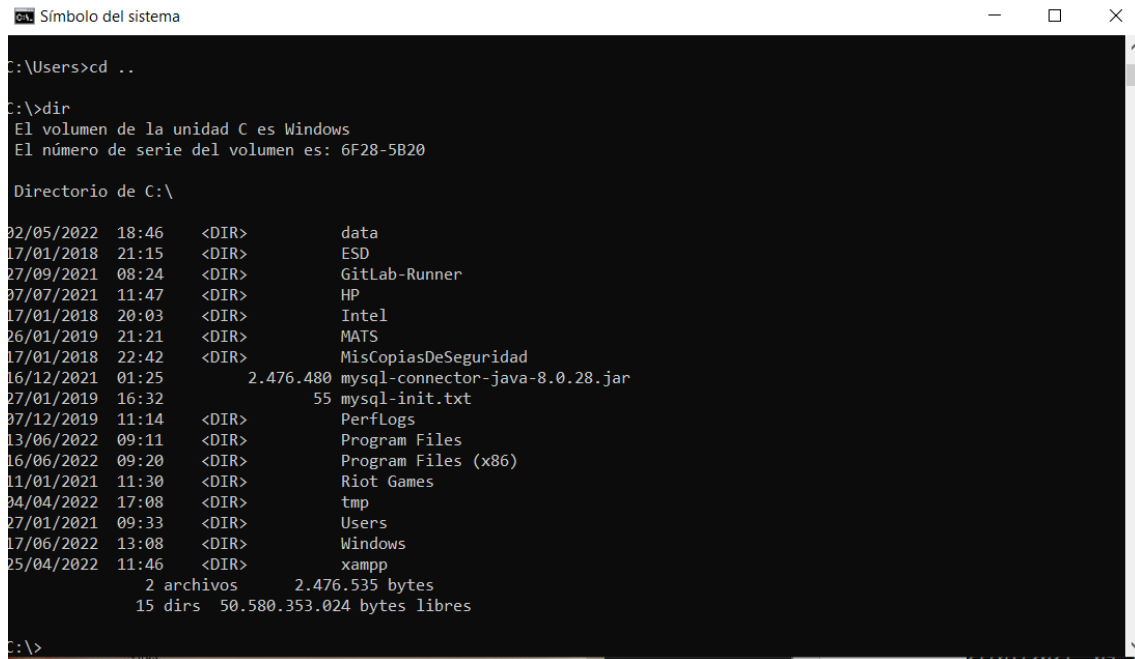
Els sistemes operatius moderns tenen desenvolupat una interfície gràfica intuïtiva que ens permet realitzar tots els processos de creació, modificació i esborrat tant d'arxius com de carpetes. Això no significa que l'ús d'ordres a través de la consola quedi apartat, encara que les persones que utilitzen l'ordinador a “nivell d'usuari” creguin que no són necessàries.

Com podem executar us comandos en manera consola? Perquè dependrà del sistema operatiu amb el qual estem treballant. No seran els mateixos ordres en Windows que en GNU/Linux. El sistema operatiu Mac OS X utilitza moltes ordenis i/o comandos igual que Linux i amb les mateixes funcionalitats.

Repassem dos sistemes operatius molt utilitzats: Windows i GNU/Linux.

WINDOWS

Per a obtenir l'entrada en consola o també denominada terminal hem d'escriure **cmd** en l'opció inicio -> buscar. Aconseguirem que ens aparegui una “pantalla negra” similar a la representada en la figura 1.14. Normalment ens mourem en la zona assignada a l'usuari (tal com apareix en la imatge esmentada). També observem com apareixen carpetes o directoris i arxius indicant l'ordre **dir**.



```

C:\Users>cd ..

C:\>dir
El volumen de la unidad C es Windows
El número de serie del volumen es: 6F28-5B20

Directorio de C:\

02/05/2022  18:46    <DIR>          data
17/01/2018  21:15    <DIR>          ESD
27/09/2021  08:24    <DIR>          GitLab-Runner
07/07/2021  11:47    <DIR>          HP
17/01/2018  20:03    <DIR>          Intel
26/01/2019  21:21    <DIR>          MATS
17/01/2018  22:42    <DIR>          MisCopiasDeSeguridad
16/12/2021  01:25    2.476.480 mysql-connector-java-8.0.28.jar
27/01/2019  16:32    55 mysql-init.txt
07/12/2019  11:14    <DIR>          PerfLogs
13/06/2022  09:11    <DIR>          Program Files
16/06/2022  09:20    <DIR>          Program Files (x86)
11/01/2021  11:30    <DIR>          Riot Games
04/04/2022  17:08    <DIR>          tmp
27/01/2021  09:33    <DIR>          Users
17/06/2022  13:08    <DIR>          Windows
25/04/2022  11:46    <DIR>          xampp
                2 archivos    2.476.535 bytes
                15 dirs    50.580.353.024 bytes libres

C:\>

```

Figura 1.14.

Una vegada que tenim la consola oberta podrem utilitzar els comandos i moure'ns per les carpetes utilitzant, per a això, les ordres o comandos que ens ofereix el sistema. Les ordres o comandos que s'utilitzen són aquells que es van crear amb el sistema operatiu MS-DOS, sistema operatiu de Microsoft anterior a la sèrie Windows.

De següent manera, es mostrarà amb algun exemple, les ordres que s'utilitzen per a la creació, modificació i esborrat d'arxius i directoris.

- Ordre **dir**: Amb aquesta ordre obtenim informació dels arxius i directoris que estan en la ubicació indicada com a paràmetre. **Sintaxis**:
 - **Sintaxi**
 - dir [unidad\directorio\fichero]
 - **Paràmetres**:
 - Alguns dels paràmetres que es poden emprar per a actualitzar el llistat de directoris i arxius són els següents:
 - **/P ->** Mostra per pantalla el llistat, per a visualitzar la pantalla següent n'hi ha prou amb prémer una tecla. En prémer la tecla es processarà el següent bloc de llistat i així successivament.
 - **/O**
 - **/ON**
 - **/OE**
 - **/OG**
 - **/OS**
 - **/OD**
 - **/O-X**
 - **/S**
- Ordre **cd**: Permet canviar de directori al qual se li especifiqui en la ruta.
 - **Sintaxi**

- `cd [unidad:]\[ruta]\[directorio]`
- **Observació**
 - Si desitgem baixar un nivell en l'arbre de directoris, només és necessari escriure **cd**.
 - Nota: S'han de tenir en compte els valors de rutes relatives al directori actiu o rutes absolutes que seran independents del directori actiu.
- **Ordre **md** o **mkdir**:** crea un directori o carpeta en la ruta que s'especifiqui.
 - **Sintaxi:**
 - `md [unidad\ruta\] <nombre>`
 - En alguns casos es pot fer `mkdir dir1\dir2` i seria equivalent a les següents accions: `mkdir dir1; cd dir1; mkdir dir2; cd dir2;`
- **Ordre **rd**:** Esborra un directori (només si està buit).
 - **Sintaxi**
 - `rd [unidad\ruta\]<nombre>`
 - **Paràmetres**
 - Els paràmetres que es poden utilitzar amb aquest comando són:
 - **/S** -> Elimina tot el directori a esborrar, encara que no estigui buit, però demana confirmació.
 - **/O** -> No demana confirmació per a eliminar un arbre de directoris quan s'utilitza juntament amb l'opció.
- **Nota:** Disposem d'altres comandos per a gestionar arxius com, per exemple:
 - **rename:**
 - Canvia de nom un arxiu
 - **del:**
 - Elimina un arxiu
 - **move:**
 - Mou un arxiu

Si desitgem conèixer **més informació d'un comando** podem utilitzar el paràmetre `/?`. Per exemple: **dir /?** Ens ofereix informació d'ajuda.

GNU/LINUX

En el cas de GNU/Linux utilitzarem l'ordre "terminal" per a accedir a la consola. Com el sistema operatiu Linux és multiterminal podem passar de l'entorn gràfic a manera terminal prement simultàniament CTRL-ALT-F2 i obtindrem accés al terminal 2 (tty2). Per a passar a l'acaba on "corre" l'entorn gràfic utilitzarem CTRL-ALT-F7.

```
javipc@javipc-VirtualBox:~$ ls -all
total 68
drwxr-x--- 14 javipc javipc 4096 jun 23 14:07 .
drwxr-xr-x  3 root   root   4096 jun 23 13:23 ..
-rw-r--r--  1 javipc javipc  220 jun 23 13:23 .bash_logout
-rw-r--r--  1 javipc javipc 3771 jun 23 13:23 .bashrc
drwx----- 10 javipc javipc 4096 jun 27 11:29 .cache
drwx----- 11 javipc javipc 4096 jun 27 10:44 .config
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Descargas
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Documentos
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Escritorio
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Imágenes
drwx-----  3 javipc javipc 4096 jun 23 14:07 .local
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Música
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Plantillas
-rw-r--r--  1 javipc javipc  807 jun 23 13:23 .profile
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Público
drwx-----  3 javipc javipc 4096 jun 23 14:07 snap
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Videos
```

Figura 1.15.

En la imatge 1.15 observem la finestra de “terminal” en una distribució Ubuntu Desktop.

A continuació, vam mostrar les ordres utilitzades per a gestionar arxius a través de la terminal.

INSTRUCCIÓ	¿QUÈ FA?
cd [directori]	Canvia el directori per l'especificat com a paràmetre.
mkdir directori	Crea un nou directori.
rmdir directori	Esborra un directori buit
mv fitxer [fitxer 2... fitxerN] destí	Mou o canvia de nom fitxers o directoris
rm fitxer1 [fitxer2... fitxerN] destí	Esborra fitxers i directoris amb el paràmetre -R (recursivo)
cp fitxer1 [fitxer2... fitxerN] destí	Còpia fitxers i directoris en el directori indicat.
pwd	Mostra en pantalla la ruta completa del directori actual o actiu.

Aquestes ordres tenen la mateixa funcionalitat en sistemes operatius Mac OS X.

1.3.2. Implementación y comprobación de las distintas órdenes

na manera de comprovar si les accions realitzades que utilitzen els comandos és mitjançant l'explorador d'arxius. A través de l'explorador d'arxius, independentment del SO amb el qual treballem, ens facilita explorar de forma més àmplia i global si cap, l'estructura dels directoris o carpetes i els arxius que el contenen.

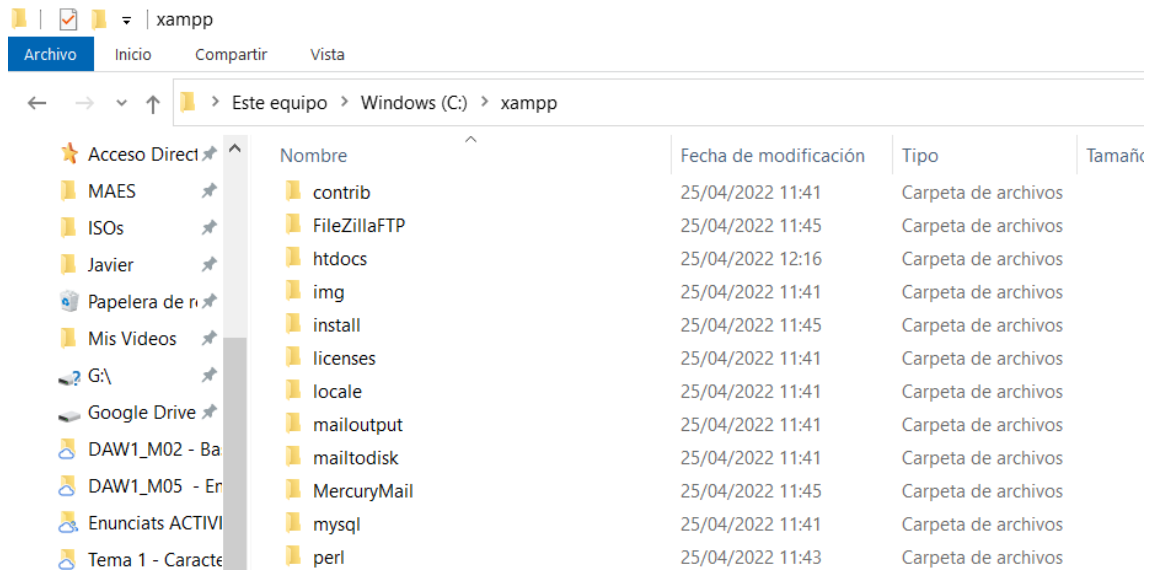


Figura 1.16.

En la figura 1.16 observem la navegació gràfica. Això marca una diferència quant a l'ús de comandos a través de la consola. Encara que la realització de tasques resulti més ràpida amb comandos de consola resulta sempre més còmode de cara a l'usuari comú accedir i manipular la informació des de l'explorador d'arxius.

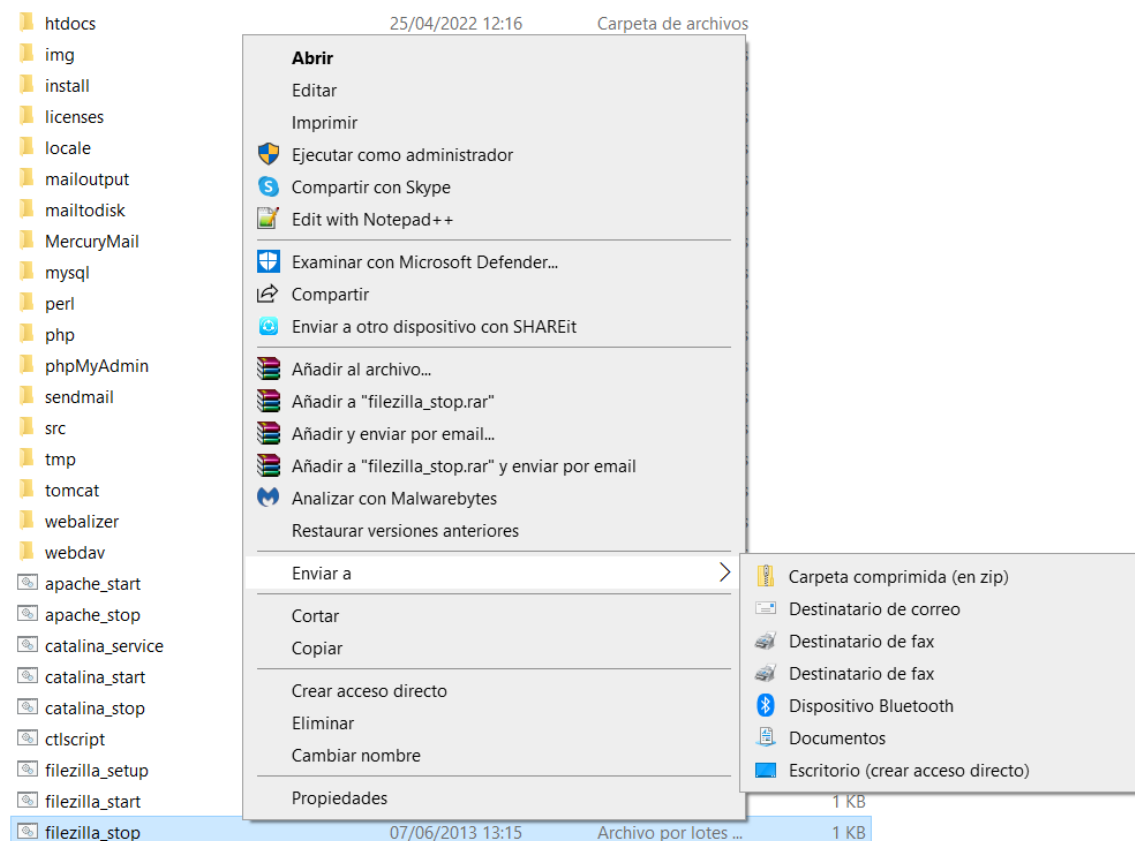


Figura 1.17.

Independentment de les opcions que es troben en la barra de tasques, també disposem d'un menú contextual que ens permet realitzar més operacions sobre un arxiu o directori com podem observar en la figura 1.17.

Totes aquestes eines programari permeten realitzar operacions sobre el sistema d'arxius.

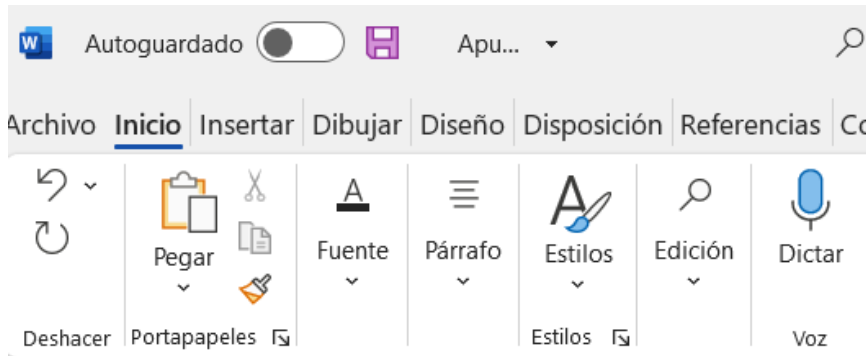


Figura 1.18

Com es veu en la figura 1.18, alguns paquets d'ofimàtica com a Office o eines com DreamWeaver o Notepad++, disposen d'opcions que permeten la creació i modificació dels documents de la zona del sistema d'arxius al qual tinguem accés i privilegis per a fer-lo.

Tornant a l'eina gràfica de l'explorador d'arxius. Amb aquesta eina del SO es poden dur a terme tasques de manera còmoda. Si posem un exemple, en copiar, moure un fitxer d'una carpeta a una altra podem utilitzar el "arrossegament" del document. Com es fa? Estem situats sobre l'àrea on està el document, obrim un altre explorador de documents i ens situem sobre la carpeta que volem moure o copiar el document, "punxem" amb el botó esquerre del ratolí sobre el document objecte i, sense deixar anar el botó del ratolí, el movem a l'altre explorador i "deixem anar" el botó.

També podem utilitzar sempre el sistema de dreceres. El sistema de dreceres és combinant tecles del teclat. Per exemple, si sobre el document seleccionat pressionem CTRL-X el document redueix la intensitat del seu color i el marca de manera que s'està tallant. Per a passar-ho a una altra part pressionem CTRL-V.

En cas de copiar utilitzarem CTRL-C + CTRL-V.

Bibliografia

Publicación de páginas Web MF0952_2 – Autor: José Talledo San Miguel – Certificado de Profesionalidad IFCD0110. Confección y publicación de páginas web. MF0952_2