MEDAC
Instituto Oficial de Formación Profesional

DESPLIEGUE DE APLICACIONES WEB
TÉCNICO EN DESARROLLO DE APLICACIONES WEB

Instalación de un servicio de transferencia de archivos en servidor

10

ÍNDICE

 ISBN: 978-84-18983-26-9

OBJETIVOS

Instalar y configurar un servidor de transferencia de archivos.

Aplicar configuraciones básicas sobre usuarios.

Utilizar el protocolo seguro de transferencia de archivos.

Utilizar un servidor de transferencia sobre el navegador web.

/ 1. Introducción y contextualización práctica

En esta unidad, aprenderemos cómo instalar y configurar servidores de transferencia de datos.

Comenzaremos con el proceso básico de instalación y continuaremos creando usuarios para acceder a la información.

Hablaremos también, de los diferentes modos de funcionamiento de un servidor de transferencia y además implementaremos el protocolo seguro SSL.

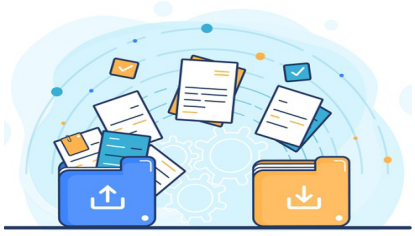

Fig. 1. Administración de servidores de aplicaciones web.

Planteamiento del caso práctico de la unidad

A continuación, vamos a plantear un caso páctico.

Escucha el siguiente audio donde planteamos la contextualización práctica de este tema, encontrarás su resolución en el apartado Resumen y Resolución del caso práctico.

Audio intro. "Caso práctico inicial"
https://bit.ly/3gtmXHc

/ 2. Instalación y configuración del servicio ftp

Para configurar un servidor de transferencia de archivos usaremos el **paquete VSFTPD** (*Very Secure FTP Daemon*). VSFTPD es un **servidor FTP** para **sistemas Linux con licencia GNU *Open Source*** que se presenta como un servidor de transferencia seguro y de alto rendimiento. Algunas de sus **características** son:

- Usuarios virtuales.
- Direcciones IP virtuales.
- Control de ancho de banda.
- Encriptación SSL.

La instalación en *Ubuntu* es tan sencilla como ejecutar el siguiente comando:

```
usuario@ubntdesktop01:~$ sudo apt-get update
usuario@ubntdesktop01:~$ sudo apt-get install vsftpd
```

Código 1. Instalación VSFTPD Ubuntu.

La configuración de este servidor FTP se realiza a través de dos ficheros fundamentales:

- **/etc/vsftpd.conf**: Fichero principal de configuración. Almacena la mayoría de los parámetros que afectan al funcionamiento del servidor de transferencia.
- **/etc/ftpusers**: El fichero *ftpusers* contiene una lista de usuarios que no podrán iniciar sesión en el demonio FTP.

En el siguiente enlace, podremos encontrar un listado completo de todas las configuraciones que podemos realizar en el fichero vsftpd.conf

Fig. 2. Inicio del fichero vsftpd.conf

VSFTPD almacena registros de los accesos, tanto fallidos como autorizados, en el fichero **vsftpd.log**, que se encuentra en el directorio de logs (/var/log).

```
usuario@ubntdesktop01:~$ sudo cat /var/log/vsftpd.log
Wed Jul 22 10:56:39 2020 [pid 7280] CONNECT: Client "::ffff:192.168.0.21"
Wed Jul 22 10:56:42 2020 [pid 7272] [anonymous] FAIL LOGIN: Client "::ffff:192.168.0.21"
Wed Jul 22 10:59:13 2020 [pid 7603] [ftp] OK LOGIN: Client "::ffff:192.168.0.21", anon password "chrome@example.com"
```

Código 2. Log de vsftpd.

Audio 1. "Servidor SCP".
https://bit.ly/34IQDOr

/ 3. Configuración acceso anónimo

La utilización de usuarios anónimos permite **iniciar sesión en un servidor FTP** sin necesidad de tener una **cuenta de usuario** validada en dicho host. Habitualmente se utiliza la combinación de usuario y contraseña ***anonymous / guest***.

Esta funcionalidad, permite crear una carpeta pública que podría utilizarse como **repositorio de información**. No obstante, el uso de usuarios anónimos podría suponer una brecha de seguridad en el servidor si no tenemos en cuenta algunos factores en la configuración.

El proceso para habilitar el acceso anónimo se realiza editando el fichero de configuración **vsftpd.conf**. Habilitaremos la opción "**anonymous_enable=YES**", aunque también debemos crear una carpeta dedicada al acceso público para no exponer la seguridad del servidor.

```
:~$ sudo mkdir /home/anonymous
:~$ sudo chown ftp:ftp /home/anonymous/

:~$ sudo nano /etc/vsftpd.conf
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
write_enable=YES
anon_root=/home/anonymous
anon_upload_enable=YES
anon_mkdir_write_enable=YES

:~$ sudo service vsftpd restart
```

Código 3. Configuración de usuarios anónimos.

```
ftp> open 192.168.0.24
Conectado a 192.168.0.24.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Usuario (192.168.0.24:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
file1
file2
file3
226 Directory send OK.
ftp: 24 bytes recibidos en 0.01segundos 3.00a KB/s.
ftp> mkdir dir1
257 "/dir1" created
```

Código 4. Prueba de conexión anónima a un servidor FTP.

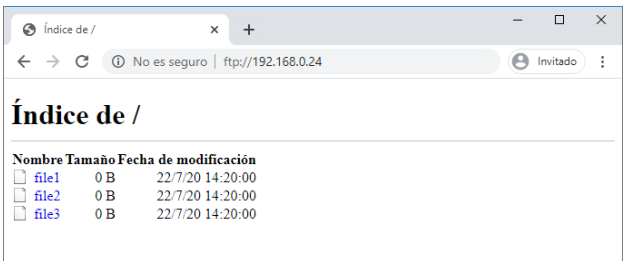

Fig. 3. Prueba de conexión anónima a un servidor FTP vía web.

/ 4. Creación de usuarios locales FTP

En este punto, crearemos usuarios para poder iniciar sesión en el servidor FTP y acceder a la información. En el servidor VSFTPD podemos encontrar usuarios de dos tipos:

- Usuarios locales del propio sistema Linux.
- Usuarios virtuales.

A la hora de crear **usuarios locales**, debemos tener en cuenta aspectos esenciales para la seguridad del sistema. El más importante es **evitar que un usuario FTP pueda iniciar sesión sobre el servidor**. Para ello, crearemos el usuario con el argumento –s para que el usuario no pueda acceder a la Shell:

```
:~$ sudo useradd ftp01 -s /usr/sbin/nologin -d /home/ftp01 -m
:~$ sudo passwd ftp01
```

Código 5. Log de vsftpd..

Para poder limitar el acceso a la Shell tendremos que añadir al fichero **/etc/shells** una línea con el valor **/usr/sbin/nologin**.

En este momento, el usuario que acabamos de crear podrá iniciar sesión en el servidor FTP, pero **no conectar por SSH**. Sin embargo, sí que podrá navegar entre los diferentes directorios y acceder a carpetas del sistema.

```
ftp> open 192.168.0.24
Conectado a 192.168.0.24.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Usuario (192.168.0.24:(none)): ftp02
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> cd /etc
250 Directory successfully changed.
ftp> pwd
257 “/etc” is the current directory
```

Código 6. Conexión a un servidor FTP y navegación entre directorios.

Para evitar esto, utilizaremos la herramienta **chroot**, que "enjaulará" el directorio raíz del usuario impidiendo acceder a carpetas de otros usuarios. Este cambio lo realizaremos en el fichero **vsftpd.conf**.

```
# Uncomment this to allow local users to log in.
local_enable=YES
chroot_local_user=YES
allow_writeable_chroot=YES
#
# Uncoment this to allow local user without shell access
check_shell=NO
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

Código 7. Fichero de configuración vsftpd.conf.

Tras realizar la configuración, no se podrá salir del directorio asignado al usuario.

```
ftp> cd /home
550 Failed to change directory.
ftp> cd /etc
550 Failed to change directory.
```

Código 8. Conexión FTP.

Vídeo 1. "Usuarios locales en FTP".
https://bit.ly/3aWkqnS

/ 5. Caso práctico 1: "Creación de usuarios FTP"

Planteamiento: En la empresa en la que trabaja Blanca, necesitan implementar un servidor FTP para que los desarrolladores puedan compartir información con el departamento de Operaciones.

Aunque no necesitan limitar el acceso a las diferentes carpetas, sí que necesitan poder tener un registro de los movimientos que se realizan. Por este motivo, han decidido crear un usuario personalizado para cada persona que necesite acceder al servidor.

Nudo: ¿Qué procedimiento deberá seguir Blanca para crear los usuarios?

Desenlace: Como el servidor será para uso interno de la empresa y no estará expuesto a internet, Blanca podrá crear usuarios de sistema para dar acceso a los diferentes usuarios.

Como medida de protección, al crearlos limitará el acceso al servidor, de manera que solo podrán iniciar en el demonio FTP.

```
:~$ sudo useradd dev1 -s /usr/sbin/nologin -d /home/dev1 -m
:~$ sudo passwd dev1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Código 9. Creación de usuario limitando el acceso a SHELL.

Si el usuario intentase iniciar sesión usando SSH, el servidor rechazará la conexión y mostrará el siguiente mensaje:

```
PS C:\Users\Miguel> ssh dev1@192.168.1.153
dev1@192.168.1.153's password:
This account is currently not available.
Connection to 192.168.1.153 closed.
```

Código 10. Conexión SSH rechazada por el servidor.

/ 6. Creación de usuarios virtuales

A diferencia de los usuarios locales, que se crean en el sistema operativo, los **usuarios virtuales** se almacenarán en una base de datos y se usarán únicamente **para iniciar sesión en el servidor FTP**. Para aplicar esta configuración, utilizaremos ***Berkeley DB y PAM***, un mecanismo de autenticación por módulos que nos permitirá enlazar la base de datos de usuarios con *vsftpd*.

En primer lugar, instalaremos *Berkeley DB* y crearemos una carpeta para almacenar la base de datos. Acto seguido, crearemos un fichero en texto plano con la relación de usuarios y contraseñas que posteriormente 'hashearemos' utilizando el comando **db_load** para convertir en un fichero con extensión .db

```
sudo apt-get install db5.3-util
sudo mkdir /etc/vsftpd
sudo nano /etc/vsftpd/vusers
 usuario1
 passwd1
 usuario2
 passwd2
sudo db5.3_load -T -t hash -f /etc/vsftpd/vusers /etc/vsftpd/vusers.db
sudo chmod 600 /etc/vsftpd/vusers.db
```

Código 11. Instalación db5.3

Continuamos con códigos de configuración:

```
sudo nano /etc/pam.d/vsftpd.v
 #%PAM-1.0
 auth      required     pam_userdb.so db=/etc/vsftpd/vusers crypt=hash
 account   required     pam_userdb.so db=/etc/vsftpd/vusers crypt=hash
 session   required     pam_loginuid.so
```

Código 12. Configuración fichero vsftpd.v

```
sudo nano /etc/vsftpd.conf
 listen=NO
 listen_ipv6=YES
 anonymous_enable=NO
 local_enable=YES
 pam_service_name=vsftpd.v
 guest_enable=YES
 guest_username=ftp
 user_sub_token=$USER
 local_root=/home/vusers/$USER
 hide_ids=YES
 virtual_use_local_privs=YES
 write_enable=YES
 chroot_local_user=YES
 allow_writeable_chroot=YES
 local_umask=022

sudo mkdir /home/vusers
sudo chown ftp:ftp /home/vusers/
sudo mkdir /home/vusers/usuario1
sudo chown ftp:ftp /home/vusers/usuario1/
sudo service vsftpd restart
```

Código 13. Fichero de configuración vsftpd.conf y creación de directorios de usuarios. https://www.geekpills.com/operating-system/linux/vsftpd-ftp-server-with-virtual-users

```
ftp> open 192.168.1.153
Conectado a 192.168.1.153.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Usuario (192.168.1.153:(none)): usuario1
331 Please specify the password.
Contraseña:
230 Login successful.
```

Código 14. Prueba de conexión al servidor FTP con usuarios virtuales.

En caso de necesitar crear más usuarios, editaremos el fichero "***vusers***" y volveremos a utilizar el comando *db_load*. También, será necesario, crear una carpeta en el directorio que hemos asignado (/home/vusers/) y asignar la propiedad al usuario FTP.

/ 7. Cuotas y FTP activo/pasivo

- **Configuración de cuotas**

  Cuando configuramos un **servidor de transferencia de archivos**, un aspecto fundamental, es **limitar la cantidad de información** que cada usuario podrá almacenar. Esto es posible gracias al uso de **cuotas de disco.**

  El uso de cuotas impide que un solo usuario sature el servidor web. Estableciendo dos tipos de límites:

  - **Límite duro**: Fija la cantidad máxima de información que se podrá almacenar.
  - **Límite blando**: Fija un umbral por debajo del límite duro que, una vez sobrepasado, avisará al usuario.

En sistemas Linux, podemos configurar el uso de cuotas de disco con la utilidad llamada ***quota***. En el siguiente enlace encontrarás un manual para instalar y configurar *quota* en Ubuntu 18.04:

Fig. 4. Instalación y configuración de quota.

- **Configuración FTP activo/pasivo**

  En el **modo activo** de FTP, el cliente abre la conexión a un **puerto aleatorio del servidor (>1024)**. Esto puede provocar problemas de conexión si el servidor estuviera tras un **firewall**.

  En cambio, en el **modo pasivo**, el cliente inicia la conexión al **puerto 21 del servidor**, y éste abrirá un puerto aleatorio en el que se establecerá la conexión.

  En la configuración del modo pasivo, podemos definir el grupo de puertos que se utilizarán en las conexiones. Esto se realiza editando el fichero **vsftpd.conf**.

```
pasv_enable=YES
pasv_min_port=10000
pasv_max_port=10100
```

Código 15. Fichero vsftpd.conf – Configuración modo pasivo

Tras reiniciar el servicio, ya tendremos configurado el **demonio FTP** para aceptar conexiones en modo pasivo.

/ 8. FPT SSL. Cifrando la conexión

Como ya sabemos, FTP realiza el intercambio de contraseñas en **texto plano, es decir sin cifrar.** Para asegurar la conexión, podemos utilizar **certificados SSL**, así como forzar el uso de conexiones cifradas que eviten posibles brechas de seguridad.

Los pasos a seguir para securizar las conexiones de nuestro servidor son los siguientes:

1. **Crear el certificado SSL.**

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/
private/vsftpd.pem
```

Código 16. Generación de certificados SSL. https://www.digitalocean.com/community/tutorials/how-to-configure-vsftpd-to-use-ssl-tls-on-a-centos-vps

2. **Editar el fichero de configuración de *vsftpd***. Añadiremos los certificados que hemos generado y activaremos SSL. Podemos incorporar otras configuraciones para forzar el uso del protocolo seguro tanto en transferencia de información como en el login.

```
:~$ sudo nano /etc/vsftpd/vsftpd.conf
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Código 17. Fichero vsftpd.conf – Configuración SSL

3. **Reinicio del servicio para aplicar cambios.**

```
usuario@srv-ftp-01:~$ sudo /etc/init.d/vsftpd restart
usuario@srv-ftp-01:~$ sudo /etc/init.d/vsftpd status
vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-07-25 11:32:24 UTC; 3s ago
  Process: 3555 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
 Main PID: 3563 (vsftpd)
    Tasks: 1 (limit: 2317)
   CGroup: /system.slice/vsftpd.service
           └─3563 /usr/sbin/vsftpd /etc/vsftpd.conf
jul 25 11:32:24 srv-ftp-01 systemd[1]: Starting vsftpd FTP server...
jul 25 11:32:24 srv-ftp-01 systemd[1]: Started vsftpd FTP server.
```

Código 18. Reinicio y comprobación del estado del servicio FTP

El último código es el rechazo del servidor por conexión insegura:

```
ftp> open 192.168.1.153
Connected to 192.168.1.153.
220 (vsFTPd 3.0.3)
Name (192.168.1.153:usuario): usuario1
530 Non-anonymous sessions must use encryption.
Login failed.
421 Service not available, remote server has closed connection
```

Código 19. El servidor rechaza conexiones inseguras

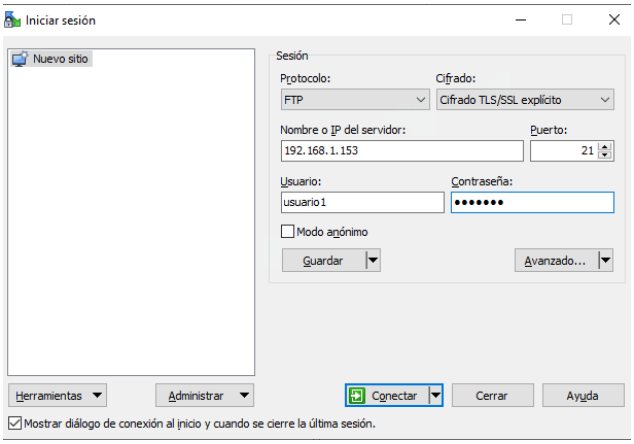

Fig. 5. Conexión utilizando SSL Explícito

/ 9. Caso práctico 2: "FTP SSL"

Planteamiento: Luis trabaja en el departamento de sistemas de una empresa que desarrolla aplicaciones web. Le han encargado configurar un servidor FTP para que los clientes puedan subir imágenes actualizadas para las nuevas campañas de publicidad.

Al tratarse de un servidor que estará expuesto a internet, Luis debe tratar de forma muy delicada la seguridad del servidor. Por consiguiente, un requisito fundamental es que las conexiones se establezcan de manera segura.

Nudo: ¿Qué procedimiento deberá seguir Luis para implementar el protocolo SSL?

Desenlace: Para facilitar el acceso a los clientes configurará un nombre DNS utilizando un subdominio de la empresa. Esto le permitirá utilizar el certificado comodín para poder cifrar las conexiones.

Lo primero que hará, será copiar los certificados a una carpeta en el servidor.,

A continuación, habrá que editar el fichero de configuración del demonio FTP añadiendo las siguientes líneas:

```
rsa_cert_file=/etc/ssl/private/certEmpresa.pem
rsa_private_key_file=/etc/ssl/private/certEmpresa.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Código 20. Configuración vsftpd.conf para activar SSL

Acto seguido, reiniciará el servicio para aplicar cambios y comprobará el correcto funcionamiento accediendo desde un cliente FTP que permita el uso de FTP SSL implícito.

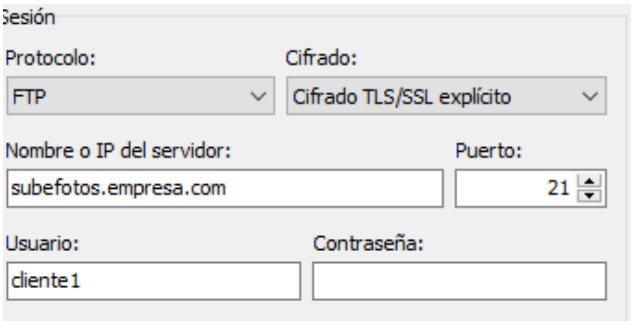

Fig. 6. Conexión segura con el servidor FTP

/ 10. Webdav

Webdav es un **protocolo de transferencia de archivos basado en los servicios web**. Este protocolo utiliza **los puertos TCP 80 y 443** para establecer las conexiones.

Para crear un servidor de transferencia *Webdav*, necesitaremos un servidor web que aloje el servicio, en este caso será **Apache**. Con el fin de evitar accesos indebidos utilizaremos autenticación ***digest*** para realizar el *login*.

Los pasos a seguir son los siguientes:

1. **Instalar Apache2**. Crear una carpeta compartida en el directorio público de Apache y asignar permisos.

```
:~$ sudo apt-get install apache2 apache2-utils
:~$ sudo mkdir /var/www/webdav
:~$ sudo chown -R www-data:www-data /var/www/
```

Código 21. Instalación de Apache y creación de directorio compartido.

2. **Activar módulos Webdav y digest.**

```
:~$ sudo a2enmod dav dav_fs auth_digest
```

Código 22. Activación de módulos de Apache.

3. **Creación del fichero de autenticación con los usuarios *webdav1* y *webdav2*.** Asignación de propiedad del fichero al usuario www-data.

```
:~$ sudo htdigest -c /etc/apache2/users.password webdav webdav1
Adding password for webdav1 in realm webdav.
sudo htdigest /etc/apache2/users.password webdav webdav2
sudo chown www-data:www-data /etc/apache2/users.password
```

Código 23. Creación de archivo con los usuarios digest.

4. **Editar un sitio de Apache para configurar el servicio.**

```
DavLockDB /var/www/DavLock
<VirtualHost *:80>
  DocumentRoot /var/www/html

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
  Alias /webdav /var/www/webdav
  <Directory /var/www/webdav>
    DAV On
    AuthType Digest
    AuthName “webdav”
    AuthUserFile /etc/apache2/users.password
    Require valid-user
  </Directory>
</VirtualHost>
```

Código 24. VirtualHost de Apache preparado para atender peticiones Webdav con autenticación digest activada.

Para aplicar los cambios será necesario reiniciar el servicio Apache.

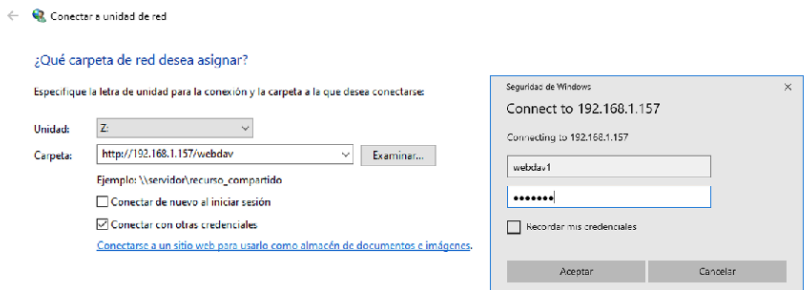

Fig. 7. Prueba de conexión Webdav en Windows.

Vídeo 2. "Configuración servidor Webdav".
https://bit.ly/2QmNWJJ

/ 11. Resumen y resolución del caso práctico de la unidad

En esta unidad hemos aprendido cómo instalar y configurar servidores de transferencia de archivos centrándonos en el protocolo FTP.

Hemos visto cómo configurar un servidor FTP, crear usuarios y configurar cuotas de disco. También hemos conocido el procedimiento para cifrar las conexiones FTP utilizando certificados SSL. De este modo, las contraseñas no se enviarán en texto plano.Finalmente, hemos aprendido cómo configurar un servidor de transferencia *Webdav* basado en Apache.

Resolución del caso práctico de la unidad

En el caso práctico inicial se plantea la siguiente situación: José y un compañero necesitan un sistema privado y seguro para intercambiar información entre ellos. Una posible solución podría ser configurar un servidor *Webdav* con autenticación *digest* y HTTPS para poder intercambiar archivos de forma segura. Dado que necesitan que el servidor esté disponible hasta que termine el proyecto, lo más practico es utilizar una Raspberry Pi para instalar el servidor y poder dejarlo siempre encendido.

/ 12. Bibliografía

Parziale, L., Liu, W., Matthews, C., Rosselot, N., Davis, C., Forrester, J., Britt, D. T., & Redbooks, I. B. M. (2006). TCP/IP *Tutorial and Technical Overview*. IBM Redbooks.

Miguel, R. M. (2020). *Administración de Servicios de Transferencia de Archivos y Contenidos Multimedia* (MF0497_3). RA-MA S.A. Editorial y Publicaciones.

/ 13. Webgrafía

http://manpages.ubuntu.com/manpages/bionic/es/man5/ftpusers.5.html

https://www.redeszone.net/tutoriales/servidores/vsftpd-configuracion-servidor-ftp/

http://www.pinchaiconos.com/n/56/configurar-el-modo-pasivo-con-vsftpd

https://www.geekpills.com/operating-system/linux/vsftpd-ftp-server-with-virtual-users

https://wiki.centos.org/HowTos/VirtualVsFtpd#:~:text=Create%20the%20MySQL%20Database%20for%20vsftpd%3A&text=enter%20%22%20yourrootsqlpassword%20%22%20%2D%20Be%20aware,mysql%3E%20GRANT%20SELECT%20ON%20vsftpd.

https://www.digitalocean.com/community/tutorials/how-to-configure-vsftpd-to-use-ssl-tls-on-a-centos-vps

https://www.digitalocean.com/community/tutorials/how-to-configure-webdav-access-with-apache-on-ubuntu-14-04

https://www.digitalocean.com/community/tutorials/how-to-set-filesystem-quotas-on-ubuntu-18-04