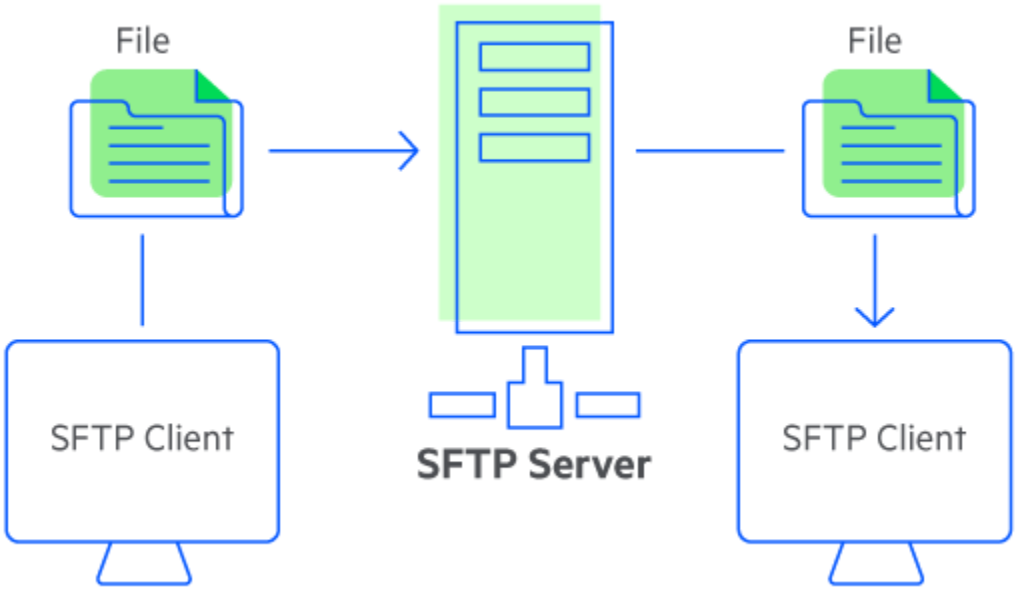
IES Zaidín Vergeles

SFTP, conexión FTP por SSH

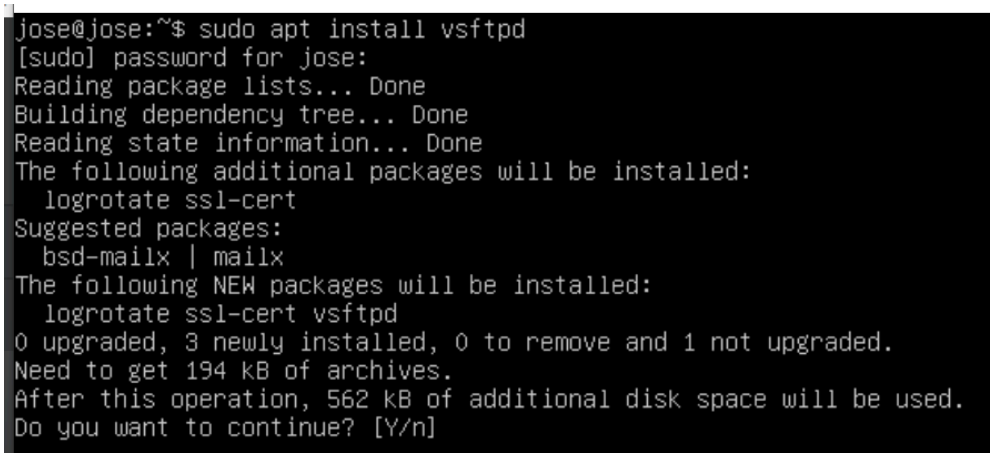


Jose Almirón López, 16 de Abril de 2024

Tabla de contenidos

Instalación SFTP

SFTP/SCP es una versión segura del protocolo FTP que utiliza SSH para establecer conexiones seguras. Esta solución es invaluable en entornos de servidores web, donde se requiere transferir archivos de manera segura. Para implementarlo, podemos instalar el servidor SFTP/SCP utilizando el comando '**apt install vsftpd**'.



Configuración de vsftpd

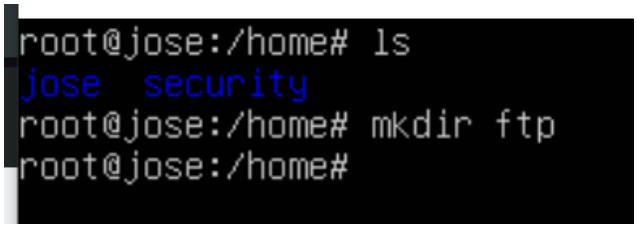
Para configurar vsftpd, trabajaremos con dos archivos principales. El primero se encuentra en la ruta **/etc/vsftpd.** En este fichero hemos modificado lo siguiente:

- **anonymous_enable=NO**: Desactiva la opción de permitir usuarios anónimos.
- **local_enable=YES**: Habilita la conexión con usuarios locales al servidor.
- **write_enable=YES**: Permite la escritura de datos mediante SFTP.
- **local_umask=022**: Establece los permisos predeterminados para archivos creados por usuarios locales.
- **ftpd_banner**: Permite personalizar un mensaje de bienvenida para el servidor.
- **chroot_list_file**: Define una lista de usuarios con acceso restringido al directorio raíz del servidor.

```
  GNU nano 6.2                                /etc/vsftpd.conf *
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
```

```
  GNU nano 6.2                                /etc/vsftpd.conf *
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Bienvenido a este servidor FTP.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
```

Después de completar la configuración básica, procedemos a crear un directorio en /home destinado a contener los usuarios FTP.

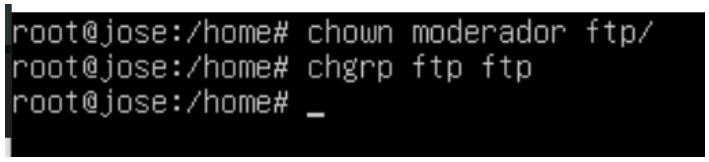


Crear las carpetas y los usuarios 'invitado' y 'moderador', así como el grupo 'ftp' si aún no existe.

```
root@jose:/home# mkdir /home/ftp/invitado
root@jose:/home# mkdir /home/ftp/moderador
root@jose:/home# groupadd ftp
groupadd: group 'ftp' already exists
root@jose:/home# useradd -g ftp -d /home/ftp/invitado/ -c "invitado" invitado
root@jose:/home# useradd -g ftp -d /home/ftp/moderador/ -c "moderador" moderador
root@jose:/home#
```

Establecemos contraseñas para los usuarios recién creados utilizando el comando '**passwd**'.

Concedemos permisos al usuario '**moderador**' y al grupo '**ftp**' para acceder a la carpeta '**ftp**'.



Establecemos los siguientes permisos para la carpeta '**invitado**'. Con el primer comando, otorgamos al grupo '**ftp**' la propiedad de la carpeta '**invitado**', y con el segundo comando, designamos al usuario '**moderador**' como el propietario de la carpeta '**invitado**'.

```
root@jose:/home/ftp# chgrp ftp invitado
root@jose:/home/ftp# chown moderador invitado
root@jose:/home/ftp#
```

Configuramos un shell para el FTP.

```
  GNU nano 6.2                                          /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/usr/bin/sh
/bin/dash
/usr/bin/dash
/bin/ftp
```

Editamos el archivo /etc/passwd con nano y modificamos la ruta de acceso de los usuarios creados para el SFTP, cambiando la ubicación de sus shells para que accedan sólo a la shell que hemos definido en el paso anterior.

```
  GNU nano 6.2                                    /etc/passwd *
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
jose:x:1000:1000:jose:/home/jose:/bin/bash
security:x:1001:1001:,,,:/home/security:/bin/bash
ftp:x:108:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
invitado:x:1002:113:invitado:/home/ftp/invitado/:/bin/ftp
moderador:x:1003:113:moderador:/home/ftp/moderador/:/bin/ftp
```

A continuación, vamos a configurar el siguiente archivo, donde incluimos la lista de usuarios para este servicio.

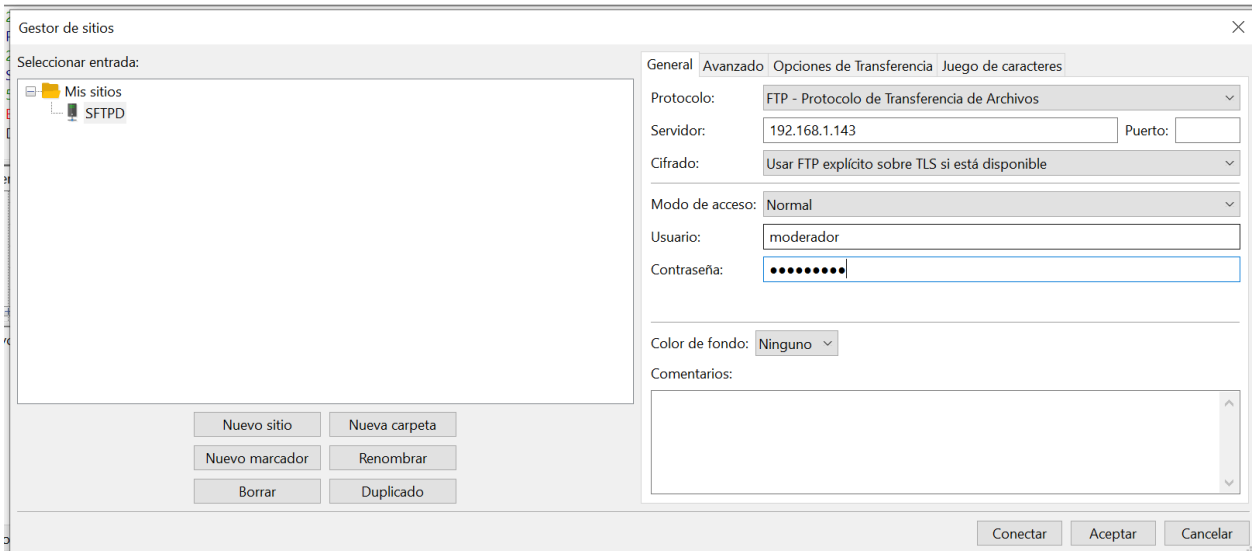
```
  GNU nano 6.2                                /etc/vsftpd.chroot.list
#Lista de usuarios FTP
invitado
moderador_
```

Una vez hayamos configurado todo, procedemos a reiniciar el servicio.

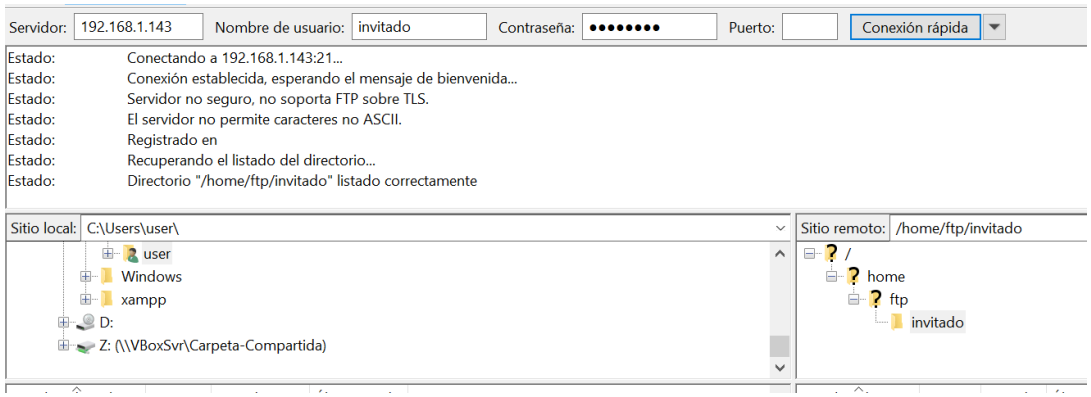
```
root@jose:/home/ftp# /etc/init.d/vsftpd restart
Restarting vsftpd (via systemctl): vsftpd.service.
root@jose:/home/ftp# _
```

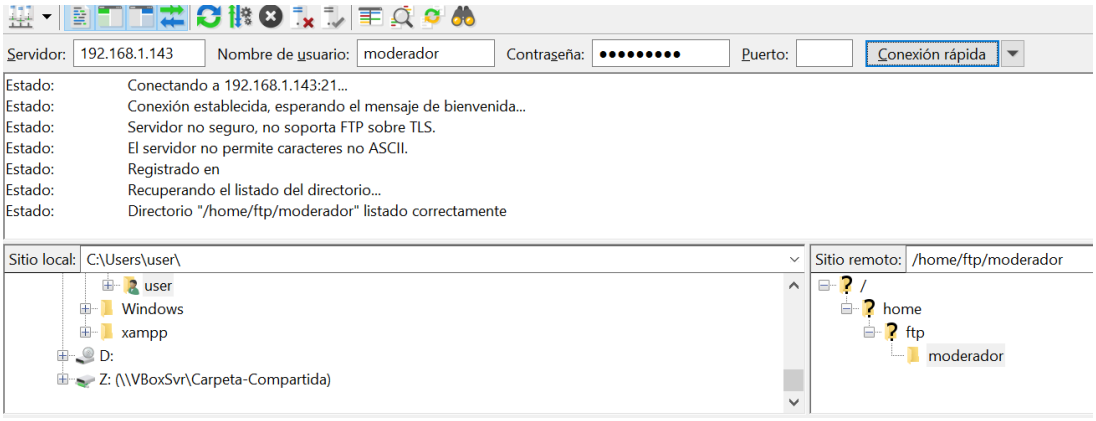
Comprobación del servicio

Para verificar el servicio, utilizaremos FileZilla, donde podemos configurar sesiones para conectarnos al servidor y verificar la funcionalidad del servicio.

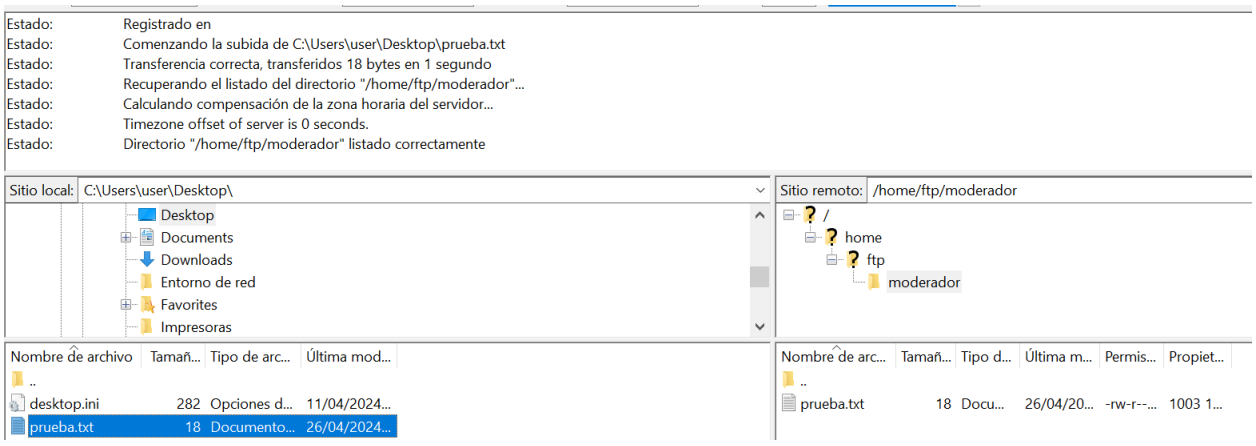


Puedes conectarte tanto con el usuario moderador como con el usuario invitado para comprobar que ambos pueden acceder correctamente al servidor.

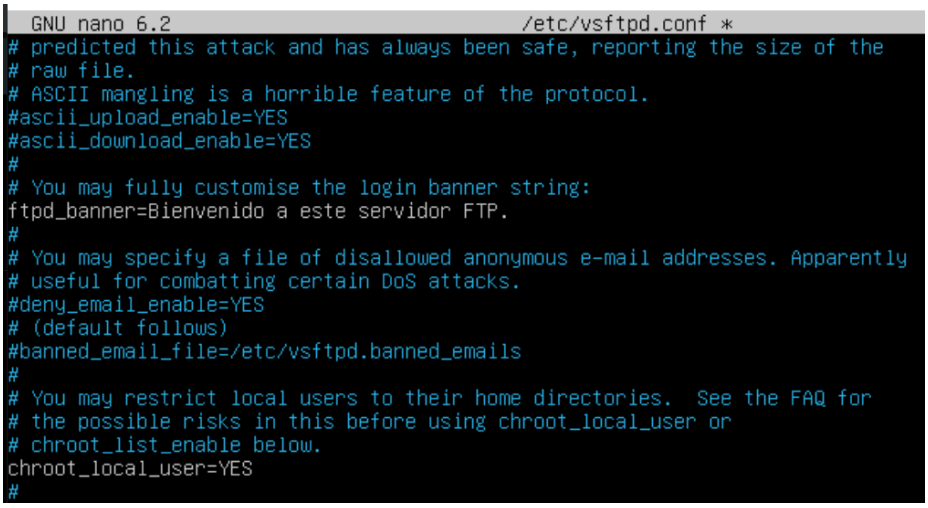




Podremos subir un fichero para comprobar que funcione correctamente.

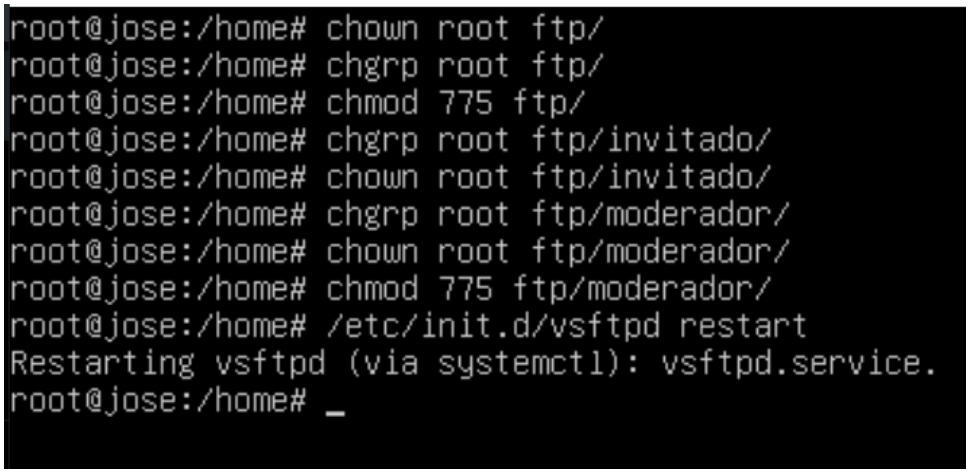


Para restringir el acceso de los usuarios solo a sus carpetas individuales en lugar de permitirles acceso a todo el directorio principal (/home), podemos descomentar la configuración 'chroot' en el archivo de configuración de SFTP. Aunque los usuarios no podrán escribir fuera de su carpeta, esta medida adicional evita que vean otras carpetas.



Creación de un certificado digital

Lo primero que haremos será dejar los permisos predeterminados.

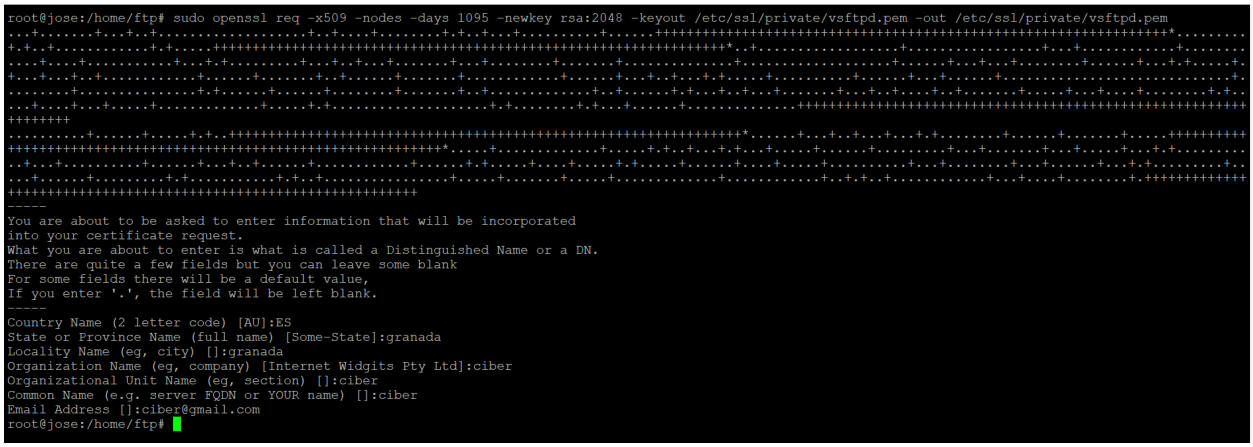


Verificamos si el servicio SSH está instalado, aunque en mi caso ya lo estaba por la práctica anterior.

```
jose@jose:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.7).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
jose@jose:~$
```

Ahora procedemos a crear el certificado digital utilizando el siguiente comando:

sudo openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

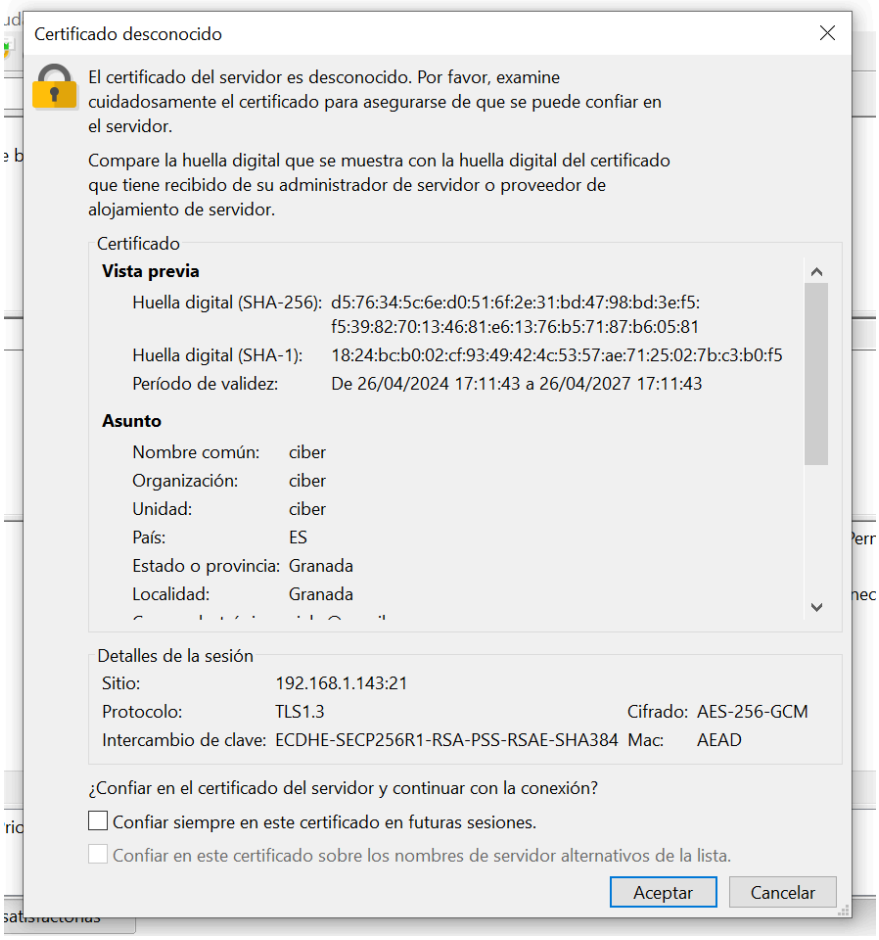


Regresamos a editar el archivo vsftpd.conf y al final agregamos la siguiente línea para habilitar el uso del certificado en nuestro FTP:

```
  GNU nano 6.2                                                  /etc/vsftpd.conf *
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES

#
```

Ahora, al acceder a través de Filezilla, nos aparecerá una solicitud para verificar el certificado.



Con esta configuración, ahora podemos establecer una conexión más segura mediante TLS.