**Manual de usuario**

Servidor DHCP

1er paso IP estatica

Configurar una dirección de ip estatica.

Entramos al archivo de configuración de las interfaces de red con el comando:

sudo nano /etc/network/interfaces

# Configuración de dirección IP fija para el interfaz ens192

auto ens192

iface eth0 inet static

address 192.168.1.10

netmask 255.255.255.0

network 192.168.1.0

broadcast 192.168.1.255

gateway 192.168.1.1

Después reiniciamos las interfaces de red del ordenador para aplicar los cambios , con el siguiente comando:

*sudo /etc/init.d/networking restart*

Configurar servidor DHCP

**Instalamos el servidor DHCP de la siguiente manera:**

*sudo apt install isc-dhcp-server*

**asignamos una direccion a la interfaz iv4 con el siguiente comando**

*sudo nano /etc/default/isc-dhcp-server*

**ejemplo: INTERFACES=”ens192”**

**Ahora, abra y edite el archivo de configuración para configurar su servidor DHCP.**

*sudo nano /etc/dhcp/dhcpd.conf*

**Comience definiendo los parámetros globales que son comunes a todas las redes admitidas**

**ejemplo:**

*default-lease-time 28600;*

*max-lease-time 7200;*

*authoritative;*

*subnet 192.168.1.0 netmask 255.255.255.0 {*

*range 192.168.1.100 192.168.1.200;*

*option routers 192.168.1.10;*

*option domain-name-servers 192.168.1.10;*

*option domain-name "grupo1.net";*

**Volvemos a reiniciar**

*sudo systemctl restart isc-dhcp-server*

**A continuación, permita las solicitudes al servidor DHCP en el Firewall, que escucha en el puerto 67/UDP.**

*sudo ufw allow 67/udp*

*sudo ufw reload*

**Y por último verificamos el estado/status para comprobar que esté funcionando**

*sudo systemctl status isc-dhcp-server*

Configurar servidor DNS local

**Instalamos el servidor DNS con el comando:**

*sudo apt install bind9 bind9-doc dnsutils*

**Luego declaramos las zonas que se encargaran de traducir los en sus direcciones IP y viceversa, Así, la configuración consiste, básicamente en la creación de 2 *zonas*, una (*zone “grupo1.net”*) que convierte nombres en direcciones *IP* y otra (*zone “1.168.192”*) que convierte direcciones *IP* en el respectivo nombre de sistema.**

*//*

*// Do any local configuration here*

*//*

*zone "grupo1.net" {*

*type master;*

*file "/etc/bind/db.grupo1.net";*

*};*

*zone "1.168.192.in-addr.arpa" {*

*type master;*

*file "/etc/bind/db.1.168.192";*

*};*

*// Consider adding the 1918 zones here, if they are not used in your*

*// organization*

*//include "/etc/bind/zones.rfc1918";*

**Verificar que el archivo de configuración no contiene errores:**

*named-checkconf*

**La resolución de nombres convierte los nombres de los sistemas en sus correspondientes direcciones IP. Para una zona “grupo1.net”, los nombres “server”, “virtual”, “ns” y “router” son asociados a sus respectivas direcciones. La base de datos para la resolución de nombres en la zona *home.lan* está guardada en el archivo** sudo nano */etc/bind/db.grupo1.net*:

*;*

*; BIND zone file for home.lan*

*;*

*$TTL 3D*

*@ IN SOA ns.grupo1.net. root.grupo1.net. (*

*2017061201 ; serial*

*8H ; refresh*

*2H ; retry*

*4W ; expire*

*1D ) ; minimum*

*;*

*NS ns ; Inet address of name server*

*MX 10 mail ; Primary mail exchanger*

*ns A 192.168.1.10*

*mail A 192.168.1.10*

*grupo1.net. A 192.168.1.10*

*server A 192.168.1.10*

*virtual A 192.168.1.10*

*router A 192.168.1.10 ; router ADSL*

*gateway CNAME router*

*www CNAME server*

*ftp CNAME server*

**Verificar que el fichero de configuración de la zona *grupo1.net* no contenga errores:**

*named-checkzone grupo1.net /etc/bind/db.grupo1.net*

**Ahora vamos a configurar la otra zona, la resolución inversa. La resolución inversa traduce las direcciones IP en los nombres correspondientes de los sistemas.**

**La resolución inversa puede configurarse en el archivo sudo nano** */etc/bind/db.1.168.192*

*;*

*; BIND zone file for 192.168.1.xxx*

*;*

*$TTL 3D*

*@ IN SOA ns.grupo1.net. root.grupo1.net. (*

*2017061201 ; serial*

*8H ; refresh*

*2H ; retry*

*4W ; expire*

*1D ) ; minimum*

*;*

*NS ns.grupo1.net. ; Nameserver address*

*10 PTR server.grupo1.net.*

*10 PTR ns.grupo1.net.*

*10 PTR mail.grupo1.net.*

*10 PTR virtual.grupo1.net.*

*10 PTR router.grupo1.net.*

**verificar que el archivo de configuración de la zona 10.1.168.192. no contenga errores:**

*named-checkzone 10.1.168.192. sudo/etc/bind/db.10.1.168.192*

**Reiniciamos el servicio:**

*systemctl restart bind9*

**Añadimos el dominio grupo1.net en el archivo /etc/resolv.conf:**

*# [...]*

*domain grupo1.net*

*search grupo1.net*

*nameserver 127.0.0.1*

*# [...]*

**Para verificar la resolución de nombres:**

*nslookup server*

*Server: 127.0.0.1*

*Address: 127.0.0.1#53*

*Name: server.home.lan*

*Address: 192.168.1.100*

**Verificar que los aliases también sean resueltos:**

*nslookup gateway*

*Server: 127.0.0.1*

*Address: 127.0.0.1#53*

*gateway.grupo1.net canonical name = router.grupo1.net*

*Name: router.grupo1.net*

*Address: 192.168.1.1*

**Para concluir con esta sección, verificar la resolución inversa:**

*nslookup 192.168.1.10*

*Server: 127.0.0.1*

*Address: 127.0.0.1#53*

*101.1.168.192.in-addr.arpa name = virtual.grupo1.net.*

Configurar Puente de Red

**A continuación vamos a hacer un puente de red para compatir internet entre las dos placas de red**

**Para crear el puente escribimos el siguiente codigo**

*ip link add name br0 type bridge*

*ip link set dev br0 up*

**Para agregar una interfaz (por ejemplo, eth0) al puente, su estado debe ser activo:**

*ip link set eth0 up*

***La adición de la interfaz al puente se realiza configurando su maestro en bridge\_name:***

*ip link set eth0 master bridge\_name*

***Para mostrar los puentes existentes y las interfaces asociadas, use el siguiente comando para ver más detalles.***

*bridge link*

Configurar servidor FTP

**Instalamos el VSFTPD**

*sudo apt-get install vsftpd*

**Ahora verás un mensaje de confirmación en el que tendrás que escribir Y y presionar Enter para continuar con la instalación.**

### Permitir el tráfico FTP desde el firewall

**Verificamos si el firewall esta activado de la siguiente manera**

*sudo ufw status*

*si ves el siguiente mensaje*

*ufw: command not found*

**Significa que el firewall no está instalado. Puedes instalarlo y habilitarlo escribiendo:**

*sudo apt-get install ufw*

*sudo ufw enable*

**Si ya está activo, todavía tienes que asegurarte de que el tráfico FTP está permitido. Para ello, ejecuta los siguientes comandos uno a uno:**

*sudo ufw allow 20/tcp*

*sudo ufw allow 21/tcp*

*sudo ufw allow 990/tcp*

*sudo ufw allow 40000:50000/tcp*

**Ahora veamos el estado de nuevo:**

*sudo ufw status*

**El resultado debería ser algo así:**

*Status: active*

*To Action From*

*-- ------ ----*

*990/tcp ALLOW Anywhere*

*20/tcp ALLOW Anywhere*

*21/tcp ALLOW Anywhere*

*40000:50000/tcp ALLOW Anywhere*

*20/tcp (v6) ALLOW Anywhere (v6)*

*21/tcp (v6) ALLOW Anywhere (v6)*

*990/tcp (v6) ALLOW Anywhere (v6)*

*40000:50000/tcp (v6) ALLOW Anywhere (v6)*

### 

### Crear el directorio de usuarios

**Una vez configurado el firewall, debemos crear el usuario que va a utilizar el acceso FTP. Para crearlo, usa el siguiente comando:**

*sudo adduser tu\_nombre*

**Usa el siguiente comando para crear la carpeta FTP:**

*sudo mkdir /home/tu\_nombre/ftp*

**Establece la propiedad usando:**

*sudo chown nobody:nogroup /home/tu\_nombre/ftp*

**Finalmente, elimina los permisos de escritura:**

*sudo chmod a-w /home/tu\_nombre/ftp*

**Ahora, usa el siguiente comando para verificar los permisos:**

*sudo ls -la /home/tu\_nombre/ftp*

**El resultado debería ser algo así:**

*total 8*

*dr-xr-xr-x 2 nobody nogroup 4096 Jun 29 11:32 .*

*drwxr-xr-x 3 tu\_nombre tu\_nombre 4096 Jun 29 11:32 ..*

**Como paso siguiente, crearemos el directorio contenedor de archivos y asignaremos la propiedad:**

*sudo mkdir /home/tu\_nombre/ftp/files*

*sudo chown tu\_nombre:tu\_nombre /home/tu\_nombre/ftp/files*

**Finalmente, agrega un archivo de prueba al directorio el cual se usará cuando probemos todo más adelante:**

*echo "vsftpd sample file" | sudo tee /home/tu\_nombre/ftp/files/sample.txt*

### 

### 

### Configurar vsftpd

**En primer lugar, verifica que el archivo de configuración tenga una configuración que coincida con las mencionadas a continuación** [**utilizando el comando nano**](https://www.hostinger.com.ar/tutoriales/instalar-nano-text-editor)**:**

*sudo nano /etc/vsftpd.conf*

**Comprueba que el contenido tiene una configuración similar a ésta:**

*. . .*

*# Allow anonymous FTP? (Disabled by default).*

*anonymous\_enable=NO*

*#*

*# Uncomment this to allow local users to log in.*

*local\_enable=YES*

*. . .*

**En el mismo archivo, procederemos a eliminar # y a habilitar el write\_enable:**

*. . .*

*write\_enable=YES*

*. . ..*

**Chroot tampoco se comentará para asegurarte de que el usuario FTP sólo accede a los archivos dentro del directorio permitido. Cambia también el valor NO por SÍ. Ten en cuenta que hay dos líneas como ésta, y tienes que descomentar ambas.**

*. . .*

*chroot\_local\_user=YES*

*. . .*

**Hay algunos valores nuevos que también debes añadir al final del archivo. En primer lugar, se agregará un user\_sub\_token en la ruta del directorio local\_root. Esto permitirá que la configuración funcione con el usuario actual y con cualquier otro usuario que se agregue posteriormente:**

*user\_sub\_token=$USER*

*local\_root=/home/$USER/ftp*

**Para garantizar que haya una cantidad considerable de conexiones disponibles, limitaremos la cantidad de puertos utilizados en el archivo de configuración:**

*pasv\_min\_port=40000*

*pasv\_max\_port=50000*

**En esta seccion ,planeamos permitir el acceso caso por caso, así que ajustemos la configuración de forma tal que el acceso solo se otorgue a los usuarios que se hayan agregado explícitamente a una lista:**

*userlist\_enable=YES*

*userlist\_file=/etc/vsftpd.userlist*

*userlist\_deny=NO*

**El flag userlist\_deny es el responsable de alternar la lógica; cuando se establece en NO, solo se permitirá el acceso a los usuarios especificados en la lista. Una vez hecho esto, haz clic en CTRL+X y confirma los cambios del archivo.**

**Por último, procederemos con la creación y adición de nuestro usuario al archivo:**

*echo "tu\_nombre" | sudo tee -a /etc/vsftpd.userlist*

**Verifica que el usuario esté realmente activo ejecutando el siguiente comando:**

*cat /etc/vsftpd.userlist*

**El resultado debe ser «tu\_nombre» como se muestra en esta captura de pantalla:**

**Reinicia el daemon utilizando el siguiente comando para cargar los cambios de configuración:**

sudo systemctl restart vsftpd

### **Hacer que el FTP sea seguro**

**Por defecto, FTP no hace ninguna encriptación de datos, por eso utilizaremos TTL/SSL para garantizar la seguridad. En primer lugar, debemos crear el certificado SSL y usarlo para proteger el servidor FTP de Ubuntu. Para comenzar, usa el siguiente comando:**

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

**El flag -days hace que el certificado sea válido por un año y hemos incluido una clave privada RSA de 2048 bits en el mismo comando.**

**Una vez sean solicitados, ingresa los datos personales correspondientes en el campo provisto.**

**Cuando termines de crear el certificado, abre nuevamente el archivo de configuración:**

*sudo nano /etc/vsftpd.conf*

**El final del archivo debe contener dos líneas que comiencen con «\_rsa«. Comenta ambas líneas así:**

*# rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem*

*# rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key*

**En lugar de eso, apuntemos el archivo de configuración al certificado que acabamos de crear. Añade los siguientes direcciones justo debajo de las líneas anteriores:**

*rsa\_cert\_file=/etc/ssl/private/vsftpd.pem*

*rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem*

***Ahora habilitaremos SSL y nos aseguraremos de que solo los clientes que tengan SSL habilitados nos puedan contactar. Cambia el valor de ssl\_enable a YES:***

*ssl\_enable=YES*

***A continuación agrega las siguientes líneas para prohibir cualquier conexión anónima a través de SSK***

*allow\_anon\_ssl=NO*

*force\_local\_data\_ssl=YES*

*force\_local\_logins\_ssl=YES*

***Configura el servidor para usar TLS usando:***

*ssl\_tlsv1=YES*

*ssl\_sslv2=NO*

*ssl\_sslv3=NO*

***Ahora cambiaremos 2 opciones más. En primer lugar, no será necesario reutilizar SSL porque puede ocasionar que muchos clientes de FTP se averíen. En segundo lugar, utilizaremos suites de encriptación de alto cifrado, lo que significa que las longitudes de claves son iguales o superiores a 128 bits.***

***require\_ssl\_reuse=NO***

***ssl\_ciphers=HIGH***

***Vuelve a guardar el archivo pulsando CTRL+X seguido de Y, y luego pulsa Intro.***

***Vamos a reiniciar vsftpd una vez más para aplicar las nuevas configuraciones:***

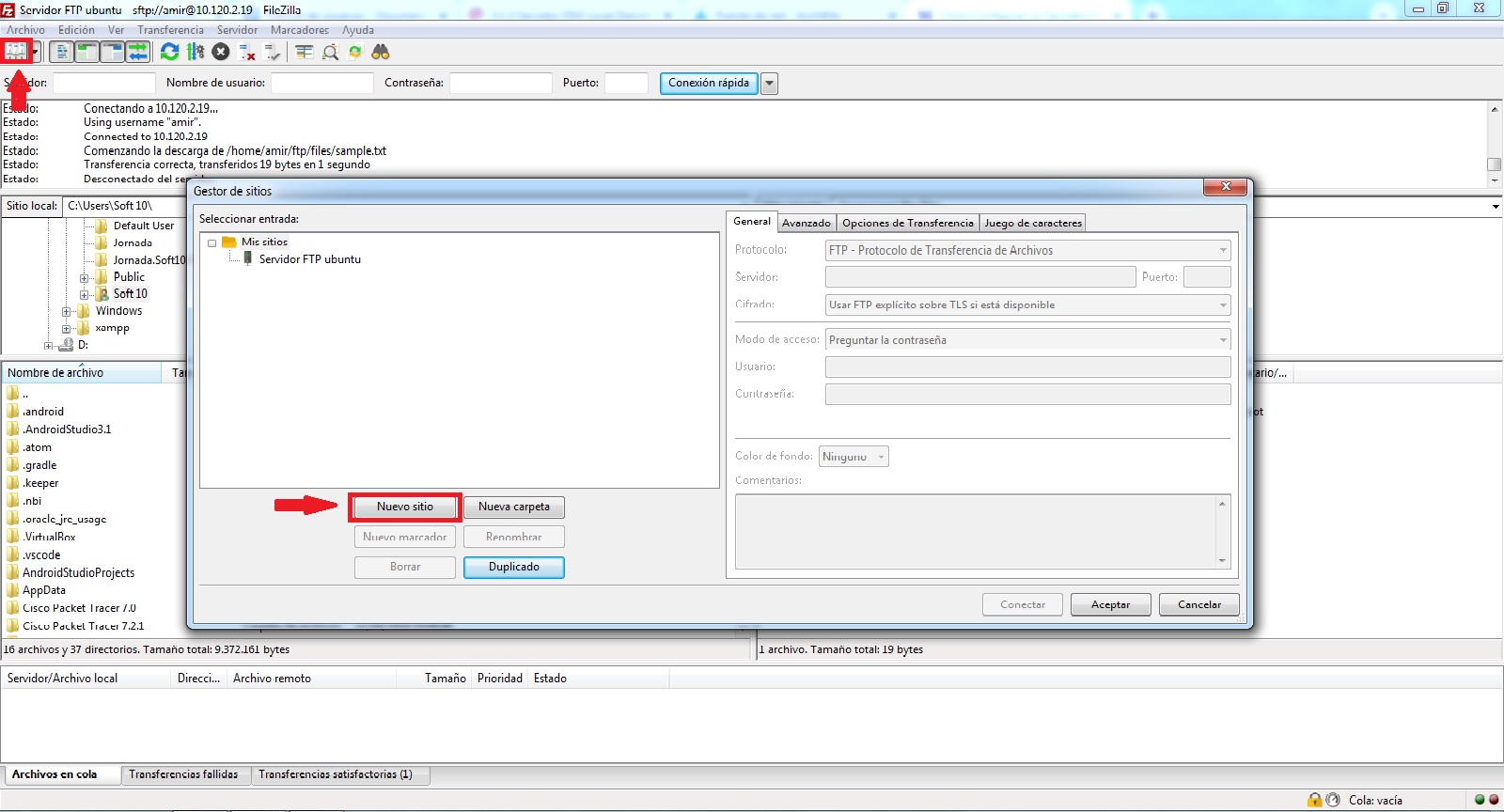
*sudo systemctl restart vsftpd*

***Y así , has configurado el servidor FTP en tu VPS de Ubuntu para que funcione con el protocolo SSL/TLS.***

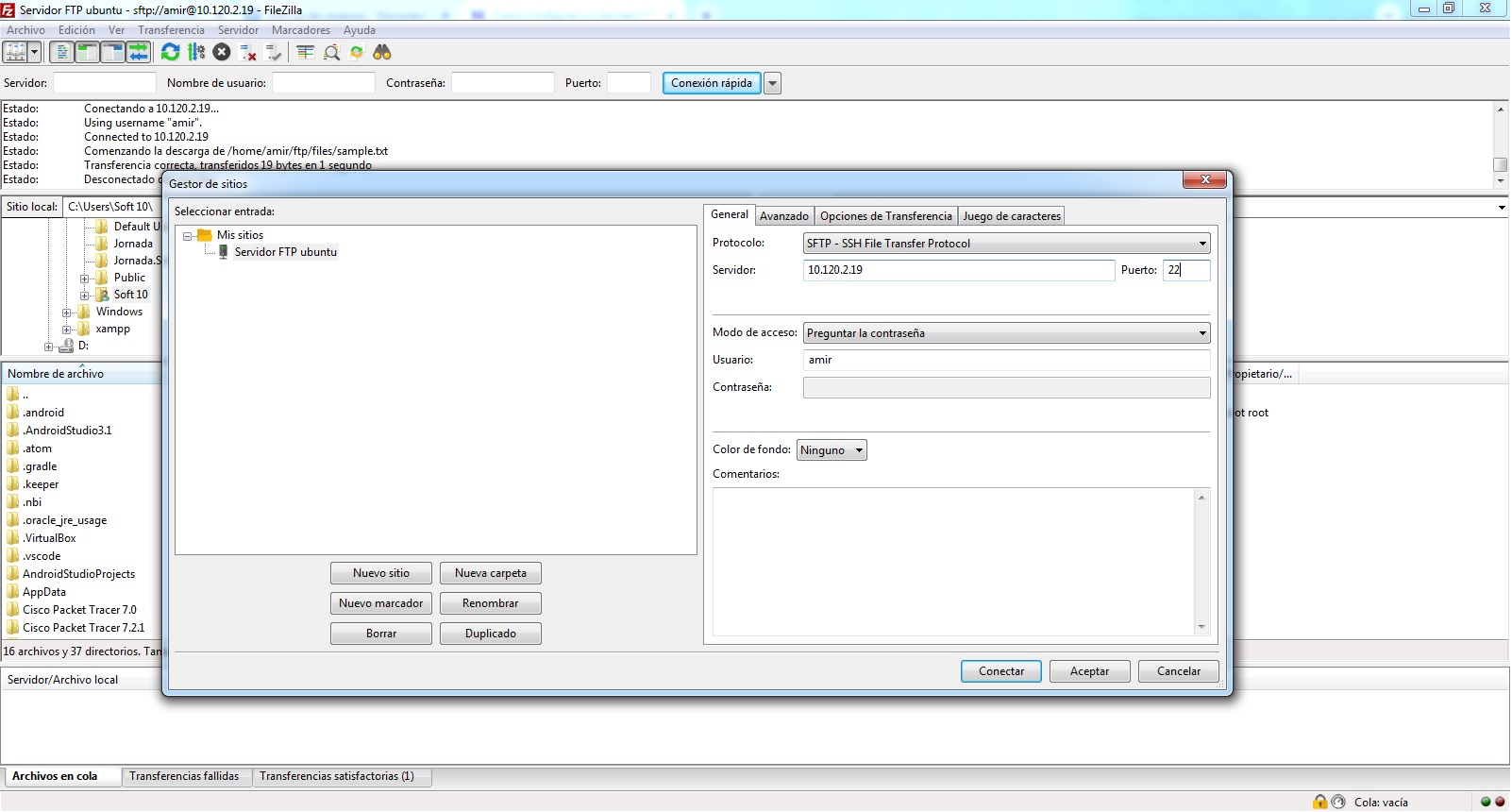
## ***Prueba de conexiones con FileZilla***

**La mayoría de clientes FTP permiten configuraciones de cifrado TSL,Para probar la conexión, utilizaremos un** [**cliente FTP de FileZill**](https://www.hostinger.com.ar/tutorials/ftp/filezilla-ftp-configuration)**a.**

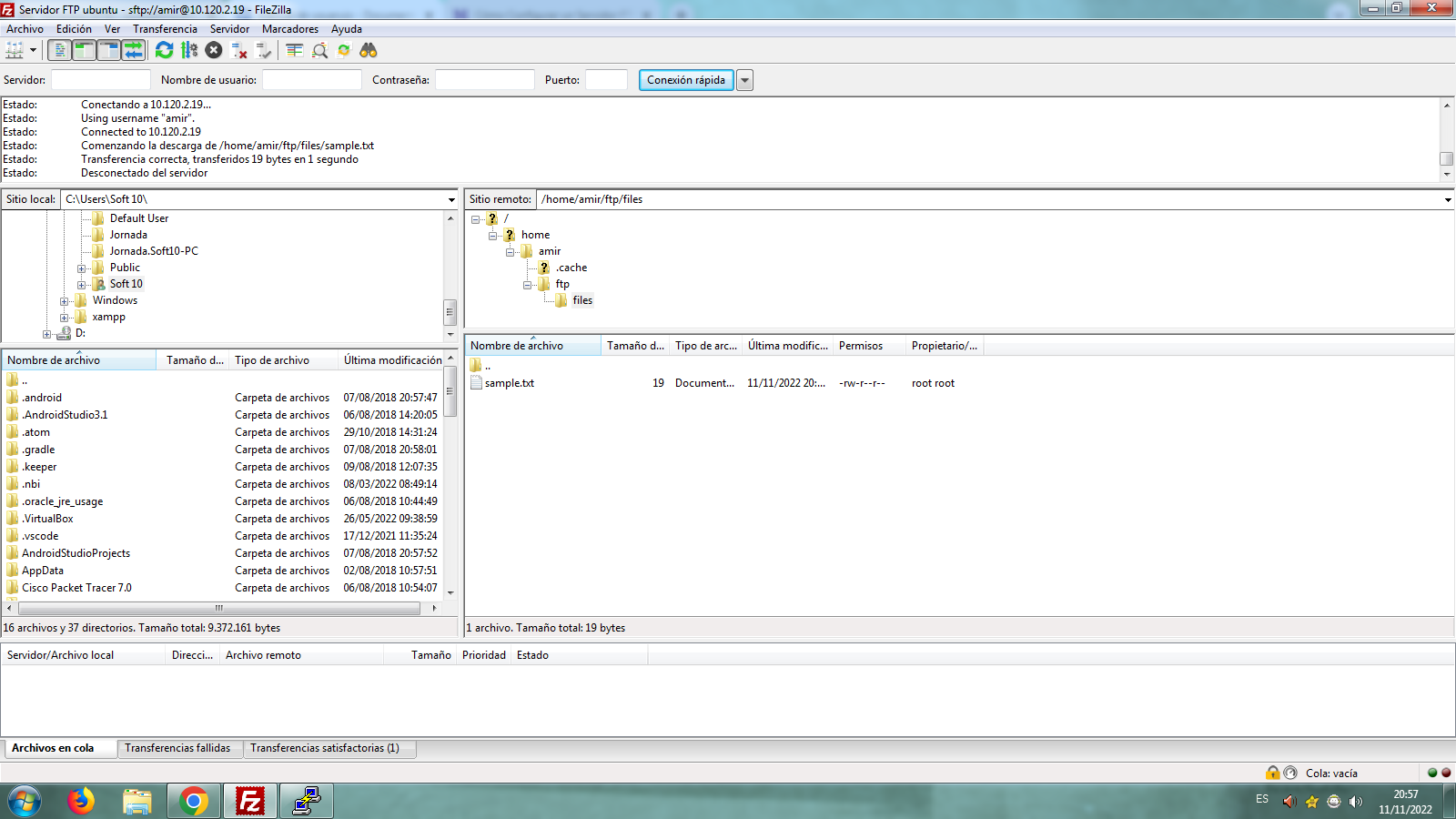
***Para comenzar inicia FileZilla y haz clic en el icono de Gestor de Sitios. Luego haz clic en el botón Sitio Nuevo en la ventana que aparece para comenzar a ingresar los detalles del servidor FTP de Ubuntu.***

**

**Completa todos los detalles requeridos con tu información del servidor FTP de Ubuntu recién creada. Como lo configuramos para usar TLS, también podemos marcar el cifrado para que sea explícitamente FTP sobre TLS. La configuración final debería verse así:**

**

**Cuando esté listo, haz clic en Conectar y aparecerá una pantalla que te pedirá ingresar la contraseña del usuario de FTP.**

**