

Tutoriales varios

- [Instala un entorno de escritorio en tu VPS Ubuntu](#)
- [Inicia tu VPS + Cpanel](#)
- [Instala un servidor de FTP en Ubuntu con VSFTPD](#)

Instala un entorno de escritorio en tu VPS

Ubuntu

Esto es algo que consultan a menudo nuestros clientes. ¿Cómo puedo acceder a una interfaz gráfica en las VPS que utilizan imágenes Linux? Esto porque quieren usar el navegador o acceder vía interfaz gráfica a otros elementos. Y la respuesta es bastante sencilla y no toma más de 15 minutos.

En este tutorial utilizaremos una imagen Ubuntu y el entorno KDE Plasma. Para partir, actualiza los repositorios y listas de paquete de tu Ubuntu:

```
sudo apt-get update && sudo apt-get upgrade
```

Cuando en medio de este proceso se te pregunte si deseas continuar, teclea "Y" (que significa "sí, continúa").

Antes de proseguir, instalaremos un administrador de pantalla ligero como SLiM o LightDM. Los administrador de pantalla proporcionan inicios de sesión gráficos y manejan la autenticación del usuario.

Para instalar SLiM, solo debes teclear:

```
sudo apt-get install slim
```

Una vez terminado el proceso, instalaremos KDE Plasma. Teclea:

```
sudo apt-get install kde-plasma-desktop
```

En el proceso se te solicitará indicar el administrador de pantalla que utilizarás. Por ejemplo: SLiM.

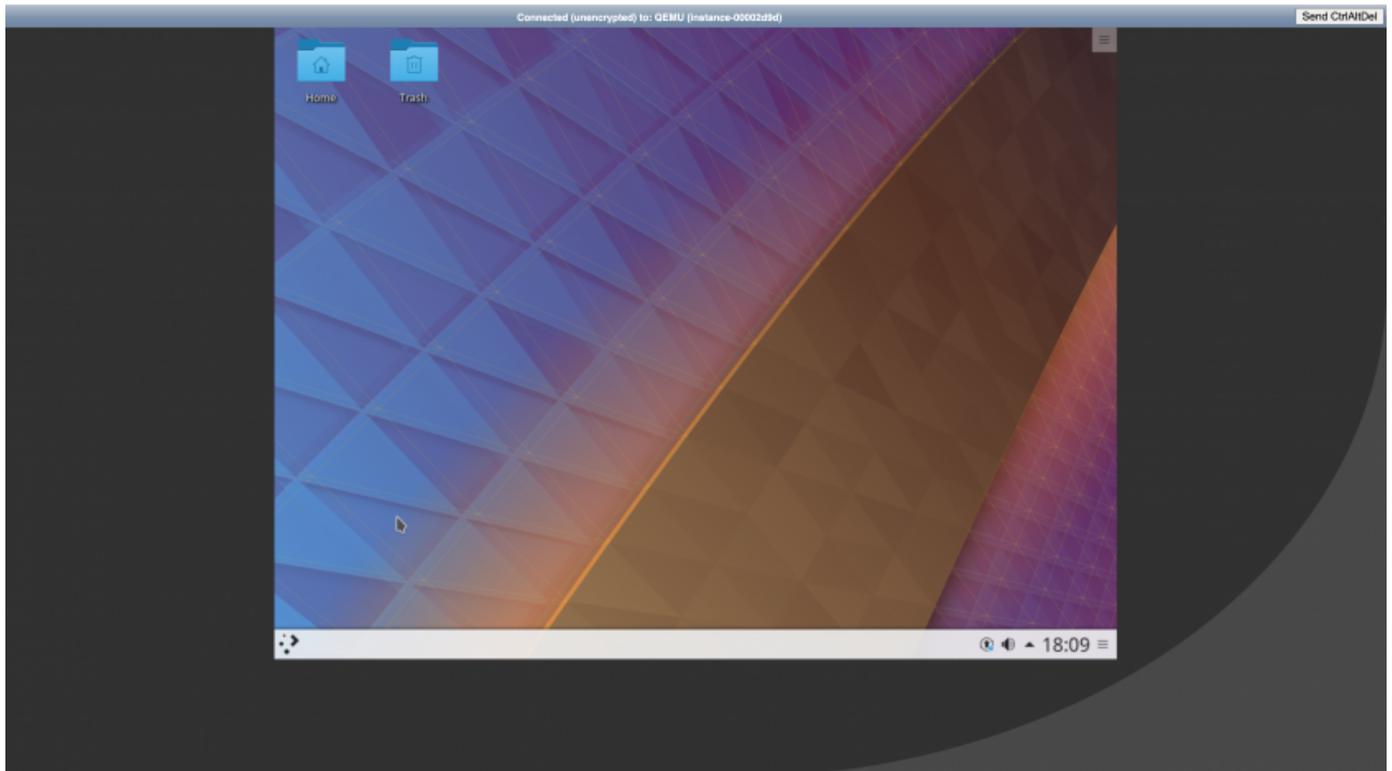
Al terminar, lanzas KDE Plasma tipeando:

```
sudo service slim start
```

Si te das cuenta, al iniciar el servicio agregué "slim", que es el administrador de pantalla que elegí para este ejemplo. Tú puedes utilizar otro.

Y eso es todo. Ahora accede a la consola web de tu VPS y se abrirá el entorno gráfico. Para acceder a la consola web, ingresa al panel de control de VPS Guru. En tu listado de servidores, pincha el nombre de tu VPS. Se abrirá la página de detalles. Allí en el extremo superior derecho verás el botón "Consola". Pínchalo y se abrirá la consola web.

¡Ah! Y si vas a usar el navegador de la VPS, no olvides de abrir en el firewall (ubicado en la página de detalles de tu VPS) los puertos TCP 80 (HTTP) y 443 (HTTPS).



Acceder a escritorio remoto con NoMachine

Si la consola web es muy limitada para tus necesidades, siempre puedes usar algo como [NoMachine](#). Este software es un escritorio remoto.

Debes descargarlo en tu equipo y en la misma VPS. Para este ejemplo, la versión que corresponde descargar en la VPS es "NoMachine para Linux DEB amd64". Lo puedes descargar vía SSH o por consola web, a través del navegador que ya tienes en tu VPS.

Una vez descargado, lo puedes instalar por SSH o haciéndole doble click al paquete en la consola web.

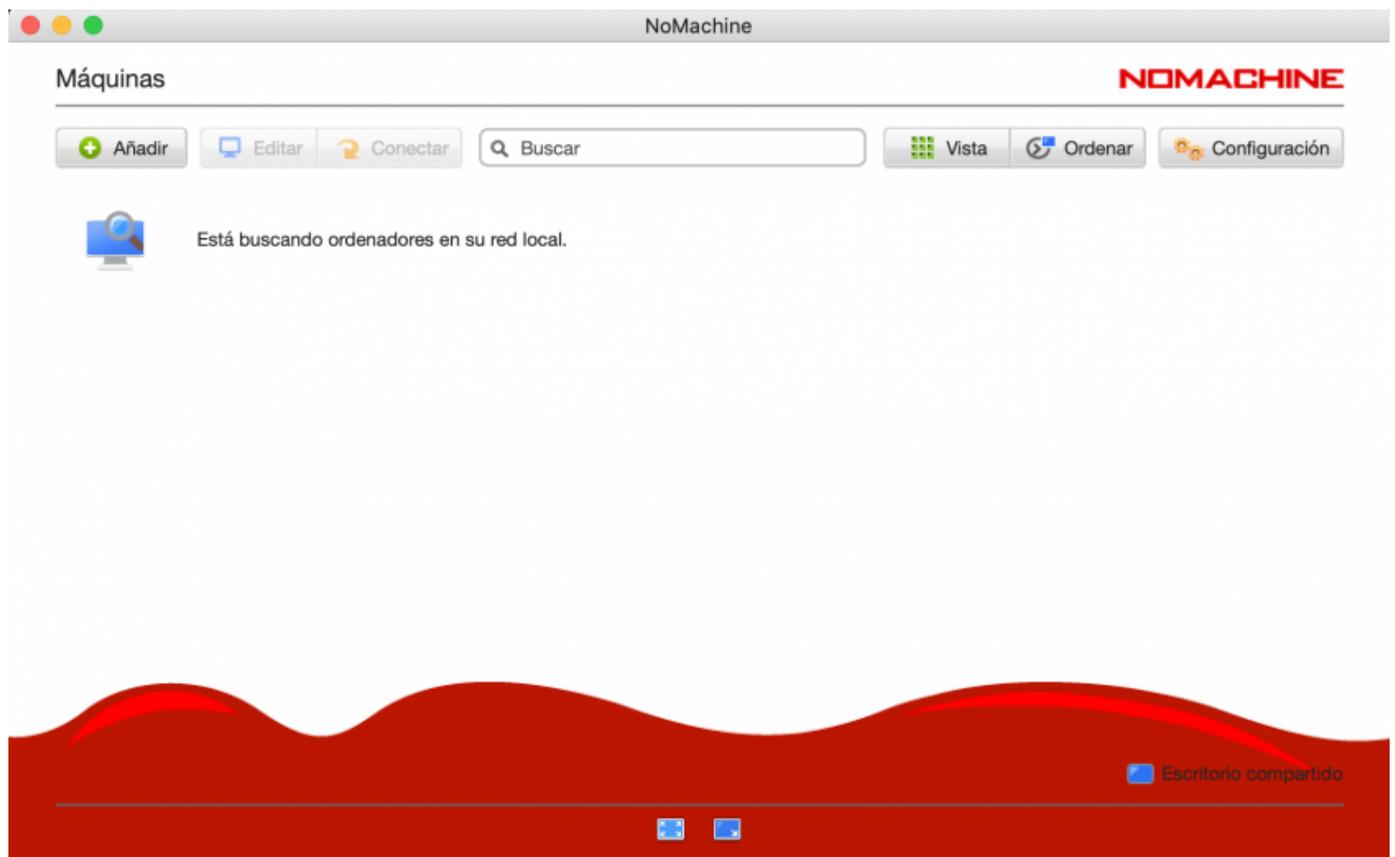
Para instalarlo por SSH, solo debes ubicar la carpeta en que descargaste el archivo y teclear:

```
sudo dpkg -i nomachine_5.1.54_1_amd64.deb
```

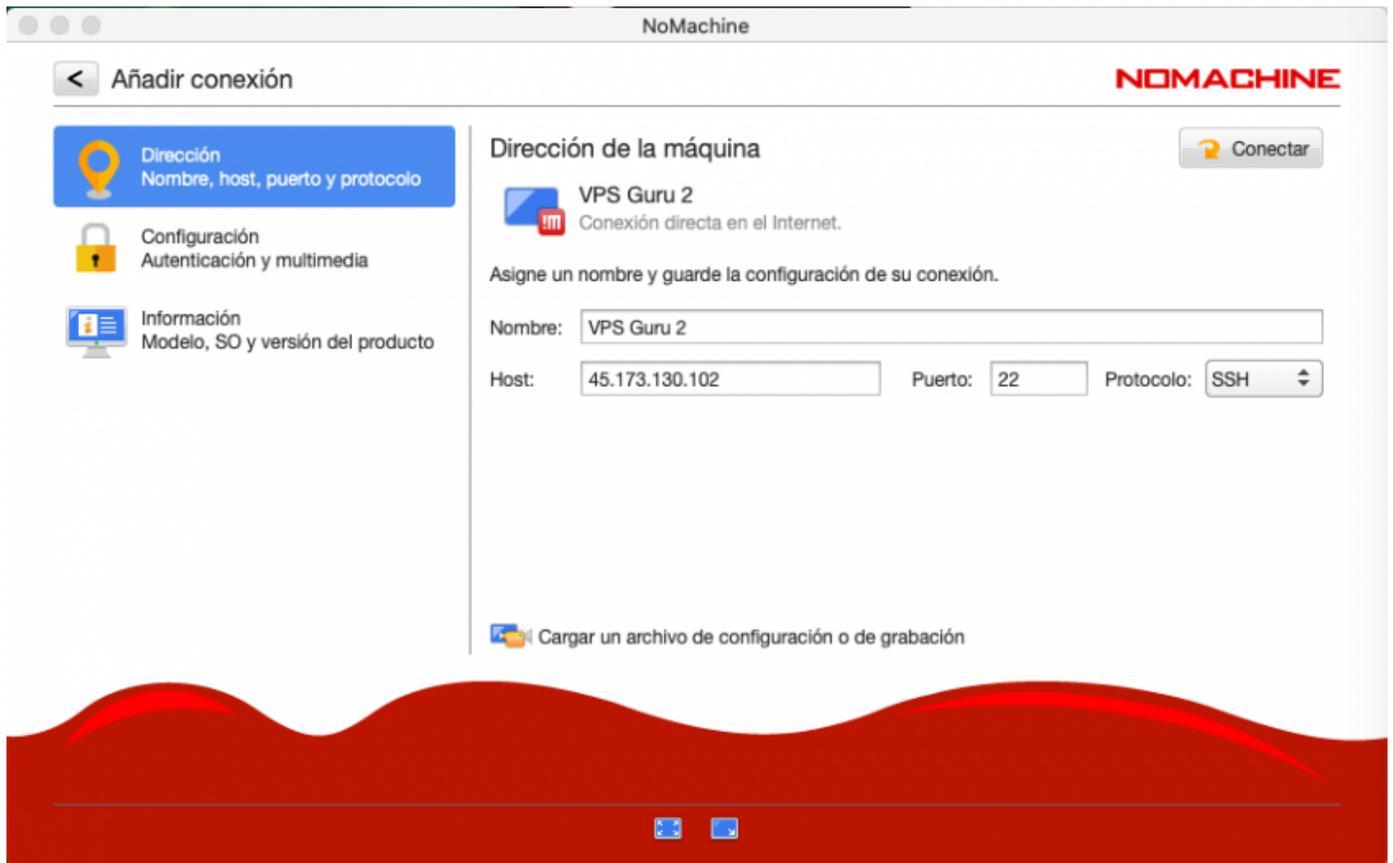
Una vez instalado, debes abrir el puerto 4000 TCP en el firewall de tu VPS (ubicado en el panel de control de VPS Guru).

Para asegurarte que todo funcione bien cuando quieras conectarte por primera vez, entra vía consola web a tu VPS y abre el software recién instalado. Revisa que esté corriendo.

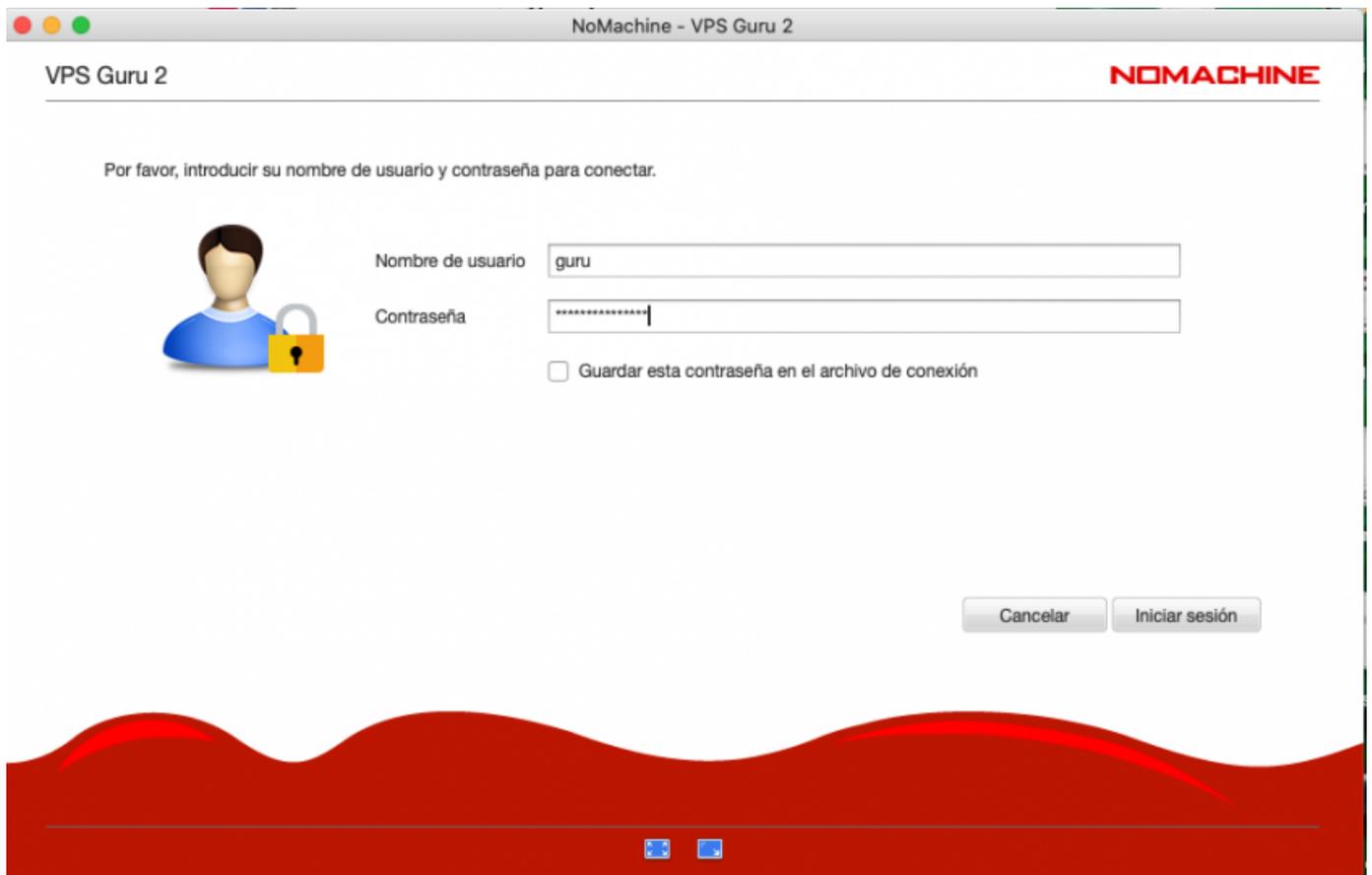
Ya está todo preparado. Ahora abre NoMachine en tu equipo.



Pincha "Añadir".



Agrega los datos de tu VPS. Recuerda seleccionar SSH.



Luego te pedirá los datos de usuario y contraseña de tu VPS.

Iniciará a conectarse. Puede que la primera vez presente problemas para conectarse e intente por NX. Pero una vez que logre la conexión será sencillo en las siguientes ocasiones.

Inicia tu VPS + Cpanel

Este tutorial está destinado a aquellos usuarios que compraron una VPS CentOS con Cpanel preinstalado, que desean administrar de manera sencilla su sitio o aplicaciones a través de este panel de control.

Puedes ubicar esta imagen dentro de nuestro listado de imágenes disponibles al momento de crear una VPS. Esta opción te ahorra la descarga e instalación, y te permite saltar directamente a la configuración.

Abriendo puertos

Una vez que se encuentre activo tu servidor con Cpanel, debes abrir los puertos TCP necesarios en el firewall ubicado en la zona “Detalle de tu Instancia” de tu VPS (para acceder a esta página accede al listado de tus VPS y pincha el nombre de la VPS que deseas configurar):

- WHM: 2087 (TCP)
- CPanel: 2083 (TCP)
- CPanel Webmail: 2095-2096 (TCP)
- FTP: 21 (TCP)
- SFTP: 22 (TCP)
- SMTP: 25 (TCP)
- SMTP SSL: 465 (TCP)
- POP: 110 (TCP)
- POP SSL: 995 (TCP)

- HTTP SSL: 443 (TCP)
- DNS: 53 y 953 (TCP y UDP)

Y no olvides de abrir el puerto TCP 80, necesario para que puedas acceder desde Internet a tu sitio web.

Define una contraseña para WHM

WHM es la plataforma que te permite crear y administrar las cuentas de Cpanel. Por lo tanto, tu primer paso será ingresar a WHM.

Para definir la contraseña de WHM debes ingresar por SSH a tu VPS y teclear lo siguiente:

```
sudo su -passwd root
```

Escribe una contraseña. A partir de ahora tu usuario de WHM será “root” y la contraseña aquella que acabas de crear. Posteriormente puedes cambiar esa contraseña desde tu panel de WHM.

Ingresa a WHM

Para ingresar a WHM accede desde:

- <https://TUIP:2087>

Donde TUIP, debe ser tu IPV4.

Dado que aún no tienes instalado un certificado SSL, es probable que te aparezca una advertencia indicando que “La conexión no es privada”. En ese caso, debes pinchar en “Configuración avanzada” y luego en el link “Continuar a...”.

Una vez que accedas a la página de inicio, se te pedirá que ingreses tus credenciales.

- Usuario: root

Contraseña: En el paso anterior se mencionó cómo crear la contraseña.

En la siguiente pantalla se te presentarán los términos y condiciones, que deberás aceptar. A continuación debes ingresar el email a los cuales Cpanel notificará los mensajes de errores y status, y tus DNS.

Compra y activa tu licencia

Luego de realizar los pasos previos, podrás ver en la parte superior de tu panel de control de WHM una notificación titulada “Trial License” que informa que tienes activada una cuenta trial, de 15 días. Dentro de esa notificación hay un botón para acceder al sitio de compra (“Purchase a license”). Si pinchas el botón, serás dirigido a una página de compra.

Si no aparece este mensaje, alternativamente puedes dirigirte a <https://store.cpanel.net/cart/> para poder realizar la compra.

Una vez que realices la compra verifica la licencia en <https://verify.cpanel.net/app/verify>

Si está todo correcto, accede a tu VPS por SSH y tipea:

```
/usr/local/cpanel/cpkeyclt
```

Inmediatamente la licencia será actualizada en tu servidor.

Soporte y documentación

VPS Guru no entrega soporte a Cpanel. Te recomendamos que accedas a la documentación que entrega Cpanel en <https://docs.cpanel.net/> o a su zona de soporte <https://cpanel.net/support/>

Instala un servidor de FTP en Ubuntu con VSFTPD

Este tutorial te dará un paso a paso para instalar y configurar un servidor de FTP en tu servidor virtual y habilitar una conexión segura con FTPS. Si bien esta guía está dirigida a usuarios de Linux Ubuntu, es perfectamente aplicable a otras distros de Linux.

Abramos puertos

Partamos configurando el firewall. En el firewall que te provee VPS Guru debes abrir los puertos:

- 20 y 21 TCP
- 40000-50000 TCP
- 990 TCP

Instalemos y configuremos

Ahora actualiza Ubuntu e instala VSFTPD

```
sudo apt update && sudo apt install vsftpd
```

Revisa si ya está corriendo:

```
sudo service vsftpd status
```

Ya instalado y corriendo, hay que crear un usuario. Por ejemplo, "tuusuario":

```
sudo adduser tuusuario
```

Ahora debes definir el directorio en el cual podrá ese usuario subir y modificar archivos vía FTP. Lo normal es que la carpeta a la que tenga acceso el usuario FTP sea la de documentos del servidor HTTP (Apache o Nginx) o una subcarpeta creada dentro de ese directorio. Por lo que debes determinar dónde está esa carpeta. En Ubuntu normalmente es `/var/www`.

Por lo que si fuéramos a dejar como carpeta del usuario `/var/www` debiéramos tipear:

```
sudo usermod -d /var/www tuusuario
```

A continuación al usuario le damos propiedad sobre el directorio:

```
sudo chown tuusuario:tuusuario /var/www/html
```

No ahondaremos en los permisos, ya que extendería mucho más este artículo, pero si llegas a tener problemas de permisos, deberás interiorizarte en cómo funcionan los permisos y en cómo aplicar manejos avanzados de los mismos.

A continuación, es hora de configurar vsftpd. Antes de eso vamos a copiar el archivo y dejar un backup:

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

Ya realizado el backup, vamos a abrir el archivo con tu editor favorito, Nano o Vim. Nano suele ser el más sencillo de ocupar y puedes encontrar una [guía aquí](#). Para abrir el archivo de configuración de vsftpd vamos a tipear:

```
sudo nano /etc/vsftpd.conf
```

Dentro del archivo vamos a buscar `#write_enable=YES` y vamos a eliminar el `#`. De esta forma, el usuario podrá subir archivos, modificarlos, etc. La línea debiera quedar así:

```
write_enable=YES
```

Ahora vamos a buscar la línea `#chroot_local_user=YES` y vamos a eliminar el `#`. Esto previene que el usuario FTP pueda navegar fuera de su directorio. La línea debiera quedar así:

```
chroot_local_user=YES
```

Busca la línea `#local_umask=022` y vamos a eliminar el `#`. De esta forma establecemos permisos de escritura, lectura y ejecución al contenido. Los permisos 022 son de sólo escritura para el grupo y los demás. Pero puedes modificar estos permisos cambiando el valor 022 por el que creas más adecuado. La línea debiera quedar así:

```
local_umask=022
```

A continuación agregaremos líneas que no existen en el archivo, y que dejaremos al final del mismo:

```
force_dot_files=YES
pasv_min_port=40000
pasv_max_port=50000allow_writeable_chroot=YES
```

`force_dot_files` nos permitirá ver los archivos que se inician con un punto, como `.htaccess`. `pasv_min_port` y `pasv_max_port` nos permiten definir un rango para los puertos de FTP pasivo (¿recuerdas la configuración inicial del firewall?).

Salva los cambios y reinicia `vsftpd`:

```
sudo systemctl restart vsftpd
```

Ahora toca probar si todo está funcionando bien, para lo cual te aconsejamos utilizar [Filezilla](#). Lo más sencillo es usar el modo de conexión rápida. Allí tipeas el hostname (la IP), el nombre del usuario creado y la contraseña, y luego presionas "Conexión rápida".

Si hay falla revisa lo que indica Filezilla y también puedes revisar lo que registró `vsftpd` en su log

```
sudo tail /var/log/vsftpd.log -n 200
```

FTPS: para darle seguridad a nuestra conexión

Lo recomendable es siempre tratar de usar FTPS ya que encripta nuestras comunicaciones con el servidor. Es decir, usar FTP con SSL/TLS.

Para lograrlo partamos por crear un nuevo certificado con la herramienta `openssl`:

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

Te pedirá que ingreses tu país, provincia y otros datos. No es necesario que los ingreses, por lo que puedes presionar "Enter" en cada uno de ellos.

Volvamos a abrir el archivo de configuración de vsftpd:

```
sudo nano /etc/vsftpd.conf
```

Encuentra la línea `ssl_enable=NO`, que debe quedar así:

```
ssl_enable=YES
```

Pega lo siguiente debajo de esa línea:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pemrsa_private_key_file=/etc/ssl/private/vsftpd.pem
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
pasv_min_port=40000pasv_max_port=50000
```

Salva los cambios y reinicia vsftpd:

```
sudo systemctl restart vsftpd
```

Abre nuevamente Filezilla e intenta conectarte. Te debiera aparecer este mensaje:

server administrator or server hosting provider.

Certificate

Vista previa

Huella digital (SHA-256): 01:81:e8:f4:20:44:da:47:4a:43:c2:26:87:59:86:d1:
17:ea:e0:74:c1:d3:4f:33:14:87:13:2f:e3:5b:b6:07

Huella digital (SHA-1): 7c:9d:bd:ea:45:a2:ee:ff:4a:33:80:d0:31:34:98:fa:bb:37:22:ad

Validity period: From 09/09/22 12:11:33 to 09/09/23 13:11:33

Subject

Organización: Internet Widgits Pty Ltd

País: AU

Estado o provincia: Some-State

Issuer

Same as subject, certificate is self-signed

Detalles

Serial: 09:54:35:e4:18:78:06:e3:7a:a3:65:b1:8b:1f:42:9b:f1:22:10:fb

Algoritmo de clave pública: RSA con 2048 bits

Algoritmo de firma: RSA-SHA256

Detalles de la sesión

Sitio: 45.173.130.187:21

Protocolo: TLS1.3

Cifrado: AES-256-GCM

Intercambio de clave: ECDHE-SECP256R1-RSA-PSS-RSAE-SHA384 Mac: AEAD

Trust the server certificate and carry on connecting?

Always trust this certificate in future sessions.

Confiar en este certificado sobre los nombres de servidor alternativos de la lista.

Cancelar

Aceptar

Luego de eso debiera ver los siguientes mensajes en el "registro de mensajes" de Filezilla:

Estado: Conexión establecida, esperando el mensaje de bienvenida...
Estado: Inicializando TLS...
Estado: Verificando certificado...
Estado: Conexión TLS establecida.

