

# Protocolo SSH

Administración de Servicios en Red

4CM1





# Acceso Remoto

El acceso remoto es la habilidad de acceder a un equipo o una red de manera remota a través de una conexión de red; este permite a los usuarios acceder a los sistemas que necesitan cuando no son capaces de hacerlo de manera física, es decir, les permite acceder a sistemas en otros equipos usando una red como medio de conexión.

El acceso remoto es una combinación de software, hardware y conexión de red, hoy en día el acceso remoto se hace mediante una conexión segura como VPN haciendo conexión entre hosts mediante una conexión cableada, Wi-Fi o de internet.



# Protocolo SSH

SecureShell o SSH es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de internet, fue creado como reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

SSH proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente.



# Características de SSH

En comparación con protocolos de acceso remoto antiguos, la **característica principal** del protocolo SSH es que **encripta toda la información que envía y recibe**, evitando así la obtención de contraseñas no encriptadas y **protegiendo** el sistema cliente y el remoto.

- El cliente puede **verificar** que se está **conectando al servidor** al que se conectó inicialmente.
- Todos los **datos enviados y recibidos** durante la conexión así como la **información de autenticación** del cliente se transfieren por medio de **encriptación de 128 bits** (difícil de descifrar y leer)
- El servidor SSH puede convertirse en un **conducto** para convertir en **seguros los protocolos inseguros** mediante el uso de una técnica llamada **reenvío por puerto**, como por ejemplo POP, incrementando la **seguridad** del sistema en general y de los datos.
- Muchas **aplicaciones SSH cliente** están disponibles para casi todos los **principales sistemas operativos** en uso hoy día.

# Cómo funciona SSH



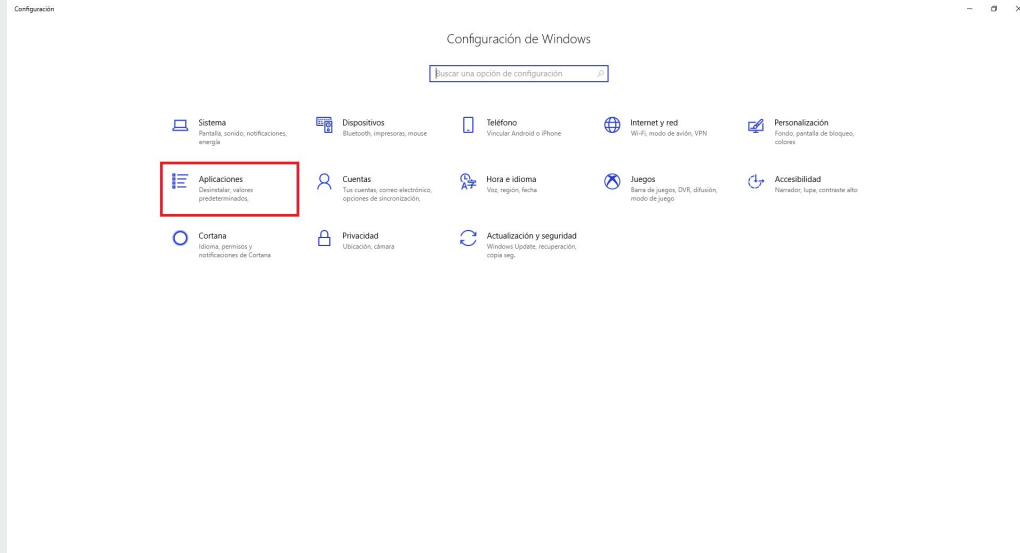
# Instalación de SSH

---



# Windows

# Servidor

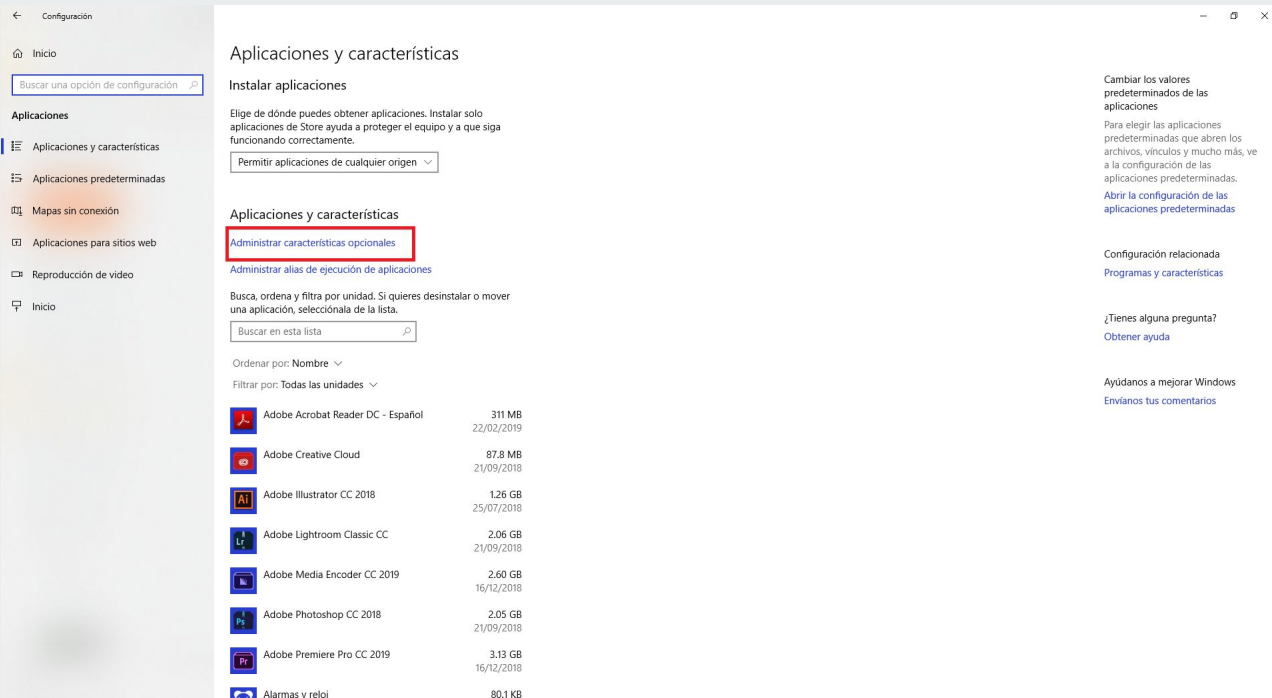


## Configuración de Windows

-> Aplicaciones



# Click en Administrar características especiales



The screenshot shows the Windows Settings application, specifically the 'Aplicaciones y características' (Apps & Features) section. The left sidebar contains navigation options: 'Inicio' (Home), 'Buscar una opción de configuración' (Search for a configuration option), 'Aplicaciones' (Apps), 'Aplicaciones predeterminadas' (Default apps), 'Mapas sin conexión' (Offline maps), 'Aplicaciones para sitios web' (Web app settings), 'Reproducción de video' (Video playback), and 'Inicio' (Home). The main content area is titled 'Aplicaciones y características' and includes a sub-section 'Instalar aplicaciones' (Install apps) with instructions on where to get apps and a dropdown menu set to 'Permitir aplicaciones de cualquier origen' (Allow apps from anywhere). Below this, the 'Aplicaciones y características' section is highlighted with a red box, containing the link 'Administrar características opcionales' (Optional features) and 'Administrar alias de ejecución de aplicaciones' (App execution aliases). A search bar 'Buscar en esta lista' (Search in this list) is present. Below the search bar, there are sorting and filtering options: 'Ordenar por: Nombre' (Sort by: Name) and 'Filtrar por: Todas las unidades' (Filter by: All units). A list of installed applications is shown, including Adobe Acrobat Reader DC - Español, Adobe Creative Cloud, Adobe Illustrator CC 2018, Adobe Lightroom Classic CC, Adobe Media Encoder CC 2019, Adobe Photoshop CC 2018, Adobe Premiere Pro CC 2019, and Alarmas y reloj (Alarms & Clock). On the right side of the window, there are links for 'Cambiar los valores predeterminados de las aplicaciones' (Change default app values), 'Configuración relacionada' (Related settings), '¿Tienes alguna pregunta? Obtener ayuda' (Have a question? Get help), and 'Ayúdanos a mejorar Windows' (Help us improve Windows).

← Configuración

Inicio

Buscar una opción de configuración

Aplicaciones

Aplicaciones y características

Aplicaciones predeterminadas

Mapas sin conexión

Aplicaciones para sitios web

Reproducción de video

Inicio

## Aplicaciones y características

### Instalar aplicaciones

Elige de dónde puedes obtener aplicaciones. Instalar solo aplicaciones de Store ayuda a proteger el equipo y a que siga funcionando correctamente.

Permitir aplicaciones de cualquier origen

### Aplicaciones y características

**Administrar características opcionales**









[Administrar alias de ejecución de aplicaciones](#)

Busca, ordena y filtra por unidad. Si quieres desinstalar o mover una aplicación, selecciónala de la lista.

Buscar en esta lista

Ordenar por: Nombre

Filtrar por: Todas las unidades

	Adobe Acrobat Reader DC - Español	311 MB 22/02/2019
	Adobe Creative Cloud	87.8 MB 21/09/2018
	Adobe Illustrator CC 2018	1.26 GB 25/07/2018
	Adobe Lightroom Classic CC	2.06 GB 21/09/2018
	Adobe Media Encoder CC 2019	2.60 GB 16/12/2018
	Adobe Photoshop CC 2018	2.05 GB 21/09/2018
	Adobe Premiere Pro CC 2019	3.13 GB 16/12/2018
	Alarmas y reloj	80.1 KB

Cambiar los valores predeterminados de las aplicaciones

Para elegir las aplicaciones predeterminadas que abren los archivos, vínculos y mucho más, ve a la configuración de las aplicaciones predeterminadas.

[Abrir la configuración de las aplicaciones predeterminadas](#)

Configuración relacionada

[Programas y características](#)

¿Tienes alguna pregunta?

[Obtener ayuda](#)

Ayúdanos a mejorar Windows

[Envíanos tus comentarios](#)

# Revisar la disponibilidad de Cliente OpenSSH y Servidor de OpenSSH

← Configuración

Administrar características opcionales

Características opcionales

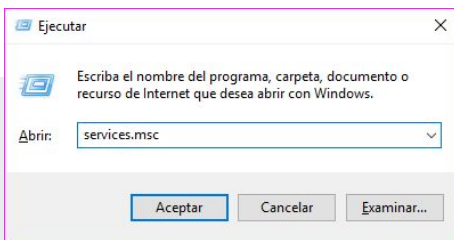
[Ver historial de características opcionales](#)

[¿Tienes alguna pregunta?](#)  
[Obtener ayuda](#)

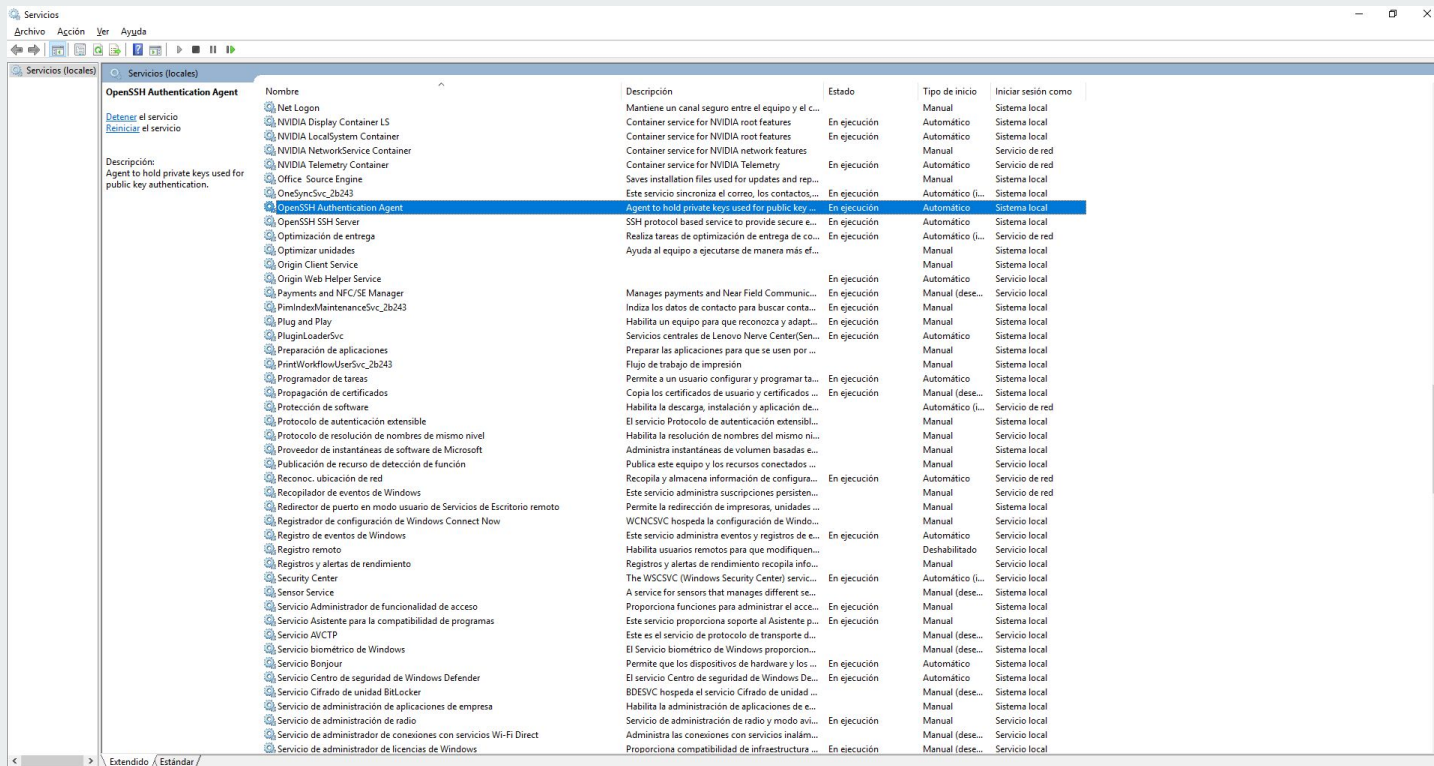
+ Agregar una característica

	Asistencia rápida de Microsoft	1.52 MB
	Cliente de OpenSSH	5.70 MB
	Escritura manual para español (México)	9.22 MB
	Escritura para español (México)	46.3 MB
	Herramientas de gráficos	65.6 MB
	Internet Explorer 11	1.74 MB
	Reconocimiento de voz en español (México)	5.76 MB
	Reconocimiento óptico de caracteres en español (México)	240 KB
	Reproductor de Windows Media	61.1 MB
	Servidor de OpenSSH	5.31 MB
	Texto a voz para español (México)	33.3 MB

Si no, hacer click en “Agregar una característica”



## Iniciar Servicios de servidor y de agente, similar a SNMP



```
Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Service -Name *ssh*

Status Name          DisplayName
-----
Running ssh-agent    OpenSSH Authentication Agent
Running sshd         OpenSSH SSH Server

PS C:\Windows\system32>
```

Revisar alta del servicio SSH

```
Administrador: Windows PowerShell
PS C:\Windows\system32> netsh advfirewall firewall add rule name="SSHD Port" dir=in action=allow protocol=TCP localport=22
Aceptar
PS C:\Windows\system32>
```

Agregar regla de conexión al Firewall

```
Administrador: Windows PowerShell

Conexiones activas

Proto Dirección local Dirección remota Estado PID
---
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 8496
[sshd.exe]
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 472
RpcSs
[svchost.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
No se puede obtener información de propiedad
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 11596
CDPSvc
[svchost.exe]
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 720
No se puede obtener información de propiedad
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 1572
EventLog
[svchost.exe]
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1444
Schedule
[svchost.exe]
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 2320
-- Más --
```

Comprobar que la regla aplicada funcione

Nota: puede haber una vulnerabilidad al dejar el puerto 22 abierto\*\*  
Solución: crear un usuario windows con permisos restringidos



Tutorial:

<https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/>

## Crear un nuevo usuario y permitir que entre por medio de ssh

Iniciar sesión como superusuario:

```
ssh root@server_ip_address
```

Crea un nuevo usuario con el comando `adduser`, ingresar dos veces la contraseña para el nuevo usuario:

```
adduser username
```

Abrir el archivo `/etc/ssh/sshd_config`, ahí se puede cambiar el puerto, como en este ejemplo 1234 y añadir a nuevos usuarios el permiso de acceder por medio de ssh:

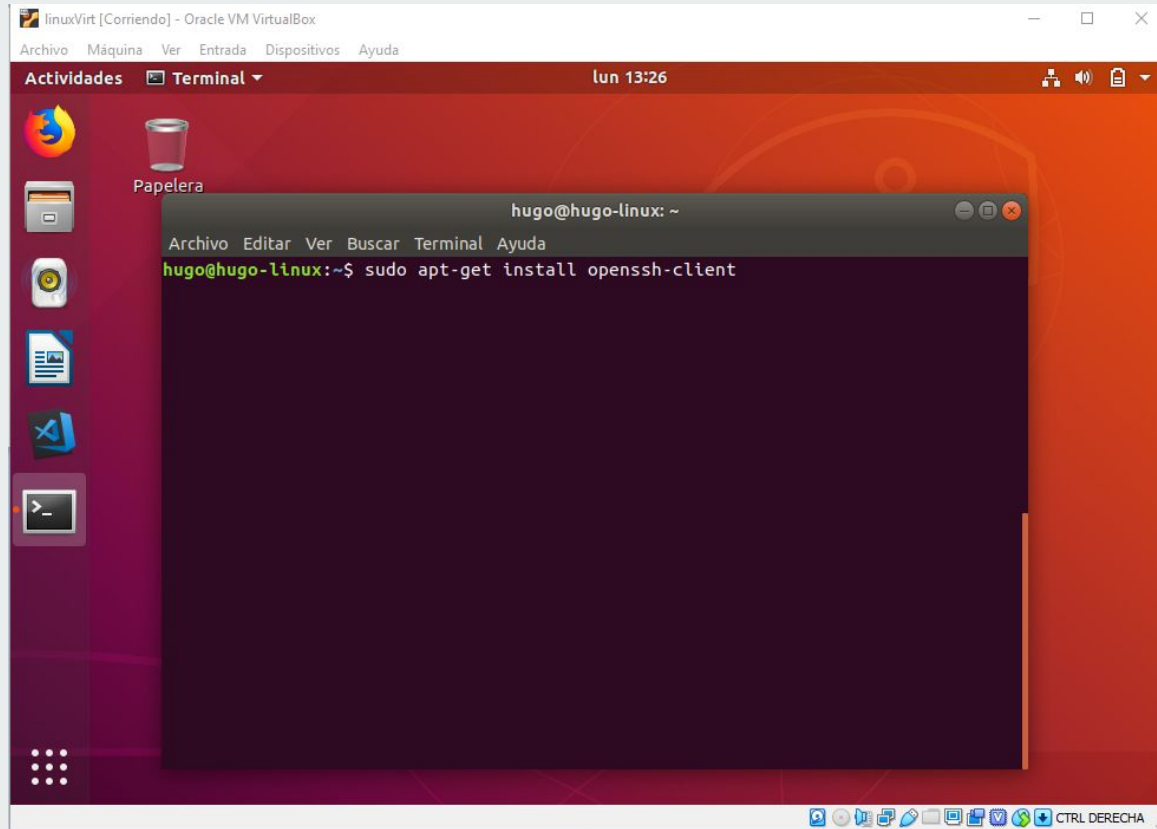
```
Port 1234
```

```
AllowUsers username
```

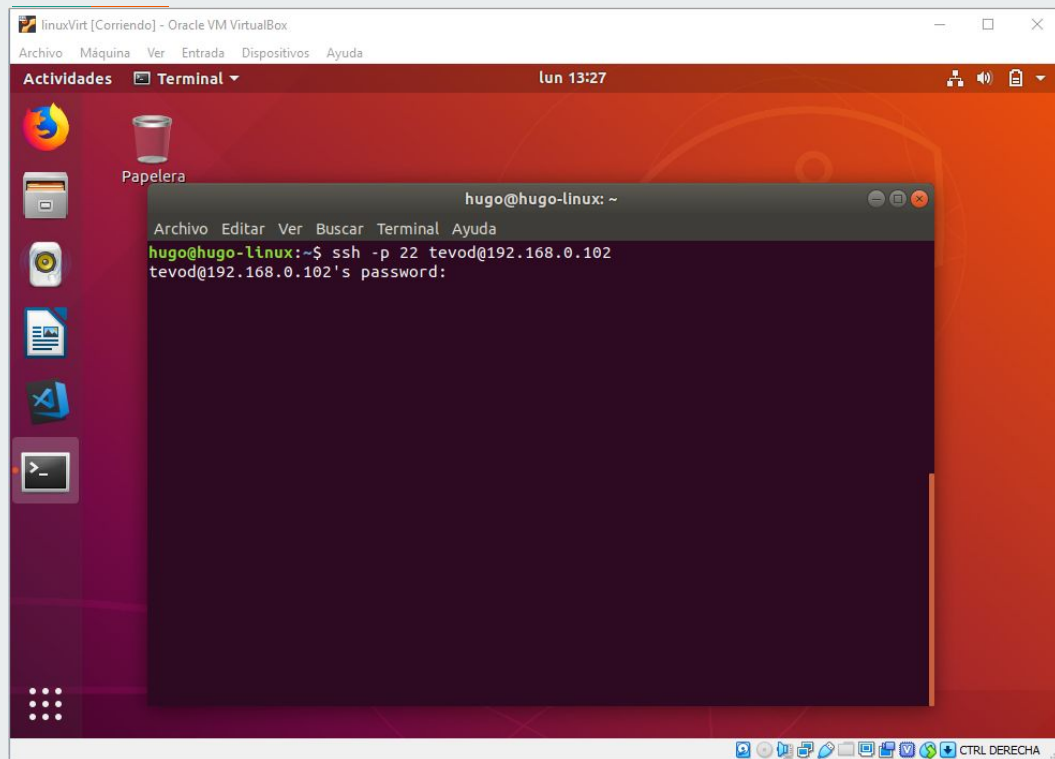
Reiniciar servicio ssh:

```
sudo service ssh reload
```

# Cliente SSH Linux

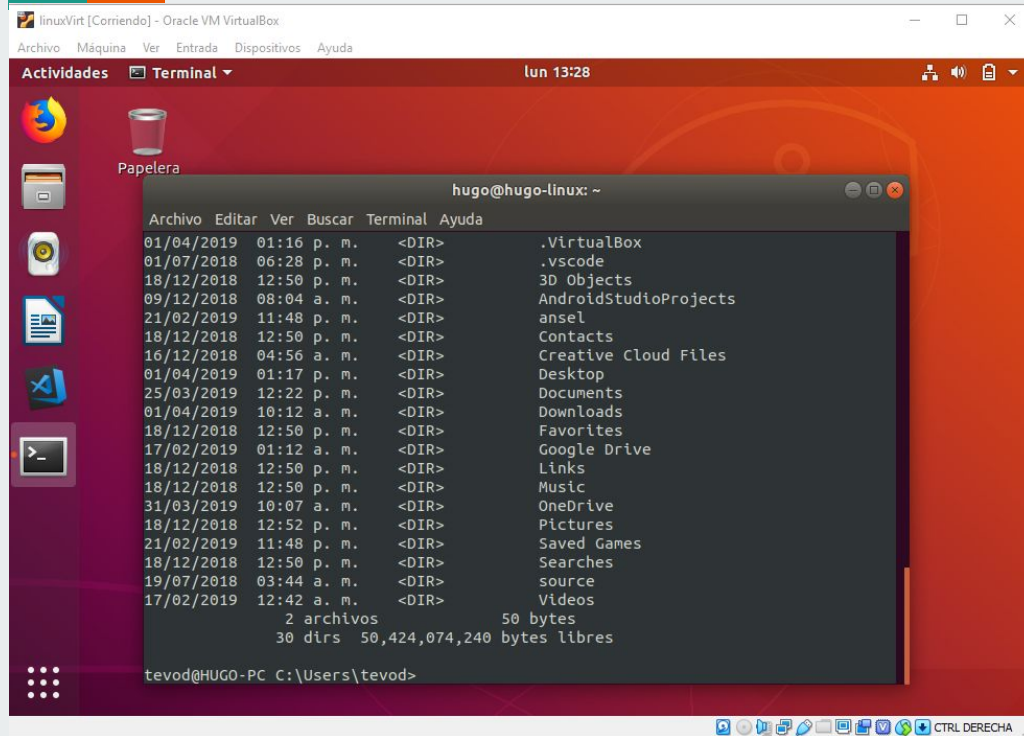


## Conexión con el servidor SSH Windows





# Conexión establecida





# Crear clave SSH




```
ssh-keygen
```

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/demo/.ssh/id_rsa):
```


```
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
```



Your identification has been saved in /root/.ssh/id\_rsa.  
Your public key has been saved in /root/.ssh/id\_rsa.pub.  
The key fingerprint is:  
8c:e9:7c:fa:bf:c4:e5:9c:c9:b8:60:1f:fe:1c:d3:8a root@here  
The key's randomart image is:

```
+--[ RSA 2048]-----+
|
|
|
|      +
|    o S  .
|   o  . * +
|   o + = O .
|     + = = +
|   ....EO+
+-----+
```



This procedure has generated an RSA SSH key pair, located in the `.ssh` hidden directory within your user's home directory. These files are:

- `~/.ssh/id_rsa`: The private key. DO NOT SHARE THIS FILE!
- `~/.ssh/id_rsa.pub`: The associated public key. This can be shared freely without consequence.



## Copiar clave ssh a servidor con ssh-copy-id

```
ssh-copy-id username@remote_host
```

```
The authenticity of host '111.111.11.111 (111.111.11.111)' can't be established.  
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.  
Are you sure you want to continue connecting (yes/no)? yes  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now  
demo@111.111.11.111's password:
```



Number of key(s) added: 1

Now try logging into the machine, with: `"ssh 'demo@111.111.11.111'"`  
and check to make sure that only the key(s) you wanted were added.



# Copiar clave ssh a servidor sin ssh-copy-id

```
cat ~/.ssh/id_rsa.pub | ssh username@remote_host "mkdir -p ~/.ssh && cat >>
~/.ssh/authorized_keys"
```

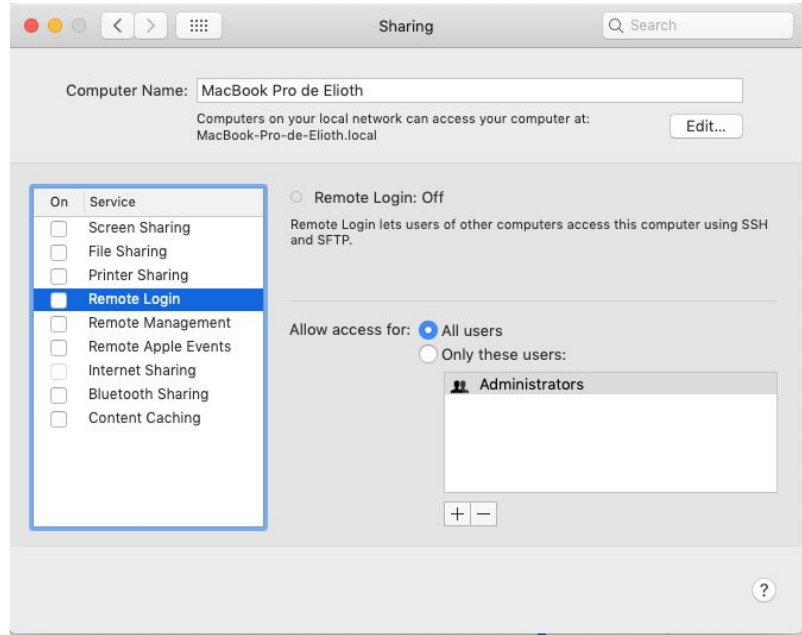
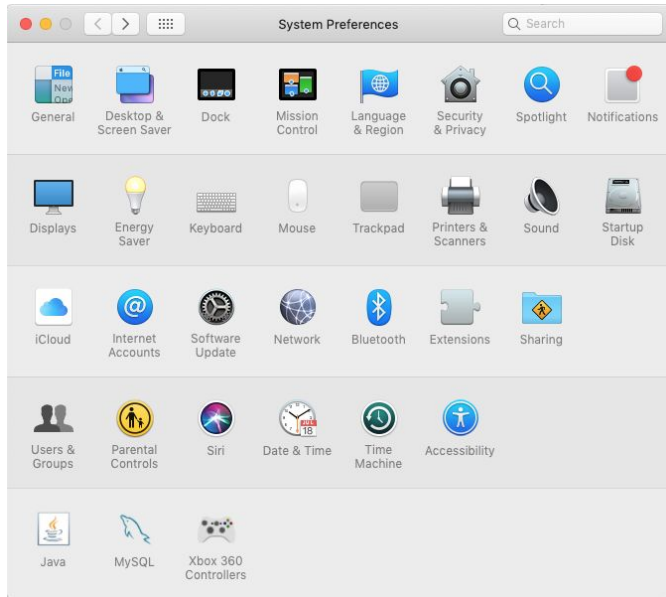
```
The authenticity of host '111.111.11.111 (111.111.11.111)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
demo@111.111.11.111's password:
```



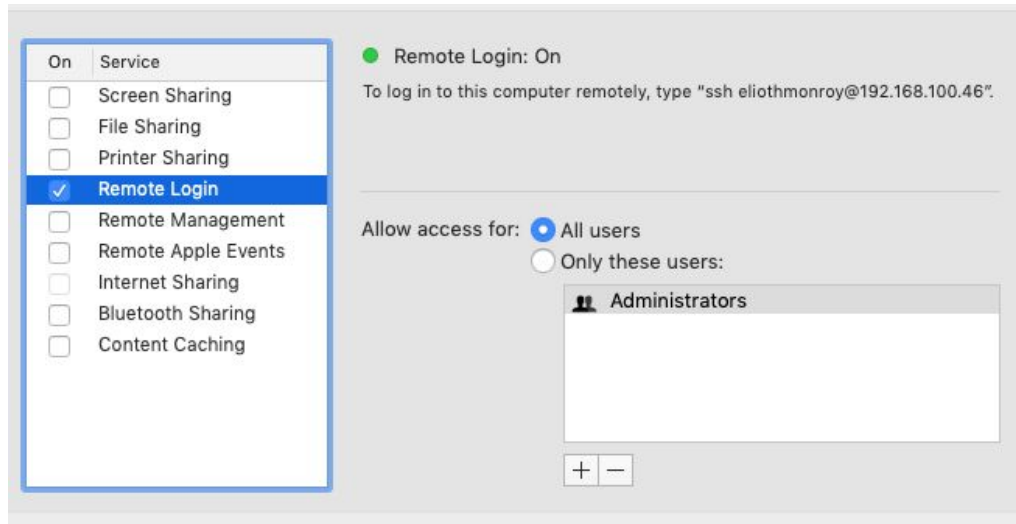


# MacOS

# Servidor



## Servidor (2)




The screenshot shows the 'Sharing' pane in macOS System Preferences. On the left, a list of services is shown with checkboxes. 'Remote Login' is checked and highlighted with a blue bar. On the right, the 'Remote Login' status is 'On', indicated by a green dot. Below this, a text box provides the SSH command to log in remotely: `ssh eliothmonroy@192.168.100.46`. Further down, the 'Allow access for:' section has two radio buttons: 'All users' (selected) and 'Only these users:'. Under 'Only these users:', there is a list box containing 'Administrators' with a user icon to its left. At the bottom of the list box are '+' and '-' buttons.

On	Service
<input type="checkbox"/>	Screen Sharing
<input type="checkbox"/>	File Sharing
<input type="checkbox"/>	Printer Sharing
<input checked="" type="checkbox"/>	Remote Login
<input type="checkbox"/>	Remote Management
<input type="checkbox"/>	Remote Apple Events
<input type="checkbox"/>	Internet Sharing
<input type="checkbox"/>	Bluetooth Sharing
<input type="checkbox"/>	Content Caching

**Remote Login: On**

To log in to this computer remotely, type `"ssh eliothmonroy@192.168.100.46"`.

Allow access for: ☒ All users ☐ Only these users:

 Administrators

+ -



## Servidor (3)

```
[MacBook-Pro-de-Elioth:Pictures eliothmonroy$ ssh localhost  
[Password:  
Last login: Sun Mar 31 20:45:41 2019 from ::1  
MacBook-Pro-de-Elioth:~ eliothmonroy$
```

```
MacBook-Pro-de-Elioth:~ eliothmonroy$ ssh eliothmonroy@192.168.100.46  
[Password:  
Last login: Sun Mar 31 20:51:04 2019 from ::1  
MacBook-Pro-de-Elioth:~ eliothmonroy$ █
```

Con control+D podemos terminar el proceso



## Servidor (4)

```
The authenticity of host '111.111.11.111 (111.111.11.111)' can't be established.  
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.  
Are you sure you want to continue connecting (yes/no)? yes
```



## Servidor (5)

```
[MacBook-Pro-de-Elioth:~ eliothmonroy$ ssh localhost  
ssh: connect to host localhost port 22: Connection refused  
MacBook-Pro-de-Elioth:~ eliothmonroy$
```

# Agente

```
MacBook-Pro-de-Elioht:~ eliothmonroy$ ssh eliothmonroy@192.168.100.88
The authenticity of host '192.168.100.88 (192.168.100.88)' can't be established.
ECDSA key fingerprint is SHA256:SfL5I3+rIDCT2A280URT5qxuEsHh8Nfj6vnhEveEVMi.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.88' (ECDSA) to the list of known hosts.
eliothmonroy@192.168.100.88's password:
Welcome to Ubuntu 18.10 (GNU/Linux 4.18.0-16-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

eliothmonroy@eliothmonroy-VirtualBox:~$ █
```



# Links útiles

- <https://dev.to/zduey/how-to-set-up-an-ssh-server-on-a-home-computer>
- <https://www.digitalocean.com/community/tutorials/ssh-essentials-working-with-ssh-servers-clients-and-keys>
- <https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/>
- <https://www.ssh.com/ssh/server>
- <https://geekytheory.com/copiar-archivos-a-traves-de-ssh-con-scp>