Como generar una clave SSH en Windows

La autenticación con clave pública para conectarse a un servidor remoto usando el protocolo SSH funciona con dos claves: una pública y otra privada. Para entender el funcionamiento se suele recurrir a la metáfora del candado y la llave. La clave pública funciona como un candado y la privada como la llave. El candado se colocará en el servidor remoto al que se quiere acceder; cuando se intenta acceder se comprobará que la máquina que intenta conectar tiene la llave, la clave privada.

Para configurar el acceso SSH con clave pública hay que:

Generar el par de claves pública/privada.

Copiar la clave pública al servidor.

Deshabilitar el acceso al servidor con contraseña.

CÓMO GENERAR EL PAR DE CLAVES PÚBLICA/PRIVADA

Hay dos formas de hacer esto, por un lado con putty y por otro lado con el subsistema de Linux para Windows

Generar par de claves mediante putty

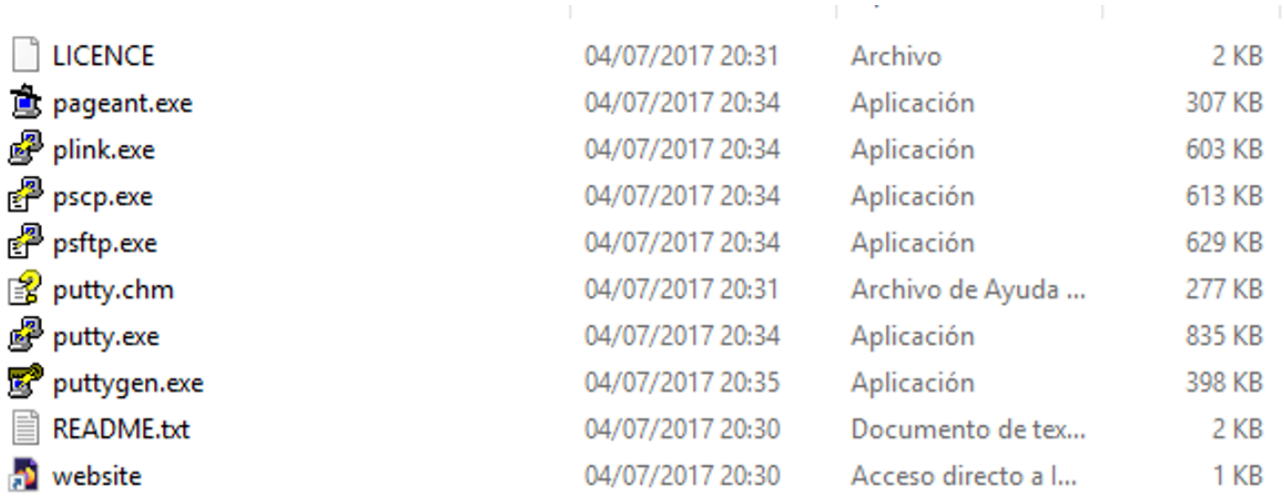
Para generar las claves se puede usar ssh-keygen en la máquina local desde la que se quiere conectar con el servidor:

Podemos descargarnos Putty de su página oficial https://www.putty.org/ en ella encontraremos un enlace a las descargas de Putty

Encontramos tres versiones, la de Windows x86 de 64 Bits, la de Windows x86 de 32 bits y la de de WIndows ARM de 64 bits.

Descargamos ell archivo, lo instalamos y tendremos en la carpeta Archivos de programa putty los ejecutables.

En dicha carpeta vemos los siguientes archivos



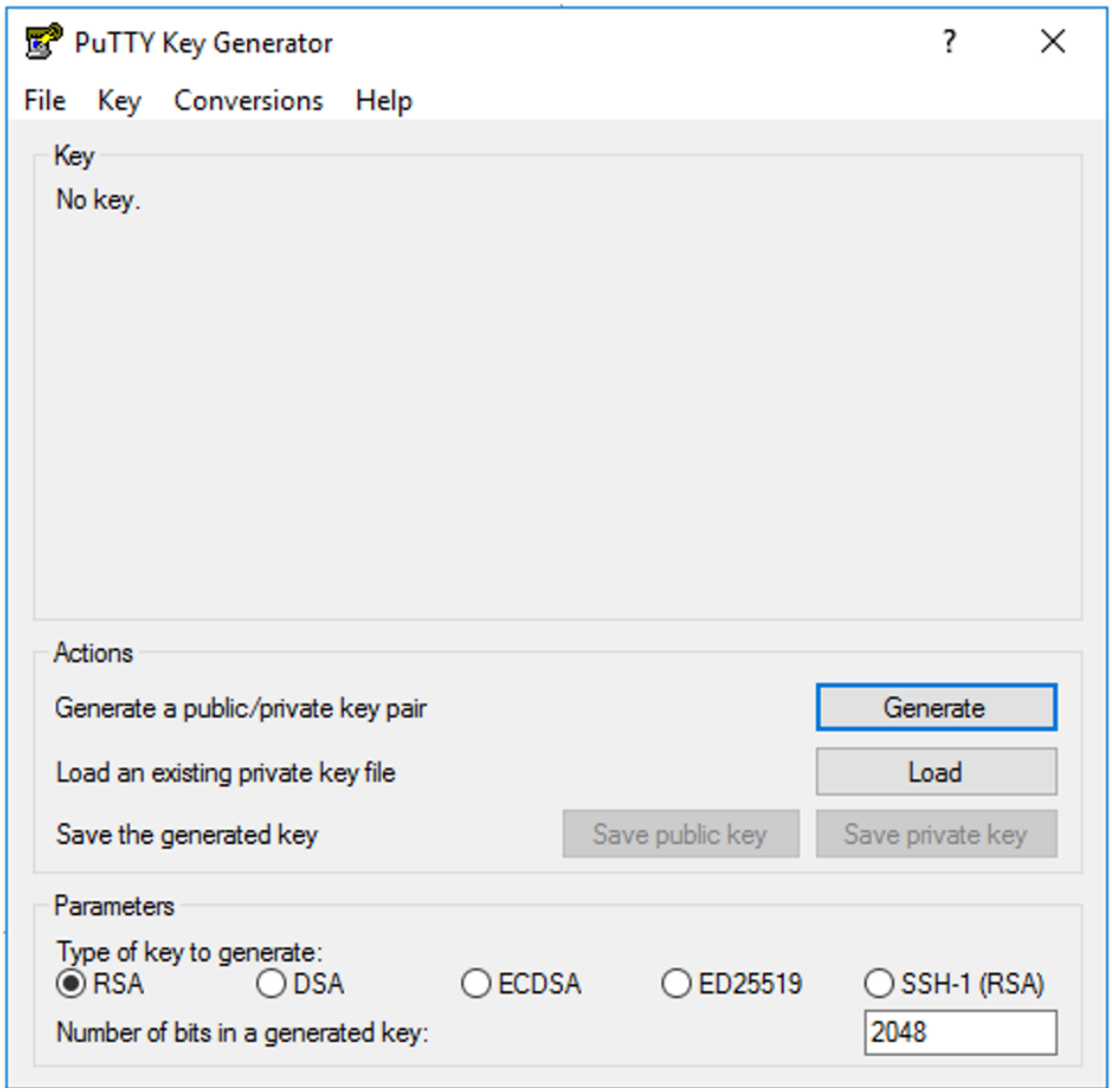
LICENCE	04/07/2017 20:31	Archivo	2 KB
pageant.exe	04/07/2017 20:34	Aplicación	307 KB
plink.exe	04/07/2017 20:34	Aplicación	603 KB
pscp.exe	04/07/2017 20:34	Aplicación	613 KB
psftp.exe	04/07/2017 20:34	Aplicación	629 KB
putty.chm	04/07/2017 20:31	Archivo de Ayuda ...	277 KB
putty.exe	04/07/2017 20:34	Aplicación	835 KB
puttygen.exe	04/07/2017 20:35	Aplicación	398 KB
README.txt	04/07/2017 20:30	Documento de tex...	2 KB
website	04/07/2017 20:30	Acceso directo a l...	1 KB

Vemos que hay varios ejecutables, pero el que nos interesa es el puttygen.exe.

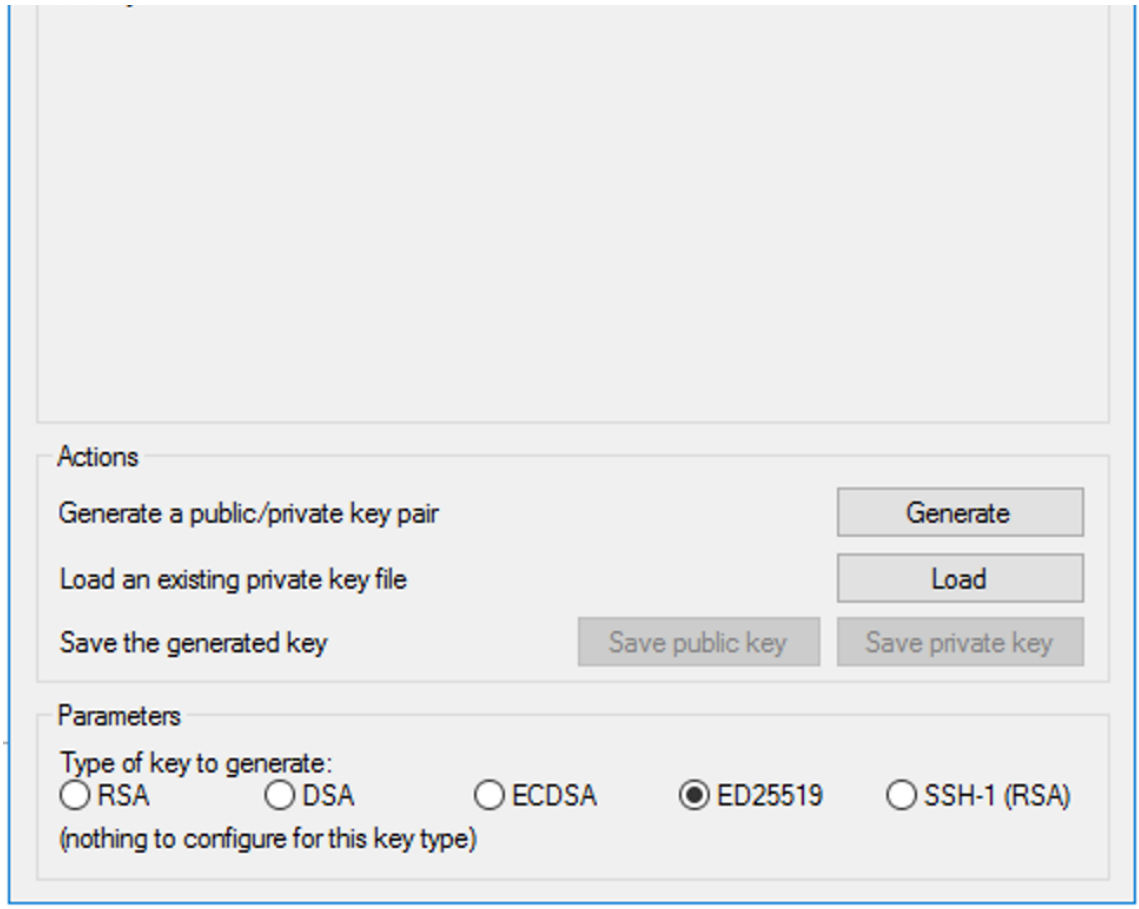
PuTTYgen es una herramienta generadora de claves para crear claves SSH para PuTTY.

Es análoga a la herramienta ssh-keygen utilizada en Linux.

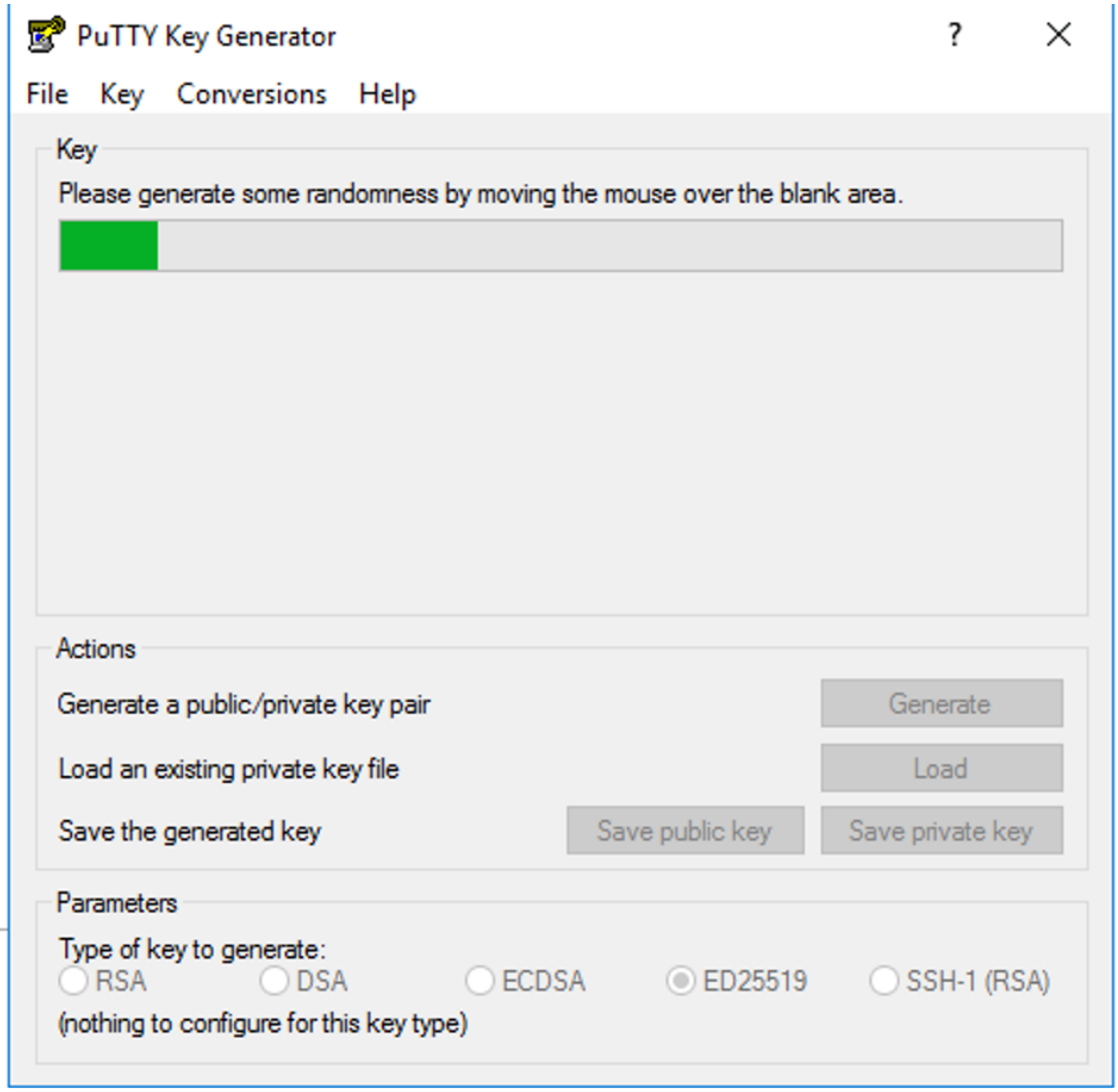
La ejecutamos y nos aparecerá la siguiente pantalla.



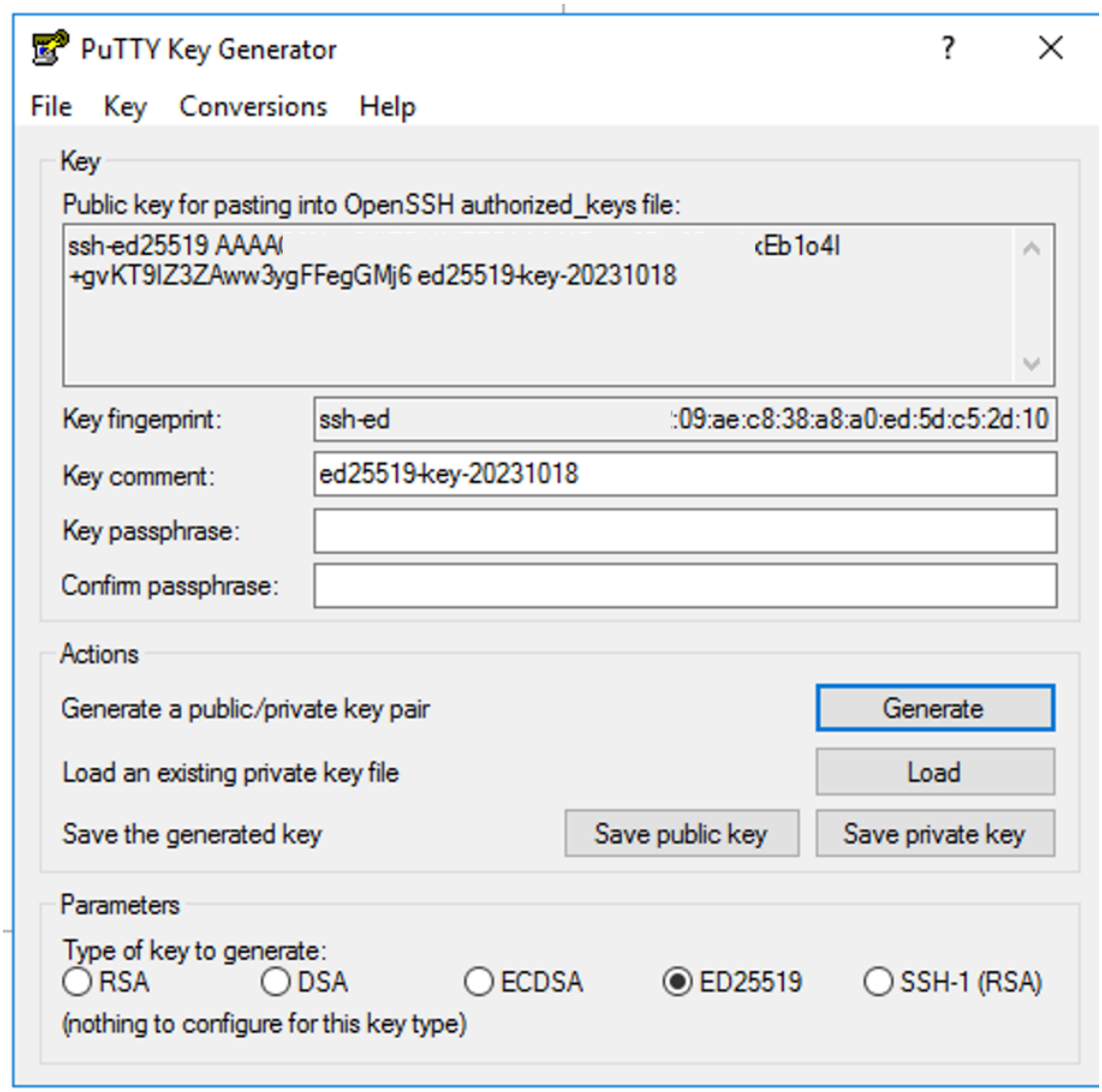
En esta pantalla, podemos ver que podemos generar varios tipos de claves. Las claves SSH antiguas usaban RSA, en la actualidad es preferible usar ED22519 por seguridad y facilidad de uso, ya que las claves son mucho más cortas.



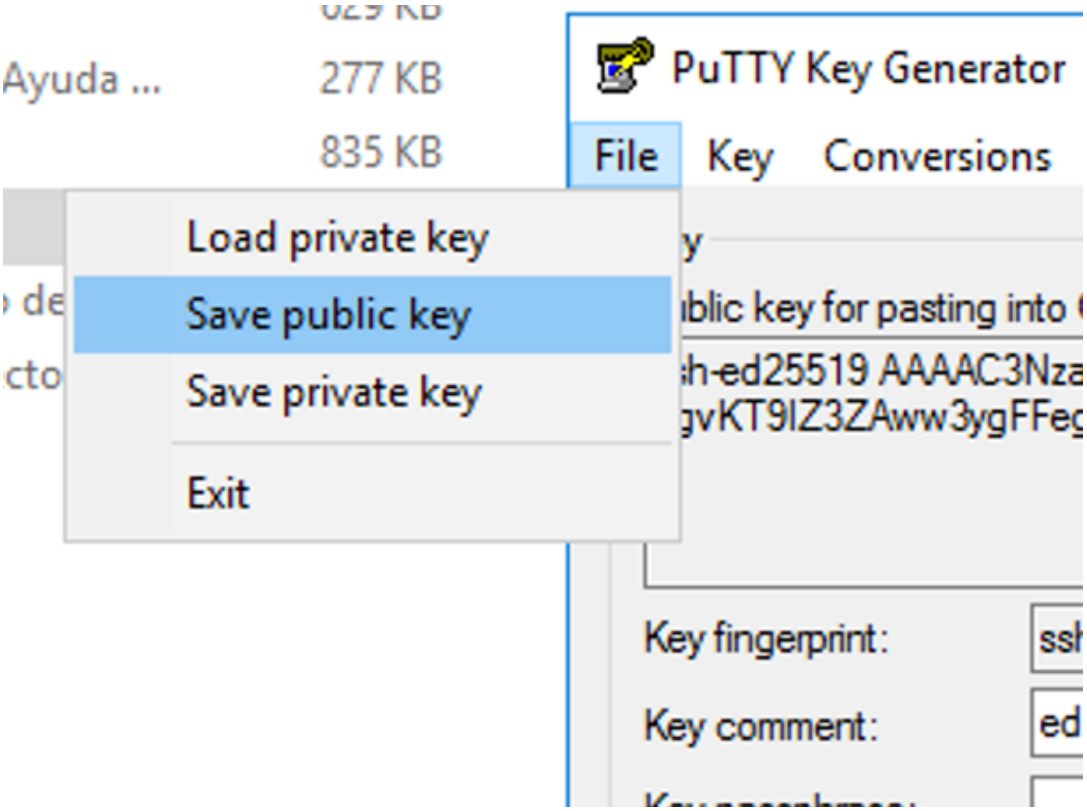
Seleccionamos ED25519 y pulsamos en Generate (Generar). Nos pedirá que movamos el ratón para generar la entropía suficiente para que la clave generada sea aleatoria



Una vez terminado el proceso, se habrá generado el conjunto de clave privada / clave pública como vemos en la siguiente imagen (Algunos datos se han ofuscado por privacidad)



Ahora sólo nos queda guardar estas claves la pública y la privada



IMPORTANTE: Nunca, nunca, nunca proporciones tu clave privada a nadie, y realiza una copia (o varias) de seguridad de ambos ficheros, ya que si mañana cambias de ordenador, usando tu clave privada en el nuevo ordenador, podrás acceder de nuevo a los servidores que tengan como autenticación tu clave pública.

GENERAR LA CLAVE CON EL SUBISTEMA DE LINUX EN WINDOWS

Este proceso es el mismo que se usa en cualquier sistema Linux, tal y como se explica aquí

COPIAR LA CLAVE PÚBLICA AL SERVIDOR

Una vez generado el par de claves en la máquina local hay que copiar la clave pública al servidor remoto. Esto lo podemos realizar de dos formas

CON SCP

```
user@localmachine$ scp ~/.ssh/id_rsa.pub user@remotemachine:/home/user/uploaded_key.pub
```

La clave pública hay que incluirla en el archivo /home/user/.ssh/authorized_keys. Si la carpeta .ssh no existe, la creamos antes de copiar, así como el archivo authorized_keys:

```
user@remotemachine$ mkdir .ssh
user@remotemachine$ chmod 700 .ssh
user@remotemachine$ touch .ssh/authorized_keys
user@remotemachine$ chmod 600 .ssh/authorized_keys
```

Por último copiamos la clave y borramos el archivo copiado al servidor:

```
user@remotemachine$ echo `cat ~/uploaded_key.pub` >> ~/.ssh/authorized_keys
user@remotemachine$ rm /home/user/uploaded_key.pub
```

USANDO SSH-COPY-ID

```
user@localmachine$ssh-copy-id -i ~/.ssh/id_rsa.pub user@remotemachine
user@remotemachine$ password:
Now try logging into the machine, with "ssh 'remote-host'", and check in:
.ssh/authorized_keys
```

DESHABILITAR EL ACCESO AL SERVIDOR CON CONTRASEÑA

Una vez habilitado el acceso SSH mendiante clave pública, se puede deshabilitar el acceso con contraseña. Esto aumentará la seguridad, pero implica que si se pierde la clave privada se perderá el acceso al servidor: hay que guardar cuidadosamente la clave privada.

La configuración del servidor SSH se puede encontrar en el archivo /etc/ssh/sshd_config. Para deshabilitar el acceso SSH con contraseña hay que añadir la siguiente línea, editando el archivo como root:

```
PasswordAuthentication no
```

Para aumentar la seguridad se pueden hacer dos ajustes adicionales en el archivo /etc/ssh/sshd_config:

Desactivar el acceso ssh para el usuario root:

```
PermitRootLogin no
```

Dar acceso SSH solo a los usuarios que lo necesiten, y no a todos:

```
AllowUsers usuario1 usuario2
```

Una vez realizados los cambios, hay que reiniciar el servidor SSH, siempre como root:

```
service sshd restart
```

ACCEDER AL SERVIDOR CON CLAVE PÚBLICA

Para conectarse al servidor con clave pública en vez de contraseña

```
user@localmachine$ ssh user@remotemachine
```

Revision #1
Created 18 October 2023 14:21:27 by Admin
Updated 18 October 2023 14:44:21 by Admin