**Paso 3: Crea un nuevo usuario y modifica sus privilegios**

Cuando configuras un VPS, comienzas con un usuario **root** , que es la cuenta que has estado usando hasta ahora. Sin embargo, generalmente es una buena idea configurar otra cuenta de usuario con privilegios de superusuario.

La razón es que la cuenta **root** puede causar daños graves si no estás seguro de lo que estás haciendo. Una cuenta **root** tiene acceso total a todas las configuraciones de tu sistema, por lo que un solo comando incorrecto puede crear problemas serios.

Una cuenta de usuario normal con privilegios de superusuario, por otro lado, necesita agregar el prefijo **sudo** a cualquier comando que desee ejecutar usando privilegios administrativos. Esto puede parecer un pequeño cambio, pero marca una gran diferencia. Con este enfoque, deberás pensarlo dos veces antes de ejecutar cualquier comando con el prefijo **sudo**, lo cual puede ayudarte a evitar inconvenientes.

Ahora configura ese nuevo usuario ingresando el siguiente comando. Reemplaza la segunda parte con el nombre de usuario que quieras usar:

**adduser nuevonombredeusuario**

Luego, escribe esta línea para agregar ese usuario al grupo **sudo**, que le otorgará privilegios de superusuario (nuevamente, reemplazando la última parte con tu nuevo nombre de usuario):

**# usermod -aG sudo nuevonombredeusuario**

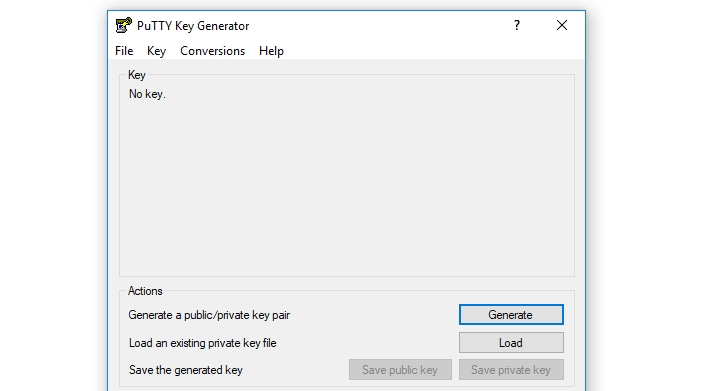
Ahora, solo nos resta crear una contraseña para esta cuenta. Sin embargo, hay un método que es mucho más seguro que usar una contraseña normal, que es lo que veremos a continuación.

**Paso 4: Habilita la autenticación de clave pública**

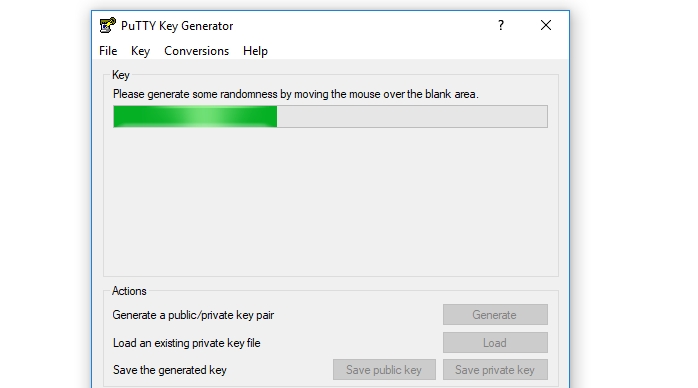
La [**autenticación de clave pública**](https://www.ssh.com/ssh/public-key-authentication) es una técnica que es posiblemente más segura que las contraseñas normales. Con este enfoque, generas un conjunto de claves tanto ‘públicas’ como ‘privadas’.

Tu servidor almacenará tu clave pública y la utilizará para autenticar la privada, a la que solo tu tendrás acceso como un archivo en tu computadora. Una vez que configures la autenticación de clave pública, necesitarás tanto la clave privada como una frase de contraseña para iniciar sesión, lo cual aumenta significativamente la seguridad.

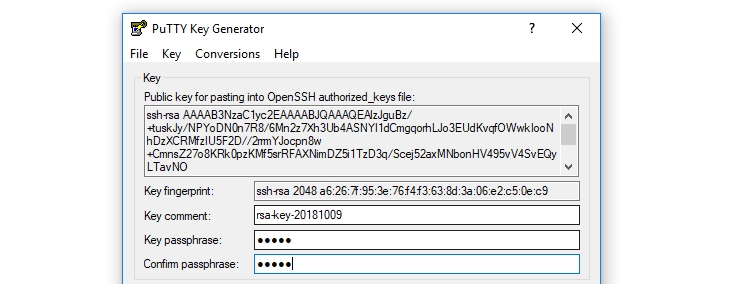
Para generar claves SSH en Windows, puedes usar [**la aplicación PuTTYgen**](https://www.ssh.com/ssh/putty/windows/puttygen), que se habrá instalado cuando configuraste el cliente anteriormente (para obtener información sobre cómo hacerlo en sistemas Linux/Unix, consulta esta guía). Busca entre tus programas y ejecuta la aplicación PuTTYgen ahora, que debería verse así:



Está bien usar la configuración predeterminada para tu par de claves, así que haz clic en el botón **Generate**. Para hacer que tu clave sea más única, el programa te pedirá que muevas el mouse para que resulte una clave más aleatoria, lo cual es bastante bueno:



En seguida, el programa te mostrará la clave pública que generó para ti. Antes de que hagas cualquier otra cosa, configura una frase de contraseña que la acompañe, la cual actuará como una contraseña para la clave:



Ahora, pulsa el botón **Save private key** (Guardar clave privada) y guarda el archivo resultante en tu computadora. También deberás copiar tu clave pública en un momento, así que no cierres esta ventana todavía.

Luego, vuelve a iniciar sesión en tu servidor con el usuario **root** original y ve al directorio de inicio de tu nueva cuenta usando **# su – nuevonombredeusuario**. La línea de comandos ahora reflejará tu nuevo usuario:



Después de eso, deberás ejecutar una serie de comandos en orden, lo que creará una nueva carpeta para tu clave pública, restringirá los permisos de esa carpeta y guardará tu clave:

mkdir ~/.ssh

chmod 700 ~/.ssh

nano ~/.ssh/authorized\_keys

El último comando abrirá [**el editor Nano**](https://www.hostinger.es/tutoriales/instalar-nano-text-editor), lo cual te permite modificar el nuevo archivo **authorized\_keys** en tu servidor. Ahora copia tu clave pública desde la ventana de PuTTYgen, y pégala aquí.

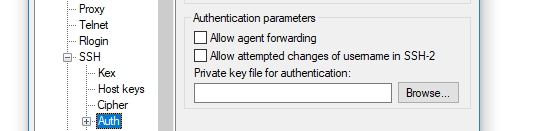
Cuando la clave esté lista, presiona **CTRL + X** para cerrar el editor y escribe **Y** cuando te solicite que confirmes los cambios en el archivo. Luego, escribe los dos siguientes comandos:

chmod 600 ~/.ssh/authorized\_keys

exit

Esos cambiarán los permisos del archivo que acabas de editar y luego te regresará al usuario **root**.

A continuación, deberás configurar PuTTY para que use tu clave privada cuando te conectes a tu servidor para que pueda reconocerte. Para hacer esto, regresa a la pantalla principal de la aplicación y vaya a la sección **Connection › SSH › Auth**. En el interior, encontrarás un campo llamado **Private key file for authentication** (Archivo de clave privada para autenticación):



Haz clic en el botón **Browse** (Explorar) y luego localiza el archivo de clave privada que almacenaste en tu computadora. Selecciónalo y listo.

Finalmente, debes decirle a tu servidor que deshabilite el método predeterminado de autenticación solo con contraseña para el nuevo usuario que acabas de configurar. Para hacerlo, inicia sesión en tu servidor como el nuevo usuario a través de SSH y ejecuta este comando:

sudo nano /etc/ssh/sshd\_config

Esto abrirá el archivo **sshd\_config** usando el editor Nano. Busca la línea que dice **PasswordAuthentication** dentro de ese archivo y elimina el signo **#** que se encuentra delante de él. Luego, cambia su valor de **Yes** a **No**, para que se vea así:

PasswordAuthentication no

Guarda los cambios en el archivo y reinicia el servidor. La próxima vez que intentes iniciar sesión, solo podrás hacerlo usando tu clave privada y frase de contraseña.