* Instalar servidor SSH sobre Termux en Android

Texto

Descripción generada automáticamente

**Instalar servidor SSH sobre Termux en Android**

[2 comentarios](https://parzibyte.me/blog/2019/07/31/servidor-ssh-termux-android/#comments) / [Android](https://parzibyte.me/blog/category/android/), [linux](https://parzibyte.me/blog/category/linux/), [Servidores](https://parzibyte.me/blog/category/servidores/), [Termux](https://parzibyte.me/blog/category/termux/) / Por [parzibyte](https://parzibyte.me/blog/author/parzibyte/" \o "Ver todas las entradas de parzibyte)

**Servidor SSH en Termux usando OpenSSH**

En este post te mostraré cómo instalar un servidor **SSH en Termux** para que puedas iniciar sesión de forma remota.

La ventaja de esto es que podrás conectarte desde una PC u otro lugar en donde puedes conectar un teclado (ya que con el teclado del teléfono es complicado)

Vamos a usar el servidor **openssh** y veremos la forma de autenticar usando **contraseña**, o usando **claves públicas y privadas**.

**Nota:** recuerda [**configurar e instalar Termux**](https://parzibyte.me/blog/2018/11/14/configurar-termux-android-linux/), y no olvides ejecutar termux-setup-storage como en el tutorial que cito.

**Instalar OpenSSH y herramientas**

Comenzamos actualizando los repositorios, e instalando el paquete **openssh**:

pkg upgrade

pkg install openssh

En ambos casos, si pregunta, elegimos que sí escribiendo la letra Y.

También es necesario instalar net-tools y procps con:

pkg install net-tools (averiguar IP)

pkg install procps (matar procesos)

pkg install nano (para editar archivos)

**Ajustes de OpenSSH**

La configuración de OpenSSH está en $PREFIX/etc/ssh/sshd\_config y podemos verla navegando con cd $PREFIX/etc/sshd y después usar cat sshd\_config:

[Texto

Descripción generada automáticamente con confianza media](https://parzibyte.me/blog/wp-content/uploads/2019/07/Mostrar-ajustes-de-OpenSSH.jpg)Autenticación con contraseña activa

El parámetro PasswordAuthentication está en yes, así que podemos ingresar con un usuario y contraseña en lugar de claves públicas y privadas.

Más adelante vamos a ver cómo cambiar este parámetro, ya que la autenticación con contraseña no es recomendada.

**Iniciar y detener demonio SSH**

Para iniciar el demonio, es decir, escuchar conexiones, se ejecuta:

sshd

Para matarlo o detenerlo, se usa:

pkill sshd

pkill viene con procps, por eso era necesario instalarlo.

**Nota:** se escucharán conexiones en el **puerto 8022**.

**Conexión a servidor SSH en Android**

Ya estamos escuchando conexiones SSH, pero todavía no sabemos nuestro **usuario, contraseña e IP**.

Averigua tu usuario escribiendo:

whoami

Ahora ponle una contraseña segura ejecutando:

passwd

[Texto

Descripción generada automáticamente](https://parzibyte.me/blog/wp-content/uploads/2019/07/Averiguar-usuario-y-cambiar-contrase%C3%B1a.jpg)Mostrar usuario con whoami y cambiar contraseña usando passwd

Finalmente mira cuál IP tienes, escribiendo:

ifconfig

(este comando viene con las **net-tools**)

Cuando tengas esos datos ya puedes conectarte desde otro lugar. Si usas linux en el terminal cliente ejecuta:

ssh TU\_IP -p 8022

En caso de que uses Putty, rellena los campos y listo.

Cualquiera de los dos métodos, te llevará al proceso de autenticación, escribe el usuario y la contraseña y ya está.

[Texto

Descripción generada automáticamente](https://parzibyte.me/blog/wp-content/uploads/2019/07/Entrar-a-servidor-SSH-en-Termux-usando-Putty.png)Conexión a servidor SSH en Termux, usando Putty en Windows

Ya puedes administrar tu [“servidor” de Linux sobre Android](https://parzibyte.me/blog/2018/11/14/configurar-termux-android-linux/) de manera remota.

Si muestra un aviso sobre *“the server’s host key”* haz click en **Sí**

**Nota:** no se recomienda para nada usar autenticación con usuario y contraseña, lo mejor y más seguro es usar claves públicas y privadas.

**Autenticación con clave pública y privada**

Este método es el que se recomienda, pues agrega más seguridad y evita ataques de fuerza bruta.

Comenzamos preparando nuestro dispositivo creando el folder **.ssh** y el archivo authorized\_keys; además de darles permiso.

Esto lo puedes hacer desde tu dispositivo o usando un cliente SSH (es decir, vamos a configurar las claves, pero por el momento, antes de configurarlas, podemos usar todavía la autenticación no segura)

[Texto

Descripción generada automáticamente](https://parzibyte.me/blog/wp-content/uploads/2019/07/Crear-directorio-de-SSH-en-Android.png)

Los comandos son:

touch ~/.ssh/authorized\_keys

chmod 600 ~/.ssh/authorized\_keys

chmod 700 ~/.ssh

Copy

El siguiente paso es generar un par de claves usando Putty como se ve [**en este tutorial**](https://parzibyte.me/blog/2019/01/11/autenticacion-windows-ubuntu-server-putty-claves-ssh/) detallado.

Si seguiste bien el tutorial de [generación de claves públicas y privadas](https://parzibyte.me/blog/2019/01/11/autenticacion-windows-ubuntu-server-putty-claves-ssh/), tu conexión de Putty debe verse así (fíjate en la parte superior, dice *Authenticating with public key*):

[Texto

Descripción generada automáticamente](https://parzibyte.me/blog/wp-content/uploads/2019/07/Autenticaci%C3%B3n-con-clave-p%C3%BAblica-a-SSH-de-Android-sobre-Termux.png)Usar Putty y clave pública para una nueva sesión SSH en Android

**Desactivar autenticación con contraseña**

Ahora que ya tienes autenticación por clave pública y privada, desactiva (lo recomiendo altamente, por la seguridad) la **autenticación por contraseña**.

Navega hasta $PREFIX/etc/ssh/ y modifica el archivo sshd\_config usando si quieres nano sshd\_config; en donde dice PasswordAuthentication escribe no.

[Captura de pantalla de un celular

Descripción generada automáticamente](https://parzibyte.me/blog/wp-content/uploads/2019/07/Desactivar-autenticaci%C3%B3n-por-contrase%C3%B1a-en-SSH-sobre-Android.png)

Guarda los cambios (CTRL + O, luego ENTER si usas **nano**) y reinicia el servidor SSH; esto hazlo desde la app de Termux pues si lo haces por SSH la conexión se romperá (obviamente)

Detén el servidor con pkil sshd y después vuelve a iniciarlo con sshd.

Así es como termina este tutorial; recuerda que tengo más material interesante sobre [Termux](https://parzibyte.me/blog/category/termux/), [Linux](https://parzibyte.me/blog/category/linux/) y [Android](https://parzibyte.me/blog/category/android/) en mi blog.

Finalmente, dejo una [referencia](https://wiki.termux.com/wiki/Remote_Access) a la wiki de Termux.