

Es un protocolo de red seguro que se utiliza para conectarse a un servidor remoto y controlarlo de forma segura a través de una red. SSH proporciona un método muy seguro y fiable.

Utiliza comúnmente para administrar servidores remotos, transferir archivos y realizar otras tareas de red de forma segura y confiable

Para poder administrarlo lo esencial a saber son los comandos.

Los cuales són ...

1. Primero de todo deberemos instalar SSH. El comando através de la terminal de UBUNTU para descargarlo es [\(`sudo apt install ssh` \)](#).
2. El siguiente comando [\(`ssh user@ip_srv` \)](#) se utiliza para establecer una conexión SSH a un servidor remoto con una dirección IP específica.
3. Usaremos el siguiente comando [\(`/etc/init.d/ssh status` \)](#) comprobaremos el servicio SSH este en marcha, en pausa o apagado.
4. El comando [\(`.ssh-keygen -t rsa` \)](#) se utiliza para generar 2 claves, pública y privada. La clave pública se puede colocar en el servidor remoto para impedir que nos solicite la contraseña todo el tiempo, mientras que la clave privada se utiliza para autenticar al usuario en el servidor remoto.
5. Se utiliza el siguiente comando [\(`cat -ssh/id_rsa.pub` \)](#) para mostrar la clave pública SSH que ha sido generada para el usuario.
6. El comando [\(`nano ~/.ssh/authorized_keys` \)](#) en Ubuntu se utiliza para abrir y editar el archivo `authorized_keys`, que es donde meteremos la clave pública para que no nos vuelva a pedir la contraseña.