# Tip cortos para linux

# Instala paquetes desde una lista de paquetes linea a linea

```
sudo apt update && xargs -a fichero.txt -I {} sudo apt install -y {}
```

# Llaves con lagoritmo EdDSA (Ed25519) ?

En esta era donde la inteligencia artificial avanza rápidamente y la computación cuántica comienza a dejar de ser ciencia ficción, es prudente reforzar nuestras prácticas de seguridad, especialmente en entornos de administración remota.

Una mejora sencilla pero significativa es abandonar el tradicional algoritmo RSA en favor de Ed25519, una variante del algoritmo EdDSA (Edwards-curve Digital Signature Algorithm), que ofrece:

- Mayor seguridad con claves más pequeñas (256 bits vs 2048/4096 en RSA)
- Mejor rendimiento y menor consumo de recursos
- Recomendado por OpenSSH y ampliamente compatible con servidores modernos

# Generar una clave Ed25519 sin interacción (ssh-keygen)

Para generar una clave SSH sin contraseña y sin preguntas interactivas, ejecuta:

```
ssh-keygen -t ed25519 -a 100 -C "$(whoami)@$(hostname)" -f ~/.ssh/id_ed25519 -N ""
```

□□ Explicación de cada parámetro:

```
Opción□Significado
-t ed25519□Tipo de clave: Ed25519 (moderna y segura)
```

```
-a 100 Número de rondas de derivación con bcrypt (protege si hay passphrase)
-C "$(whoami)@$(hostname)" Comentario con nombre de usuario y host para identificar la clave
-f ~/.ssh/id_ed25519 Ruta donde se guarda la clave privada (y .pub para la pública)
-N "" Passphrase vacía (clave sin cifrar, útil para automatismos)
```

# ¿Cuándo usar claves sin passphrase?

Este tipo de clave puede ser útil en:

- Automatizaciones y scripts donde no es posible ingresar manualmente la passphrase
- Acceso controlado a través de restricciones en authorized_keys (from=, command=, etc.)
- Sistemas de CI/CD o servidores internos sin exposición directa

> ⚠ Advertencia: No usar claves sin passphrase en equipos compartidos o inseguros. Si alguien obtiene la clave privada, tendrá acceso inmediato sin requerir nada más.

# ? Verificar la clave generada

Puedes ver el fingerprint de la clave:

```
ssh-keygen -lf ~/.ssh/id_ed25519
```

# ? Referencias

- OpenSSH Key Management
- SSH Key: Ed25519 vs RSA

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

---

Revision #3
Created 15 August 2023 07:42:19 by Abkrim
Updated 2 June 2025 14:13:30 by Abkrim