

Termux is an **Android terminal emulator and Linux environment app** that works directly with no rooting or setup required. A minimal base system is installed automatically - additional packages are available using the APT package manager.



**Secure.** Access remote servers using the ssh client from OpenSSH. Termux combines standard packages with accurate terminal emulation in a beautiful open source solution.

**Feature packed.** Take your pick between Bash, fish or Zsh and nano, Emacs or Vim. Grep through your SMS inbox. Access API endpoints with curl and use rsync to store backups of your contact list on a remote server.

**Customizable.** Install what you want through the APT package management system known from Debian and Ubuntu GNU/Linux. Why not start with installing Git and syncing your dotfiles?

**Explorable.** Have you ever sat on a bus and wondered exactly which arguments tar accepts? Packages available in Termux are the same as those on Mac and Linux - install man pages on your phone and read them in one session while experimenting with them in another.

**Portable - With batteries included.** Can you imagine a more powerful yet elegant pocket calculator than a readline-powered Python console? Up-to-date versions of Perl, Python, Ruby and Node.js are all available.

**Ready to scale up.** Connect a Bluetooth keyboard and hook up your device to an external display if you need to - Termux supports keyboard shortcuts and has full mouse support.

**Tinkerable.** Develop by compiling Go, Rust, Swift, or C files with Clang and build your own projects with CMake and pkg-config. Both lldb/GDB and strace are available if you get stuck and need to debug.



## Sponsors and Funders

# Termux

*Termux es un emulador de terminal avanzado para Android diseñado para desarrolladores, administradores de sistemas y especialistas en ciberseguridad que necesitan un entorno Linux completo en movilidad. Permite transformar un dispositivo móvil en una estación de trabajo técnica para ejecutar scripts en Python, Node.js o Ruby, gestionar servidores vía SSH y realizar auditorías de red. Es ideal para profesionales que dominan la línea de comandos y buscan potencia sin necesidad de acceso root.*

[Visitar Sitio Oficial](#) [Preguntar a ChatGPT](#) [Preguntar a Claude](#) [Preguntar a Grok](#)

## Contenido del Dossier

- [Información de la Herramienta](#)
- [Consejos de Implantación](#)
- [Preguntas Frecuentes](#)
- [Contratos y Condiciones](#)

## INFORMACIÓN DE LA HERRAMIENTA

---

### Qué y para quién es

Termux es un emulador de terminal avanzado para Android que proporciona un entorno Linux completo sin necesidad de acceso root o configuraciones complejas. Es una herramienta diseñada para desarrolladores, administradores de sistemas, especialistas en ciberseguridad y entusiastas de la informática que necesitan un entorno de desarrollo o ejecución de scripts portátil y potente sobre arquitectura ARM o x86\_64.

### Principal ventaja profesional

Permite transformar un dispositivo móvil en una estación de trabajo técnica completa, ofreciendo acceso a un sistema de gestión de paquetes (APT) con miles de herramientas de código abierto (Python, Node.js, Git, SSH) que funcionan de forma nativa en el sistema operativo Android.

### Para quién no es

No es una herramienta para usuarios domésticos que buscan aplicaciones de interfaz gráfica convencional o entretenimiento. Profesionales que requieran software privativo exclusivo de Windows/macOS o que no tengan familiaridad con la interfaz de línea de comandos (CLI) encontrarán la curva de aprendizaje frustrante e innecesaria.

### funcionalidades clave

- Entorno Linux aislado que no requiere particiones ni flasheos del dispositivo.
- Gestor de paquetes APT basado en la distribución Debian/Ubuntu para instalar herramientas de programación y redes.
- Soporte completo para lenguajes de programación incluyendo C/C++, Rust, Go, Python, Ruby y Node.js.
- Cliente y servidor SSH para administración remota de servidores desde el móvil o para acceder al móvil desde un PC.
- Posibilidad de ejecutar entornos de escritorio básicos y aplicaciones gráficas mediante servidores X11.
- Acceso a APIs de Android (contactos, GPS, cámara) mediante el addon Termux:API para automatización.

### Precios

- Versión gratuita: La aplicación y todos sus paquetes son completamente gratuitos y de código abierto (Open Source).
- Rango de precios: 0€. No existen suscripciones ni versiones premium, aunque se aceptan donaciones para el mantenimiento del proyecto.

### Perfil del usuario

Empresas de consultoría tecnológica, departamentos de IT, proveedores de servicios gestionados (MSP) y profesionales independientes de seguridad informática.

- Administradores de sistemas y DevOps.
- Desarrolladores de software y aplicaciones web.
- Auditores de seguridad y especialistas en Pentesting móvil.
- Ingenieros de redes.

### Nivel técnico requerido

- Nivel técnico para su uso: Alto. Requiere fluidez en entornos de terminal y sistemas tipo Unix/Linux.
- Nivel técnico para su instalación: Bajo. Se instala como cualquier otra aplicación, aunque su configuración óptima requiere comandos manuales.
- Necesidades de soporte: Generalmente autogestionado por el profesional; no suele requerir intervención del departamento de IT corporativo excepto para políticas de seguridad móvil.
- Conocimientos necesarios: Manejo de Bash/Zsh, gestión de paquetes Linux y familiaridad con protocolos de red.

### Ejemplos de uso profesional

- Pruebas de penetración y auditorías de red desde dispositivos móviles en el emplazamiento del cliente.
- Administración remota de servidores en la nube mediante SSH en situaciones de emergencia sin acceso a un portátil.
- Ejecución de scripts de automatización en Python para procesamiento de datos o logs en movilidad.
- Desarrollo y validación de código fuente localmente antes de subirlo a repositorios Git.

### Uso y distribución

- Versión móvil: Disponible para Android (recomendado vía F-Droid para actualizaciones).
- GitHub: Repositorio para código fuente y scripts de compilación.
- CLI: Interfaz pura de línea de comandos.

### Open source

Proyecto bajo licencia GPLv3. El código fuente de la aplicación, los scripts de construcción de los paquetes y los repositorios son públicos y auditables.

### Integraciones

- Facilidad de integración: Low code / Full code según el uso de scripts.
- API propia: Dispone de Termux:API, una extensión que permite a la línea de comandos interactuar con el hardware de Android mediante comandos simples.
- Ejemplos concretos: Integración con Tasker para automatizar tareas del sistema Android basadas en eventos, conexión con hosts remotos mediante OpenSSH y sincronización de archivos con Rclone.

### Notas finales

información legal, licencias, contratos

- El uso de la herramienta debe cumplir con las políticas de seguridad de la empresa (BYOD o dispositivos corporativos), ya que permite la ejecución de herramientas de red potentes.
- La versión de Google Play Store está oficialmente obsoleta debido a restricciones de nivel de API de Android; la versión mantenida es la distribuida por F-Droid y GitHub.

### Para más información:

- Sitio web oficial: <https://termux.dev/en>
- Github: <https://github.com/termux/termux-app>
- Wiki de documentación: [https://wiki.termux.com/wiki/Main\\_Page](https://wiki.termux.com/wiki/Main_Page)
- Repositorios de paquetes: <https://github.com/termux/termux-packages>

## CONSEJOS DE IMPLANTACIÓN

---

Aplicación profesional

- **Sectores:** Consultoría técnica, ciberseguridad, administración de sistemas (DevOps), ingeniería de redes y desarrollo de software.
- **Presupuesto:** 0€ (Open Source). Requiere inversión en tiempo para configuración y securización.
- **Puntos clave:** Movilidad extrema para tareas críticas, auditorías in-situ y administración de servidores sin necesidad de ordenador portátil.

Madurez digital requerida

- **Usuarios:** Nivel experto. Dominio de línea de comandos (CLI), gestión de paquetes Linux (APT) y protocolos de red (SSH/SFTP).
- **Equipo:** Capacidad de autogestión técnica y comprensión de entornos Unix/Linux.
- **Empresa:** Políticas de seguridad móvil (BYOD) claras, ya que la herramienta permite el uso de recursos de red potentes desde dispositivos personales.

Plan orientativo de implantación

Pasos necesarios y estimaciones

- **Evaluación inicial (1-2 días):** Identificación de casos de uso (ej. acceso a servidores, pentesting) y compatibilidad del hardware (ARM64 recomendado).
- **Instalación y configuración base (1 hora):** Descarga desde F-Droid o GitHub (Google Play está obsoleta). Ejecución de `pkg update && pkg upgrade`.
- **Despliegue de herramientas específicas (2-4 horas):** Instalación de entornos de ejecución (Python, Node.js), editores (Neovim) y utilidades de red (Nmap, OpenSSH).
- **Hardening y Seguridad (1 día):** Configuración de llaves SSH (ED25519), cifrado de almacenamiento local y configuración de VPN (ej. Tailscale) para aislar el tráfico.
- **Integración y Flujo de trabajo (Continuo):** Sincronización de archivos o repositorios Git para trabajar en movilidad.

Necesidades de formación del equipo

- Entrenamiento en administración remota vía terminal desde pantallas táctiles.
- Configuración de atajos de teclado y uso de multiplexores de terminal como tmux.
- Protocolos de seguridad específicos para terminales móviles (gestión de llaves privadas en Android).

Perfiles necesarios

- **Técnicos:** Administradores de sistemas, desarrolladores Full Stack o especialistas en seguridad (CISO/Pentester).
- **Personal externo:** No se requiere, salvo consultoría específica en ciberseguridad para auditar el uso de la app en la red corporativa.

Retorno de la inversión (ROI)

- **Tiempos:** Reducción drástica del Tiempo Medio de Respuesta (MTTR) ante incidencias críticas al permitir intervención inmediata desde el móvil.
- **KPIs:** Número de incidencias resueltas en movilidad, disponibilidad del sistema, ahorro en hardware (sustitución parcial de portátiles en tareas ligeras de monitorización).

Otros

- **Seguridad Crítica:** Se recomienda utilizar termux-auth para añadir capas de autenticación biométrica a la terminal.
- **Limitación de API:** Para interactuar con sensores del móvil (GPS, batería), es imprescindible instalar el add-on Termux:API.
- **Actualizaciones:** No usar la versión de Play Store; las actualizaciones de seguridad solo se mantienen activas en los repositorios de F-Droid y GitHub.

## PREGUNTAS FRECUENTES

---

### ¿Qué es exactamente Termux y cuál es su utilidad en un entorno profesional?

Termux es un emulador de terminal avanzado para Android que proporciona un entorno de ejecución Linux completo y aislado. Funciona de forma nativa sobre arquitecturas ARM y x86\_64, permitiendo a los profesionales ejecutar herramientas de diagnóstico de red, compiladores de lenguajes de programación y scripts de automatización directamente en un dispositivo móvil sin necesidad de modificar el sistema operativo original (root).

### ¿Es Termux una herramienta de código abierto (Open Source)?

Sí, el proyecto está desarrollado bajo la licencia GPLv3. Tanto el código fuente de la aplicación como los scripts de compilación de sus paquetes son públicos y están disponibles para auditoría en GitHub, lo que garantiza transparencia y seguridad para el entorno corporativo.

### ¿Cuál es el coste de adquisición y mantenimiento de la herramienta?

Termux es una herramienta completamente gratuita. No requiere el pago de licencias, suscripciones ni existen versiones 'premium' de pago. Su mantenimiento se sustenta mediante una comunidad de voluntarios y donaciones opcionales, lo que supone un coste de propiedad (TCO) de cero euros para la empresa o el profesional independiente.

### ¿Es posible descargarlo de GitHub o repositorios oficiales?

Efectivamente. La distribución de Termux se realiza principalmente a través de su repositorio oficial en GitHub y mediante el repositorio de software libre F-Droid. Es importante destacar que la versión disponible en Google Play Store está obsoleta debido a restricciones técnicas de Android, por lo que se recomienda encarecidamente la instalación desde fuentes oficiales de la comunidad para recibir actualizaciones de seguridad.

### ¿Cumple con la normativa de seguridad y privacidad en el tratamiento de datos?

Termux opera como un entorno aislado dentro de Android. Por defecto, no recopila datos del usuario ni los envía a servidores externos. No obstante, al permitir el uso de herramientas de red y acceso al sistema de archivos a través de Termux:API, su implementación en el ámbito profesional debe estar sujeta a las políticas de seguridad móvil y cumplimiento (BYOD) de cada organización.

### ¿Funciona mediante interfaz gráfica o requiere conocimientos técnicos previos?

El uso de Termux es predominantemente técnico y se basa en una interfaz de línea de comandos (CLI). Aunque es posible ejecutar entornos de escritorio básicos mediante servidores X11, se requiere una curva de aprendizaje alta y familiaridad con sistemas tipo Unix/Linux, gestión de paquetes APT y comandos de terminal Bash o Zsh.

### ¿Qué lenguajes de programación y herramientas soporta para desarrollo?

Soporta una amplia gama de lenguajes como Python, Rust, Go, Node.js, Ruby y C/C++. Además, permite la integración con Git para el control de versiones y el uso de OpenSSH para la administración remota de servidores, convirtiendo el dispositivo móvil en una estación de trabajo técnica funcional.

### ¿Permite interactuar con el hardware del dispositivo Android?

Sí, a través del complemento opcional Termux:API. Esta extensión permite que los scripts ejecutados en la terminal interactúen con sensores GPS, la cámara, los contactos o el estado de la batería, facilitando la creación de automatizaciones complejas integradas con el hardware del terminal.

## CONTRATOS Y CONDICIONES

---

Informe técnico descriptivo: Termux

Termux es un emulador de terminal y entorno Linux para Android. Al tratarse de una herramienta de infraestructura y desarrollo de código abierto (Open Source), su impacto legal inicial es bajo, pero aumenta a **Alto** si se utiliza para procesar datos corporativos o realizar auditorías de seguridad sin supervisión.

Principales recomendaciones

- **Control de Inventario:** Registrar el uso de Termux en la empresa como una herramienta de desarrollo/administración para cumplir con el esquema de seguridad.
- **Evitar la versión de Google Play:** La versión de la Play Store está obsoleta y no recibe parches de seguridad. Utilizar únicamente versiones de F-Droid o GitHub.
- **Gestión de Auditorías:** Si se utiliza para Pentesting o auditorías de red, debe quedar reflejado en el contrato de servicios el uso de herramientas de código abierto instaladas en dispositivos móviles.
- **Política BYOD:** Establecer directrices claras sobre si los empleados pueden instalar Termux en dispositivos personales que acceden a redes corporativas, dado que permite SSH y redireccionamiento de puertos.

Privacidad y protección de datos

- **Responsabilidades:** El usuario es el único responsable del software que instale dentro de Termux (Python, bases de datos, etc.). La aplicación en sí no recolecta datos personales por defecto.
- **Ubicación de los datos:** Los datos se almacenan localmente en el directorio privado de la aplicación en el dispositivo Android. Si se sincronizan con servicios externos (vía scripts de Rclone o Git), la responsabilidad del cumplimiento del RGPD recae sobre la empresa.
- **Derechos ARCO:** Al ser un entorno local bajo control del usuario, la gestión de acceso y supresión se realiza directamente borrando los archivos o desinstalando la aplicación.

Propiedad intelectual

- **Propiedad de datos:** La empresa mantiene la propiedad total de cualquier script o código desarrollado dentro del entorno de Termux.
- **Licencia de software:** Termux se distribuye bajo licencia **GPLv3** (una licencia de "copyleft" fuerte). Esto implica que si la empresa modifica el código fuente de la aplicación Termux y lo distribuye, debe compartir dichas modificaciones bajo la misma licencia. El uso de librerías internas adicionales puede estar bajo licencia **MIT** o **Apache 2.0**.
- **Resultados:** Los programas o scripts creados por la empresa utilizando herramientas de Termux (como compiladores de C o Python) son propiedad intelectual de la empresa y no se ven afectados por la naturaleza GPLv3 del emulador.

Usos y prohibiciones

- **Usos admitidos:** Administración remota de servidores, desarrollo de software móvil, aprendizaje de línea de comandos Linux y automatización de tareas locales.
- **Usos prohibidos:** Queda prohibido el uso de la herramienta para realizar ataques informáticos no autorizados, interceptación de comunicaciones en redes ajenas o cualquier actividad que vulnere la Ley de Ciberseguridad o el Código Penal español.

Seguridad y certificaciones

- **Seguridad:** Termux utiliza un entorno aislado (sandbox) proporcionado por Android. No requiere privilegios de "root", lo que minimiza el riesgo de comprometer el sistema operativo completo.
- **Certificaciones:** No posee certificaciones ISO o SOC2 propias al ser un proyecto comunitario. Sin embargo, participa en programas como el "GitHub Secure Open Source Fund" para mejorar su cadena de suministro y generar SBOM (Software Bill of Materials).

Otros

- **IA y Scripts:** Si se integran modelos de IA (como mediante la instalación de paquetes de LLM locales), se debe considerar el cumplimiento de la **AI Act** respecto a la transparencia y la gestión de riesgos si el sistema se clasifica de alto riesgo.

Fuentes consultadas:

- [Licencia y código fuente](#)

- [Política de Seguridad y vulnerabilidades](#)
- [Certificación GitHub Secure Open Source Fund](#)
- [Documentación Wiki y FAQ legal](#)

**Para más información y herramientas:**

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

[Inicio](#) [Todas las herramientas](#) [Categorías](#)

Este documento ofrece recomendaciones generadas mediante análisis humano y sistemas de IA automatizados. La información tiene carácter meramente informativo y no constituye asesoramiento legal, profesional ni garantía de resultados. Las marcas, logotipos y nombres comerciales pertenecen a sus respectivos propietarios y se utilizan únicamente con fines identificativos.