GUÍA DE PRIVACIDAD

GrapheneOS

Los principios, sin tecnicismos

Qué es, cómo protege tu móvil y por qué es distinto de Android.

01

Qué es GrapheneOS

GrapheneOS es un sistema operativo para móviles centrado en la seguridad y la privacidad. Lo desarrolla un proyecto sin ánimo de lucro, de código abierto, que se financia con donaciones. Parte de Android, pero lo endurece y le quita lo que más filtra datos.

MÁS SEGURO

Defensas añadidas para que un fallo en una app no llegue a controlar el móvil.

MÁS PRIVADO

Sin servicios de Google por defecto y con permisos que puedes recortar.

CÓDIGO ABIERTO

Cualquiera puede revisar cómo está hecho y comprobar lo que promete.

02

Cuatro ideas previas

Con estas cuatro ideas se entiende todo lo demás.

1. **El sistema operativo.** Es el programa que controla el móvil: reparte la memoria, gestiona la pantalla y decide qué puede hacer cada aplicación. Si tiene un fallo, ninguna app puede protegerte del todo.
2. **Android.** Es el sistema que usan casi todos los móviles que no son iPhone. Su base es de código abierto, pero cada fabricante, y sobre todo Google, le añade servicios propios.
3. **Los permisos.** Cada aplicación pide acceso a cosas como la cámara, la ubicación o los contactos. Tú decides qué le das y qué no.
4. **El sandbox.** Es una caja de arena: cada app vive en su propio espacio y no puede ver el de las demás ni tocar el sistema.

03

El problema: un móvil confía demasiado

En un móvil normal conviven muchas aplicaciones y servicios con acceso a tus datos, y todo ese software tiene fallos. Un ataque suele aprovechar un error en una app o en un archivo recibido para salir de su caja y tomar el control.

> **La idea central.** GrapheneOS no promete que el móvil sea invulnerable. Intenta hacer que atacarlo sea mucho más difícil y que las aplicaciones sepan mucho menos de ti.

04

Los tres principios de GrapheneOS

DENTRO

Aislar

Cada app, cada perfil y cada pieza del sistema en su propia caja.

FUERA

Reducir

Apagar por defecto lo que no hace falta y puede ser una puerta de entrada.

TÚ

Controlar

Permisos más finos para decidir qué ve cada aplicación.

Aislar: cajas dentro de cajas

GrapheneOS refuerza el aislamiento de Android. Además, permite crear varios perfiles en un mismo móvil, cada uno con sus aplicaciones, sus datos y sus claves de cifrado. Puedes tener un perfil personal, otro para el trabajo y otro para una identidad que no quieres mezclar. Es como tener varios móviles dentro de uno.

Reducir: menos puertas abiertas

Cada función activada es una posible vía de ataque, así que el sistema apaga lo que no necesitas. El puerto USB, con el móvil bloqueado, solo carga la batería. Los radios como Bluetooth, NFC y UWB vienen desactivados de fábrica. Y se añaden defensas en la memoria, que es donde suelen aprovecharse los errores de programación: el procesador etiqueta los bloques de memoria y bloquea cualquier acceso con una etiqueta equivocada.

Controlar: permisos de verdad

Android ya deja decir que no a la cámara o a la ubicación. GrapheneOS va más lejos. Puedes quitar a una app el acceso a internet, impedirle leer los sensores, darle acceso solo a ciertos archivos o enseñarle una agenda con solo algunos contactos. Si una calculadora pide internet, puedes negárselo y seguirá funcionando.

> Los tres principios se refuerzan entre sí: aislar limita el daño, reducir da menos oportunidades al atacante y controlar te devuelve la decisión sobre tus datos.

05

Del botón de encendido a la pantalla

1. Al encender el móvil, un chip de seguridad comprueba que el sistema es el que tiene que ser. Si lo han manipulado, te avisa.
2. El sistema arranca y descifra los datos con una clave que depende de tu PIN o contraseña. Sin ella, el contenido es ilegible.
3. Cada aplicación se ejecuta en su propia caja, con solo los permisos que le hayas dado.
4. Si el móvil lleva un tiempo bloqueado, se reinicia solo: tras el reinicio, los datos vuelven a estar cifrados hasta que introduces la contraseña.
5. Las actualizaciones llegan con frecuencia, se descargan sin molestar y, si fallan, el sistema vuelve a la versión anterior.
6. Si alguien te obliga a desbloquear el móvil, un PIN de coacción puede borrar el dispositivo en lugar de abrirlo.

06

Las aplicaciones de siempre

GrapheneOS no incluye los servicios de Google, pero eso no te deja sin aplicaciones. Si necesitas algo que depende de Google, puedes instalar Google Play como una aplicación más.

EN UNA CAJA

Sandboxed Google Play

Google Play funciona sin privilegios especiales, dentro del aislamiento de un perfil.

NAVEGADOR

Vanadium

Un navegador basado en Chromium, endurecido, que es el motor web del sistema.

VERIFICACIÓN

Auditor

Comprueba desde otro móvil que el sistema no ha sido manipulado.

Por qué importa

Normalmente, los servicios de Google tienen permisos muy amplios sobre el sistema. Aquí, Google Play es solo una app y no tiene más poder que cualquier otra. Algunas apps bancarias o de pago exigen comprobaciones que solo cumplen los móviles certificados: conviene probarlas antes.

07

Cómo empezar

1. **Comprueba que tu móvil es compatible.** El soporte oficial es para modelos Pixel, desde el 6 hasta el 10a. Los Pixel 8 y posteriores reciben siete años de actualizaciones.
2. **Haz una copia de lo que quieras conservar.** La instalación borra el móvil por completo.
3. **Instala desde el navegador.** La web oficial te guía: conectas el móvil por cable a un ordenador con Chrome o Chromium y sigues los pasos.
4. **Configura un PIN largo** o una contraseña, activa el reinicio automático y deja el puerto USB en el modo por defecto.

REFERENCIA

Glosario rápido

TÉRMINO	SIGNIFICADO
Sistema operativo	El programa que controla el móvil y sus aplicaciones
Android	El sistema móvil más extendido, de base abierta
Sandbox	Caja aislada en la que vive cada aplicación
Permiso	Autorización para acceder a una función o a tus datos
Bootloader	Primer programa que arranca y carga el sistema
Arranque verificado	Comprobación de que el sistema no ha sido alterado
MTE	Etiquetas de memoria para bloquear accesos erróneos
Perfil	Espacio separado con sus apps, datos y claves
PIN de coacción	PIN especial que borra el móvil al introducirlo

> **Siguiente paso.** La guía completa, "GrapheneOS a fondo", explica cada pieza con más detalle: el arranque verificado, las defensas de memoria, los permisos, los perfiles, la instalación y la comparación con Android de serie y con iOS.

Fuentes: web de GrapheneOS (funciones, preguntas frecuentes e instalación) y Android Authority.