GUÍA DE PRIVACIDAD

GrapheneOS a fondo

Guía completa

Esta guía explica cómo funciona GrapheneOS, el sistema operativo para móviles centrado en la privacidad y la seguridad: qué endurece respecto a Android, qué protege de verdad y qué queda fuera de su alcance.

De Android endurecido a la seguridad del hardware

Contenido

INTRODUCCIÓN Y BASES

· Cómo usar esta guía 3

· Los conceptos básicos 3

CAPÍTULOS

01 Qué es GrapheneOS y qué problema resuelve 5

02 Dispositivos compatibles: por qué solo ciertos móviles 6

03 Arranque verificado y el chip de seguridad 7

04 El aislamiento de las aplicaciones: SELinux y seccomp 9

05 La memoria: hardened_malloc, MTE y endurecimiento del núcleo 10

06 Menos superficie de ataque: lo que está apagado por defecto 12

07 Permisos mejorados: Network, Sensors, Storage Scopes y Contact Scopes 14

08 Perfiles de usuario y espacios separados 15

09 Desbloqueo, reinicio automático y PIN de coacción 17

10 Google Play en una caja: Sandboxed Google Play 18

11 El navegador y las aplicaciones propias 19

12 Instalación: desde el navegador y con el bootloader bloqueado 20

13 Actualizaciones 22

14 Lo que GrapheneOS no protege 22

15 Comparación con Android de serie y con iOS 24

16 Buenas prácticas 25

17 Fuentes 25

INTRODUCCIÓN

Cómo usar esta guía

Público y prerrequisitos. No hace falta saber de sistemas operativos ni de seguridad informática. La sección "Antes de empezar" presenta los conceptos que se usan después: qué es un sistema operativo, qué es Android, cómo funcionan los permisos, qué es el cifrado del almacenamiento, qué significa "root" y qué es el bootloader. A partir de ahí la guía va subiendo de nivel poco a poco.

Estado del proyecto. GrapheneOS cambia con frecuencia: cada mes llegan versiones nuevas y la lista de dispositivos crece con el tiempo. Esta guía recoge la situación actual, con soporte oficial para varios modelos de Pixel y una alianza anunciada con Motorola para dispositivos futuros. Si un detalle puede haber cambiado, consulta la web oficial del proyecto.

Cómo leerla. Si partes de cero, empieza por "Antes de empezar". Los capítulos 1 a 3 explican la idea general, los dispositivos y el arranque. Los capítulos 4 a 9 describen las defensas técnicas del sistema. Los capítulos 10 a 13 tratan de las aplicaciones, la instalación y las actualizaciones. Los capítulos 14 a 16 explican los límites, la comparación con otros sistemas y las buenas prácticas.

ANTES DE EMPEZAR

Los conceptos básicos

Para entender qué aporta GrapheneOS hay que conocer seis ideas: qué hace un sistema operativo, qué es Android, cómo se aíslan las aplicaciones, cómo se cifra un móvil, qué es el acceso root y qué papel tiene el bootloader.

El sistema operativo

El **sistema operativo** es el programa que controla el móvil: reparte la memoria, gestiona la pantalla, la red y la cámara, y decide qué puede hacer cada aplicación. Todo lo demás se apoya en él. Si el sistema operativo tiene un fallo de seguridad, ninguna aplicación puede protegerte del todo, igual que una puerta blindada no sirve de mucho en una casa con las paredes de cartón.

Android y AOSP

Android es el sistema operativo de la mayoría de los móviles del mundo. Su base se publica como código abierto con el nombre de **AOSP** (Android Open Source Project). Cada fabricante parte de esa base y le añade lo suyo: aplicaciones, servicios y, en el caso de Google, los **servicios de Google Play** (la tienda, las notificaciones, la ubicación y muchas otras funciones que corren con privilegios altos). GrapheneOS parte también de AOSP, pero sin los servicios de Google, y lo endurece por dentro.

Aplicaciones y permisos

Cada aplicación de Android se ejecuta en un **sandbox** ("caja de arena"): un espacio propio, aislado de las demás, con sus propios archivos. Si quiere salir de esa caja para algo concreto, como leer tus contactos, usar la cámara o acceder a internet, tiene que pedir un **permiso**, y el sistema lo concede o lo niega. Los permisos son la forma en que decides qué sabe de ti cada aplicación.

El cifrado del almacenamiento

Todo lo que guarda un móvil moderno (fotos, mensajes, contraseñas) está **cifrado**: se convierte en un revoltijo ilegible que solo se deshace con una clave. La clave sale de tu PIN o contraseña combinada con un componente de hardware del propio teléfono. Hay un detalle importante: tras encender el móvil, los datos permanecen cifrados hasta que lo desbloqueas por primera vez. Después, aunque la pantalla se bloquee, parte de la clave sigue en memoria para que el teléfono funcione. Por eso un móvil apagado, o recién reiniciado y sin desbloquear, es mucho más difícil de atacar que uno que lleva días encendido.

Root

Root (o "superusuario") es un nivel de acceso que puede hacer cualquier cosa en el sistema, saltándose las reglas de aislamiento. Algunos usuarios rootean su móvil para personalizarlo, pero eso abre una puerta de par en par: cualquier aplicación o fallo que consiga ese nivel controla el teléfono entero. GrapheneOS no incluye root y lo desaconseja, porque debilita justo las barreras que el sistema quiere reforzar.

El bootloader

El **bootloader** es el primer programa que se ejecuta al encender el móvil. Su trabajo es cargar el sistema operativo. Un bootloader **bloqueado** solo arranca software firmado por una clave de confianza y comprueba que no ha sido modificado; uno **desbloqueado** arranca lo que sea, lo cual permite instalar otro sistema pero deja el móvil sin esa comprobación. Instalar GrapheneOS exige desbloquear el bootloader un momento, y al final se vuelve a bloquear, esta vez con la clave de GrapheneOS.

CAPÍTULO 1

Qué es GrapheneOS y qué problema resuelve

GrapheneOS es un sistema operativo móvil de código abierto, mantenido por un proyecto sin ánimo de lucro que se financia con donaciones. Nació en 2014 y se basa en AOSP. No es una aplicación ni un parche: sustituye el sistema operativo completo del teléfono por otro con las mismas aplicaciones de Android, pero con muchas defensas añadidas.

El objetivo es doble. Por un lado, la **seguridad**: que un fallo en una aplicación, un archivo malicioso o un atacante con el móvil en la mano lo tenga lo más difícil posible. Por otro, la **privacidad**: que el sistema no envíe datos a terceros por su cuenta y que tú controles qué ve cada aplicación.

El modelo de amenazas

Ninguna herramienta protege contra todo. Antes de decidir si GrapheneOS te sirve, conviene saber de qué defiende.

AMENAZA	QUÉ HACE GRAPHENEOS
Aplicación maliciosa o curiosa	Aísla más cada app y te deja recortar permisos que Android estándar no permite recortar (red, sensores, contactos, archivos)
Fallo de seguridad en el navegador o en un archivo recibido	Dificulta que el fallo se convierta en control del móvil con defensas de memoria y un sandbox más estricto
Móvil robado, perdido o confiscado	Reduce lo que se puede extraer con el móvil bloqueado: puerto USB cerrado, reinicio automático, contraseñas largas, PIN de coacción
Rastreo por servicios del sistema	No incluye servicios de Google y limita lo que envía el propio sistema
Atacantes con muchos recursos y exploits desconocidos	Eleva el coste del ataque, pero no puede garantizar inmunidad

La tabla deja ver el enfoque: GrapheneOS no promete invulnerabilidad, sino **subir el precio** de atacar el teléfono y **recortar lo que las aplicaciones saben de ti**. Lo que queda fuera (la red del operador, lo que tú mismo cuentas en una app, la manipulación de las personas) se trata en el capítulo 14.

CAPÍTULO 2

Dispositivos compatibles: por qué solo ciertos móviles

GrapheneOS no se instala en cualquier teléfono. El proyecto da soporte oficial únicamente a modelos concretos, porque su seguridad depende del hardware: un sistema operativo endurecido sobre un chip sin las protecciones adecuadas sería, en palabras del propio proyecto, imposible de hacer razonablemente seguro.

Soporte actual. El soporte oficial cubre 21 dispositivos, desde el Pixel 6 hasta el Pixel 10a, incluidos los Pixel 10, 10 Pro, 10 Pro XL y 10 Pro Fold. El proyecto recomienda los Pixel 8 y posteriores, que reciben al menos siete años de actualizaciones de seguridad desde su lanzamiento. Un ejemplo: el Pixel 10 y el 10 Pro tienen soporte garantizado por el fabricante hasta agosto de 2032.

Qué exige GrapheneOS al hardware

El proyecto publica los requisitos que debe cumplir un dispositivo para que valga la pena darle soporte. Los principales:

- **Memoria etiquetada** (MTE o equivalente) y protección del flujo de ejecución (BTI y PAC o equivalentes), que se explican en el capítulo 5.
- **Arranque verificado** con protección contra versiones antiguas, tanto del firmware como del sistema.
- **Almacén de claves en hardware** (StrongBox), atestación de claves y limitación de intentos de PIN mediante un chip seguro aparte.
- **Componentes aislados**: módem, GPU y otros no deben poder leer la memoria principal sin control.
- **Actualizaciones** de al menos cinco años (los Pixel actuales llegan a siete).
- **Puerto USB** con datos desactivables por hardware y sin acceso de depuración con el móvil bloqueado.

En la práctica, solo los Pixel cumplían todo esto cuando el proyecto se consolidó, y por eso hasta ahora han sido el único soporte oficial.

Más allá de Pixel: la alianza con Motorola

El proyecto lleva tiempo diciendo que ampliar el soporte a cualquier móvil iría contra sus objetivos, y que prefiere colaborar con fabricantes que construyan dispositivos que cumplan sus requisitos. Esa colaboración se concretó en marzo de 2026, cuando Motorola anunció una alianza a largo plazo con la fundación de GrapheneOS para "futuros dispositivos pensados para ser compatibles con GrapheneOS". Hasta donde se ha comunicado, no hay modelo confirmado ni fecha de lanzamiento. También se ha dicho que fabricantes que no cumplen los requisitos, como Fairphone, quedan descartados.

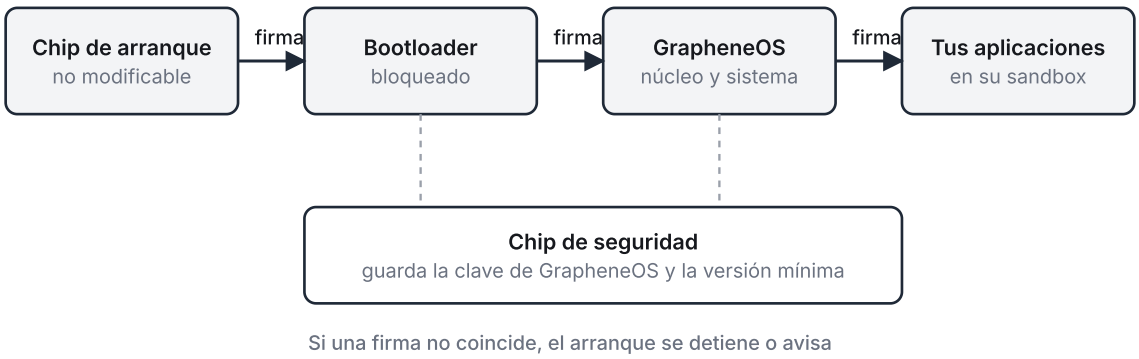
CAPÍTULO 3

Arranque verificado y el chip de seguridad

La primera línea de defensa ocurre antes de que el sistema arranque. El objetivo es asegurar que lo que se ejecuta en el móvil es exactamente lo que GrapheneOS publicó, sin una sola modificación.

La cadena de confianza

Piensa en una cadena de relevos. Cuando enciendes el móvil, un primer programa grabado en el chip, que no se puede modificar, comprueba la firma del siguiente. Ese comprueba el siguiente, y así hasta el sistema operativo. Si alguien ha alterado una pieza, la firma no coincide y el arranque se detiene o avisa. Esto se llama **arranque verificado** (*verified boot*).



Cada eslabón comprueba la firma del siguiente antes de cederle el control

Para que sirva, la comprobación final necesita una clave de confianza. Con el bootloader bloqueado, el Pixel acepta la clave de GrapheneOS, que se guarda en el **chip de seguridad** del teléfono (un procesador aparte, pensado para guardar secretos y resistir ataques físicos). Cada vez que se enciende, el móvil muestra en pantalla una huella de esa clave. Un aviso amarillo al arrancar significa "sistema verificado con una clave que no es la de fábrica", y es lo normal en GrapheneOS.

Protección contra versiones antiguas

Un atacante podría intentar instalar una versión antigua y vulnerable del sistema. Por eso el chip recuerda el número de versión más reciente y rechaza cualquier versión anterior (*rollback protection*). GrapheneOS extiende esa comprobación a las actualizaciones de componentes del sistema, que también se verifican al instalarlas y al arrancar.

El chip de seguridad y los intentos de PIN

El chip de seguridad hace otro trabajo clave: **limita los intentos de adivinar tu PIN**. La clave que cifra el móvil se deriva de tu PIN y de un secreto que vive dentro del chip. Si alguien extrae la memoria del teléfono e intenta probar millones de PIN por fuerza bruta, el cálculo necesita al chip, y el chip frena los intentos y los espacia cada vez más. Por eso una contraseña larga, que un atacante tendría que probar durante siglos aun sin freno, añade protección a una barrera que ya es difícil.

CAPÍTULO 4

El aislamiento de las aplicaciones: SELinux y seccomp

En Android cada aplicación vive en su propia caja. GrapheneOS refuerza esas cajas con dos mecanismos del núcleo del sistema.

SELinux: un reglamento para cada proceso

SELinux es un sistema de reglas obligatorias. Cada programa del móvil tiene una etiqueta, y un reglamento dice con precisión qué etiquetas pueden tocar qué recursos. Funciona como el control de acceso de un edificio con tarjetas: aunque consigas entrar en una planta, la tarjeta no te abre las demás. Lo importante es que estas reglas **no las puede cambiar el programa**, ni siquiera si consigue ejecutar código propio dentro de la aplicación. GrapheneOS endurece esas reglas respecto a las de Android estándar y las aplica también a sus propios componentes.

seccomp: una lista de llamadas permitidas

Cuando una aplicación necesita algo del sistema (abrir un archivo, crear una conexión), hace una *llamada al sistema*. **seccomp** es un filtro que le recorta ese menú: la aplicación solo puede usar las llamadas de una lista corta, y si intenta una que no está, el sistema la detiene. Así, un fallo en la aplicación tiene menos herramientas del núcleo a su alcance para escapar de su caja.

El navegador, la parte más expuesta

El navegador procesa contenido que viene de internet sin que nadie lo revise, por eso es el objetivo favorito de los atacantes. GrapheneOS mejora el aislamiento de los procesos que dibujan las páginas (el *renderer*), de forma que un fallo al interpretar una web quede encerrado y no llegue al resto del móvil. En el capítulo 11 se ve el navegador Vanadium.

CAPÍTULO 5

La memoria: hardened_malloc, MTE y endurecimiento del núcleo

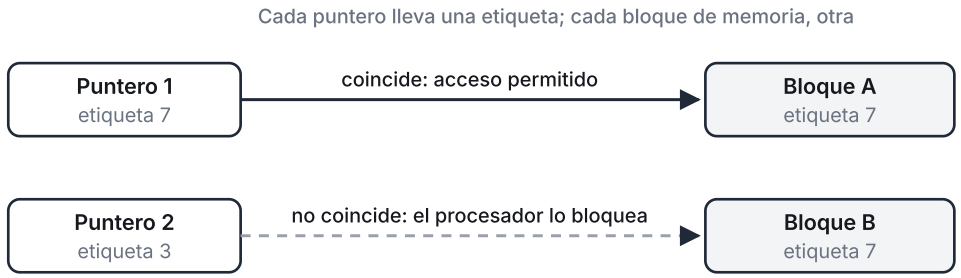
La mayoría de los ataques graves contra móviles aprovechan errores de **memoria**: un programa lee o escribe donde no debe y un atacante lo convierte en control. Son los fallos más comunes en el código escrito en C y C++, y GrapheneOS dedica mucho esfuerzo a hacerlos inofensivos.

hardened_malloc: un administrador de memoria desconfiado

Cuando un programa pide memoria, un componente llamado *asignador* se la reparte. El asignador de serie de Android es rápido, pero confiado. **hardened_malloc** es el asignador propio de GrapheneOS, diseñado para dificultar la explotación de errores: guarda sus datos de control lejos de los datos del programa, borra cada bloque al liberarlo, retrasa la reutilización de bloques liberados, deja huecos de guarda entre regiones y añade marcas aleatorias. Si un programa escribe más allá del límite, es mucho más probable que choque con una trampa y el sistema lo detenga que no que el atacante gane algo.

MTE: etiquetas de memoria

La **memoria etiquetada** (*Memory Tagging Extension*, MTE) es una función del procesador, disponible en los Pixel más modernos. Funciona como las llaves y cerraduras de colores: cada trozo de memoria recibe un color (una etiqueta) y cada puntero que apunta a él lleva el mismo color. Cuando el programa intenta acceder, el procesador compara los dos colores. Si no coinciden, ha ocurrido un error de memoria y el acceso se bloquea en el acto. GrapheneOS usa MTE en las asignaciones de hardened_malloc de hasta 128 KB, en los asignadores del núcleo y en el navegador Vanadium.



La etiqueta del puntero debe coincidir con la del bloque; si no, el acceso se bloquea

Fórmula clave. La protección de MTE se puede medir. Con una etiqueta de 4 bits hay 16 colores posibles:

$$P_{\text{detección}} = 1 - \frac{1}{2^4} = \frac{15}{16} \approx 93{,}75\,\%$$

> **En palabras:** de cada dieciséis accesos erróneos a memoria, el procesador detiene quince; solo uno pasa sin ser notado porque, por pura casualidad, el color erróneo coincide con el correcto.

Desglose de la fórmula:

- **4 bits de etiqueta.** Cada trozo de memoria lleva una etiqueta de 4 bits, es decir, un número entre 0 y 15. Cuatro bits son lo que cabe en los bits sin uso de un puntero de 64 bits.
- **2^4 = 16 colores.** Es el número de etiquetas distintas. Si el atacante no sabe cuál es la correcta, elige una al azar entre 16.
- **1/16.** Es la probabilidad de acertar el color por casualidad. Es la única vía por la que un error pasa desapercibido.
- **1 – 1/16 = 15/16.** El complemento: la probabilidad de que el error sea detectado.

Un ejemplo con números. Un atacante intenta leer un trozo de memoria que no es suyo. La memoria tiene el color 7 y el puntero del atacante lleva el 3. Los colores no coinciden y el procesador bloquea el acceso. Para pasar, el atacante necesitaría que el puntero llevara también el 7, algo que no controla porque las etiquetas se asignan al azar. Si lo intentara cien veces, lo probable es que el sistema lo detuviera en las primeras.

Por qué funciona: lo que decide el resultado no es qué hace el atacante, sino una coincidencia de colores que él no puede ver ni elegir. Además, cada fallo de etiqueta se registra, y en la práctica el programa se cierra al primer error, de modo que un atacante rara vez tiene la segunda oportunidad que necesitaría.

Endurecimiento del núcleo

El **núcleo** (*kernel*) es la parte central del sistema operativo, y quien lo controla controla el móvil. GrapheneOS le añade varias barreras:

- **Borrado de memoria liberada**: las páginas y los bloques que ya no se usan se rellenan de ceros, para que no queden restos.
- **Direcciones más impredecibles**: usa un espacio de direcciones de 48 bits con 33 bits de aleatoriedad (ASLR).
- **Módulos firmados**: solo se cargan módulos del núcleo firmados con una clave propia de cada compilación.
- **Modo lockdown**: en modo de confidencialidad forzada, ni siquiera el código con privilegios altos puede leer la memoria del núcleo.
- **Protecciones de hardware ARMv9**: BTI y PAC, que impiden saltar a mitad de una función o falsificar direcciones de retorno, y en el núcleo también CFI y ShadowCallStack.

Sobre la aleatoriedad de las direcciones, la cifra es esta:

> $$2^{33} \approx 8{,}6 \times 10^{9}$$

> **En palabras:** el sistema puede colocar los programas en unos ocho mil seiscientos millones de posiciones distintas, así que un atacante que no sabe dónde está cada pieza tiene que adivinar entre una cantidad enorme.

CAPÍTULO 6

Menos superficie de ataque: lo que está apagado por defecto

La idea más sencilla de seguridad es esta: lo que está apagado no se puede atacar. GrapheneOS reduce la **superficie de ataque** desactivando funciones peligrosas o recortándolas a lo imprescindible.

Compilación y código dinámico

Muchos ataques consisten en meter código nuevo dentro de un programa en marcha. GrapheneOS lo dificulta de dos formas. Sustituye la compilación al vuelo (*JIT*) del entorno de ejecución de Android por compilación previa, y bloquea la carga dinámica de código en casi todos los procesos del sistema. Para las aplicaciones que tú instales hay tres interruptores: carga dinámica de código desde memoria, desde almacenamiento, y JIT del WebView.

Radios apagadas

La conectividad NFC, Bluetooth y UWB viene desactivada por defecto. Las radios son una vía de entrada, y la mayor parte de la gente no usa todas a la vez. Además, el análisis de Wi-Fi y de Bluetooth para calcular la ubicación está desactivado de serie.

El puerto USB-C

El puerto de carga es también un puerto de datos, y es una vía clásica para extraer información de un móvil bloqueado. GrapheneOS ofrece cinco modos:

MODO	QUÉ HACE
Desactivado	No hay datos ni carga
Solo carga	Nunca acepta datos
Solo carga con el móvil bloqueado	Con el móvil bloqueado solo carga
Solo carga con el móvil bloqueado, salvo antes del primer desbloqueo	Variante intermedia
Activado	Funciona como siempre

El valor por defecto es **solo carga con el móvil bloqueado**: en cuanto se bloquea la pantalla, el sistema corta las conexiones de datos nuevas tanto en el hardware como en el núcleo, y desactiva los modos alternativos del puerto, como la salida de vídeo. Es una protección más fuerte que el interruptor estándar de Android.

Depuración y rastros

La depuración de código nativo (*ptrace*) está bloqueada para las aplicaciones del sistema y se puede bloquear para las tuyas. Las capturas de pantalla quitan los datos de versión y hora que otros sistemas dejan dentro de la imagen.

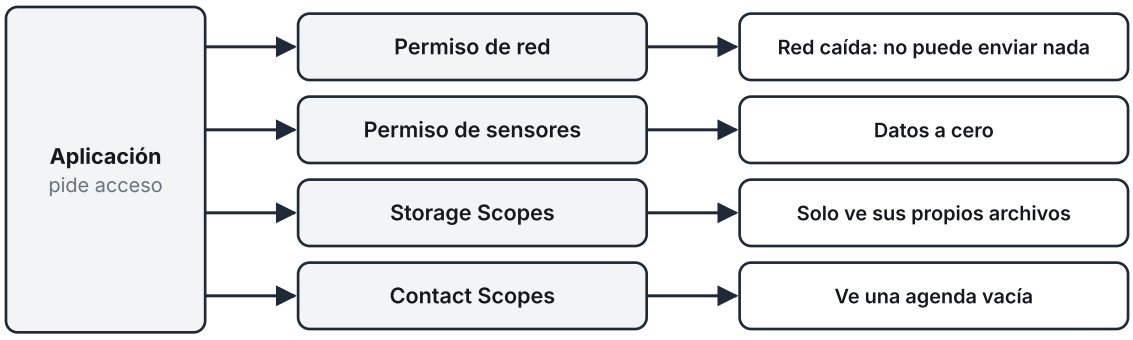
CAPÍTULO 7

Permisos mejorados: Network, Sensors, Storage Scopes y Contact Scopes

Android estándar deja a cada aplicación pedir cosas y solo te deja negar algunas. GrapheneOS añade permisos nuevos para recortar lo que Android da por hecho.

Permiso de red

Android concede por defecto el acceso a internet a toda aplicación que lo declare, y no te deja quitárselo. En GrapheneOS existe un **permiso de red** que se puede quitar, incluso al instalar. Si se lo quitas a una app, la red le aparece caída, de modo que no muestra errores de permiso revocado ni se bloquea. Una aplicación de notas, de linterna o de calculadora no necesita red, y sin ella no puede enviar datos a nadie.



Los permisos añadidos por GrapheneOS recortan lo que Android da por hecho

Permiso de sensores

El acelerómetro, el giroscopio o el barómetro no piden permiso en Android, y se usan para identificarte o para espiar lo que escribes. En GrapheneOS un permiso de **sensores** los bloquea y la app recibe datos a cero. Puedes dejarlo bloqueado por defecto para las aplicaciones que instales.

Storage Scopes: archivos a medida

Normalmente, una app que pide acceso a "archivos" ve toda la memoria del móvil. Con los **Storage Scopes**, la aplicación cree que tiene el permiso pero solo ve los archivos que ella misma ha creado y los que tú añadas a mano. Es como prestar un cajón a un amigo en lugar de darle la llave de la casa.

Contact Scopes: una agenda con filtro

Con los **Contact Scopes**, una aplicación que pide los contactos recibe una agenda que parece vacía, salvo los contactos o grupos que tú elijas compartir. Bloquea además todas las escrituras en la agenda. Muchas apps piden la agenda completa solo para sugerir amigos o subirla a sus servidores, y así esa subida se queda sin nada.

Portapapeles seguro

La función **Secure Paste** impide que una aplicación lea lo que otra ha copiado, con interruptores por aplicación y globales. Evita que una app de fondo vea una contraseña que acabas de copiar.

CAPÍTULO 8

Perfiles de usuario y espacios separados

Un mismo móvil puede tener varias identidades digitales separadas, y GrapheneOS lo lleva más lejos que Android estándar.

Perfiles

Un **perfil** es como un móvil dentro del móvil: tiene sus propias aplicaciones, sus propios datos, su propio cifrado y, si quieres, su propia configuración de VPN. Lo que hay en un perfil no se ve desde otro. GrapheneOS permite hasta 32 perfiles (31 más uno de invitado), frente a los 4 de Android estándar. Algunos usos típicos:



Cada perfil es un espacio aislado, con sus aplicaciones y sus claves

- Un perfil personal y otro para el trabajo.
- Un perfil donde se instala Google Play, para las pocas apps que lo necesitan, y otro limpio para todo lo demás.
- Un perfil para una identidad distinta, por ejemplo una cuenta de redes sociales que no quieres enlazar con tu nombre.

Cuando terminas de usar un perfil puedes pulsar **Terminar sesión**: el sistema lo cierra y borra sus claves de la memoria y del hardware, de modo que sus datos quedan cifrados otra vez. También puedes impedir que se instalen aplicaciones en los perfiles secundarios.

Por qué separar sirve

Las aplicaciones pueden inferir el modelo de móvil y detectar GrapheneOS, y también pueden reconocer un perfil concreto. Si quieres que dos identidades no se enlacen entre sí, ponerlas en perfiles diferentes es la forma más fiable. Un *Espacio privado* de Android, que oculta apps tras un segundo bloqueo, se puede usar con el mismo fin de organización, pero los perfiles de usuario separan más: tienen claves de cifrado propias.

CAPÍTULO 9

Desbloqueo, reinicio automático y PIN de coacción

El móvil bloqueado es la primera barrera si te lo roban o te lo confiscan. Estas funciones la refuerzan.

Contraseñas más largas y huella con segundo factor

Android estándar limita la contraseña a 16 caracteres. GrapheneOS permite hasta **128**. El desbloqueo con huella está limitado a cinco intentos en total, y se puede activar un segundo factor: tras reconocer la huella, el sistema pide también el PIN. Si lo prefieres, puedes desactivar la huella para desbloquear y usarla solo para confirmar acciones dentro de aplicaciones.

La fuerza de una contraseña depende de cuántas combinaciones hay:

$$N = c^{L}$$

En palabras: el número de contraseñas posibles crece de forma explosiva con la longitud: cada carácter extra multiplica por el número de caracteres disponibles.

Con un PIN de 6 dígitos hay 10^{6} = un millón de combinaciones. Con una contraseña de 12 caracteres elegidos entre unas 60 opciones hay unos 2×10^{21} combinaciones. La diferencia entre una y otra es de quince órdenes de magnitud.

Teclado desordenado

El **PIN scrambling** cambia de sitio los números del teclado cada vez que lo abres. Sirve contra quien mira de reojo y contra las marcas de dedos en la pantalla, que delatarían qué teclas pulsas. Funciona en la pantalla de bloqueo y en el PIN de la tarjeta SIM.

Reinicio automático

Como se explicó en los conceptos básicos, un móvil recién reiniciado está mucho mejor protegido que uno que lleva días encendido. El **reinicio automático** reinicia el móvil si lleva bloqueado un tiempo sin que nadie lo desbloquee: por defecto 18 horas, configurable entre 10

minutos y 72 horas. Desbloquear cualquier perfil reinicia la cuenta. El mecanismo vive en el arranque del sistema, así que un fallo del sistema no lo puede esquivar.

PIN de coacción

GrapheneOS tiene un **PIN y contraseña de coacción** (*duress*). Si alguien te obliga a desbloquear el móvil y escribes esa credencial, el sistema borra el dispositivo y las eSIM de forma irreversible, sin reiniciar. Necesita configurar tanto el PIN como la contraseña, y se activa en los ajustes de seguridad del perfil Propietario. Si la credencial de coacción coincidiera con la real, prevalece la real. Hay que usarlo con cuidado: no es un modo de "fingir" que desbloqueas, sino un borrado definitivo.

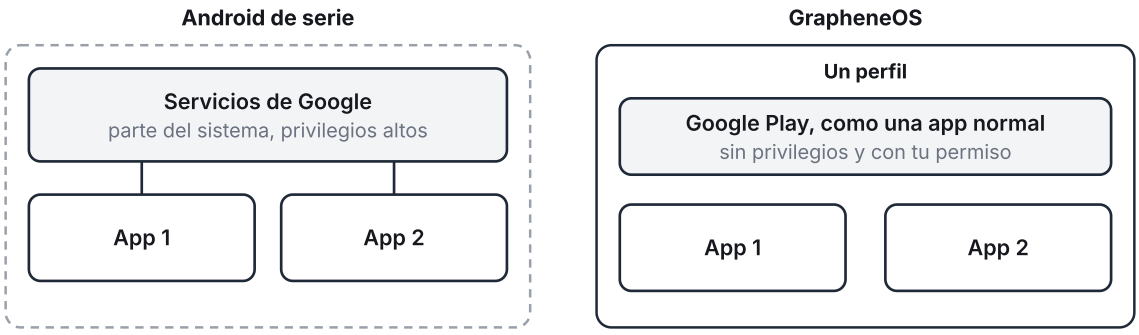
CAPÍTULO 10

Google Play en una caja: Sandboxed Google Play

Muchas aplicaciones, desde bancos hasta mapas, esperan encontrar los servicios de Google Play. GrapheneOS no los incluye, pero ofrece una forma de usarlos sin renunciar al aislamiento.

Una app como las demás

Con **Sandboxed Google Play** los servicios de Google se instalan como una aplicación normal, **sin privilegios especiales**, dentro del sandbox de un perfil. Una capa de compatibilidad hace que las aplicaciones crean estar en un Android con Google. En un Android estándar esos servicios son parte del sistema y pueden ver casi todo; aquí, en cambio, necesitan tu permiso como cualquier app, y solo pueden usarlos las aplicaciones del perfil donde están instalados.



En GrapheneOS, Google queda dentro de una caja y solo la usan las apps de ese perfil

Google Play como app sin privilegios, dentro del sandbox de un perfil

Qué funciona y qué se reencamina

La tienda, las compras dentro de las apps y la descarga de recursos funcionan. Las peticiones de ubicación van, por defecto, a una implementación propia de GrapheneOS, no a Google; puedes cambiarlo si prefieres el servicio de Google. Android Auto también funciona con privilegios reducidos. Para instalar aplicaciones desde la tienda hace falta una cuenta de Google.

Compromisos

Una aplicación que se niega a funcionar sin ciertas comprobaciones de Google puede fallar en GrapheneOS, porque el sistema no pasa las verificaciones de integridad que Google reserva a los fabricantes certificados. Algunas aplicaciones bancarias y de pago funcionan; otras no. Conviene comprobarlo antes de depender de una.

CAPÍTULO 11

El navegador y las aplicaciones propias

GrapheneOS trae un conjunto mínimo de aplicaciones propias, pensadas para reducir lo que se envía hacia fuera.

Vanadium, el navegador

Vanadium es una versión endurecida de Chromium, y es también el motor que usan las demás aplicaciones para mostrar páginas web. Entre sus protecciones: memoria etiquetada, aislamiento estricto de cada sitio, JIT de JavaScript desactivado por defecto (con un interruptor por sitio), cookies de terceros desactivadas, WebGPU desactivado y listas de bloqueo de anuncios y rastreadores. No admite extensiones, y el proyecto aconseja no añadirlas porque aumentan la superficie de ataque y la huella digital.

Otras aplicaciones

- **Cámara y visor de PDF**: aplicaciones propias, aisladas y endurecidas.
- **Auditor**: comprueba, con ayuda de otro móvil, que el sistema y el firmware son los originales, mediante atestación de hardware.
- **Seedvault**: copias de seguridad cifradas.
- **Tienda de aplicaciones propia**, con un espejo de Google Play.

Red y servicios

Los servidores de GrapheneOS se usan para comprobar la conexión, la hora de red y las actualizaciones del navegador. Sus registros se borran a los pocos días. El cifrado de DNS protege las consultas, pero no oculta qué sitios visitas, porque el nombre del servidor viaja aún en claro dentro de la conexión. Para esconder tu IP hace falta una VPN o Tor.

CAPÍTULO 12

Instalación: desde el navegador y con el bootloader bloqueado

Instalar GrapheneOS es un proceso guiado que se hace desde un ordenador, y borra todo el contenido del móvil, así que hay que copiar antes lo que quieras conservar.

Qué necesitas

- Un móvil con soporte oficial, de preferencia no vendido por un operador: las versiones de operador pueden tener el bootloader bloqueado de forma que no se pueda abrir.

- Un ordenador con Windows, macOS, Linux o ChromeOS, un cable USB-C de calidad y conectado directamente al ordenador, sin concentradores.
- Un navegador compatible, como Chromium, Chrome, Edge, Vanadium o Brave con sus protecciones desactivadas. Evita la navegación privada y las versiones empaquetadas como Snap o Flatpak.

El proceso, paso a paso

El instalador web usa **WebUSB**, una tecnología que permite a una página hablar con el móvil por cable desde el propio navegador, sin programas que instalar.

1. **Activar el desbloqueo OEM** en las opciones de desarrollador del móvil.
2. **Entrar en el modo fastboot**: apagar el móvil y encenderlo mientras se mantiene pulsado el botón de bajar volumen.
3. **Desbloquear el bootloader** desde la página y confirmarlo en el móvil. Esto borra todos los datos.
4. **Descargar y grabar** la versión de GrapheneOS. El instalador graba el firmware y el sistema automáticamente; mientras tanto no hay que tocar el móvil.
5. **Volver a bloquear el bootloader** y confirmarlo. Esto borra los datos otra vez y activa el arranque verificado completo con la clave de GrapheneOS.
6. **Primer arranque**: el desbloqueo OEM queda desactivado por defecto. Debe seguir así.

Verificar la instalación

En cada arranque, el móvil muestra una huella de la clave con que se ha verificado el sistema. En los Pixel 6 y posteriores aparece completa y puedes compararla con las huellas oficiales publicadas. Para una comprobación más fuerte, la aplicación **Auditor** usa la atestación de hardware, y necesita un segundo dispositivo Android o un servicio de seguimiento opcional.

Si quisieras volver al sistema original, existe una herramienta de grabado de Google: primero se desbloquea el bootloader, se borra la clave de GrapheneOS y se instala el sistema de fábrica.

CAPÍTULO 13

Actualizaciones

La mayor parte de los fallos de seguridad se arreglan con parches, así que lo que protege de verdad es **recibirlos a tiempo**.

Cómo se actualiza

El actualizador de GrapheneOS busca versiones nuevas cada pocas horas, las descarga en segundo plano y las instala en una copia secundaria del sistema. Para activarlas basta un reinicio. Si el primer arranque tras la actualización falla, el sistema vuelve solo a la versión anterior. Las actualizaciones están firmadas, no se pueden degradar a versiones antiguas y el servidor se trata como no fiable. Se pueden elegir las redes permitidas, el nivel mínimo de batería y si debe estar cargando.

Parches de Android y del núcleo

GrapheneOS incorpora los parches mensuales de Android y las versiones recientes del núcleo Linux de soporte largo, y suele ir por delante del sistema de fábrica. Además, el proyecto comunica fallos a Google y detecta parches que se han quedado sin aplicar.

Cuánto dura el soporte

El soporte del fabricante marca la vida útil del teléfono: cinco años en los móviles antiguos y siete en los Pixel 8 y posteriores. Un móvil sin parches no es seguro, por buen sistema que lleve.

CAPÍTULO 14

Lo que GrapheneOS no protege

Este capítulo es tan importante como los anteriores: sirve para no esperar de GrapheneOS lo que

no puede dar.

LÍMITE	POR QUÉ
Rastreo del operador móvil	La red te localiza por las antenas. Solo el modo avión corta las radios por completo
Hardware cerrado	El módem y parte del firmware son de los fabricantes. GrapheneOS los aísla, pero no puede revisarlos
Identidad de la instalación	Las apps pueden detectar GrapheneOS, el modelo y el perfil. Para identidades distintas hacen falta perfiles distintos
Aplicaciones que te rastrean	Si usas una red social, ella sabe lo que haces en ella. El sistema solo limita qué más ve
DNS cifrado y sitios visitados	El DNS cifrado no oculta los sitios visitados; para ocultar tu IP hace falta VPN o Tor
Aplicaciones que intervienen el tráfico	Los bloqueadores que exigen instalar un certificado propio debilitan el cifrado de las páginas
Robo del móvil	No incluye la protección contra restablecimiento de fábrica de Google
Manipulación de las personas	Un engaño que te convence de dar una contraseña o instalar algo no lo detiene ninguna defensa técnica

La manipulación, los engaños por mensaje y el phishing explican la mayor parte de los robos de cuentas, y ningún sistema operativo los evita por completo.

CAPÍTULO 15

Comparación con Android de serie y con iOS

Cada sistema tiene un enfoque distinto y conviene verlo sin partidismo.

ASPECTO	ANDROID DE SERIE (PIXEL)	GRAPHENEOS	IOS
Código	Parte abierto, parte cerrado	Abierto	Cerrado
Servicios de Google	Integrados con privilegios altos	No incluidos; opcionales en una caja	No aplica
Control de permisos	Los estándar de Android	Los estándar más red, sensores, archivos y contactos	Permisos propios del sistema
Defensas de memoria	Las de Android	Más fuertes: hardened_malloc, MTE en más componentes	Las del fabricante
Compatibilidad de apps	Máxima	Alta, con excepciones en apps que exigen certificación de Google	Máxima en su ecosistema
Hardware	De Google	Pixel, con Motorola anunciado	Del fabricante, integrado

Cada fila tiene sus matices. iOS es un sistema muy cuidado, pero cerrado: no se puede revisar por dentro de forma independiente. Android de serie tiene la mayor compatibilidad, con más servicios de terceros integrados. GrapheneOS apuesta por el control del usuario y por el endurecimiento, a cambio de una lista corta de móviles y de algunas aplicaciones que no funcionan.

CAPÍTULO 16

Buenas prácticas

El mejor sistema se debilita si se usa mal. Estas costumbres sacan el máximo partido a GrapheneOS.

1. **Usa una contraseña larga**, no solo un PIN de seis dígitos, y activa el teclado desordenado.
2. **Deja el reinicio automático activado** y cámbialo a un tiempo corto si te preocupa un robo o una confiscación.
3. **Mantén el puerto USB-C en el modo por defecto** (solo carga con el móvil bloqueado), o en uno más estricto.
4. **Reduce permisos**: quita la red a las apps que no la necesiten, usa Contact Scopes y Storage Scopes, y bloquea sensores por defecto.
5. **Separa con perfiles**: un perfil para Google Play y otro limpio, y un perfil distinto para cada identidad que no quieras enlazar.
6. **Instala pocas apps**, de fuentes fiables, y desinstala las que no uses.
7. **Actualiza siempre** y no desactives el actualizador.
8. **Usa Vanadium** y no añadas extensiones ni navegadores con otros motores.
9. **Combina con una VPN o Tor** si necesitas ocultar tu IP: el sistema protege el móvil, no tu conexión.
10. **Apaga las radios** que no uses y activa el modo avión cuando no quieras ser localizado.

CAPÍTULO 17

Fuentes

- GrapheneOS: funciones, preguntas frecuentes y dispositivos, instalación web y guía de uso.
- Alianza con Motorola (marzo de 2026): Android Authority.
- Colaboración con un fabricante y requisitos de dispositivos: PiunikaWeb.