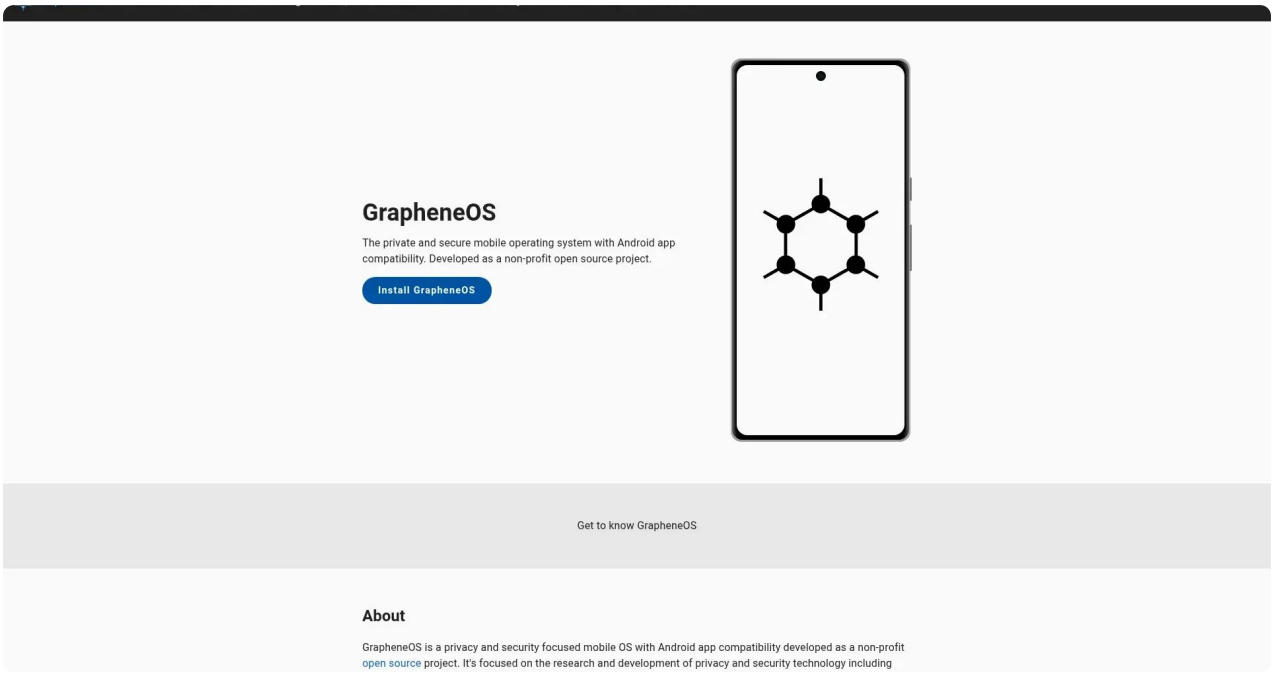

GrapheneOS

Sistema operativo móvil de código abierto basado en Android (AOSP) diseñado para profesionales, empresas y organizaciones que requieren seguridad extrema y privacidad absoluta. Es la herramienta ideal para perfiles que manejan información sensible, permitiendo un aislamiento total de aplicaciones mediante sandboxing avanzado, endurecimiento del kernel y eliminación de telemetría, todo ello manteniendo la compatibilidad con apps modernas en un entorno de confianza cero.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
GrapheneOS es un sistema operativo móvil de código abierto basado en Android (AOSP), enfocado exclusivamente en la privacidad y la seguridad extrema. Está diseñado para profesionales, empresas y organizaciones que manejan información sensible y requieren un nivel de protección superior al que ofrecen los sistemas comerciales estándar. Es la opción de referencia para perfiles con una mentalidad de "confianza cero" y sectores donde la interceptación de datos o el espionaje corporativo son riesgos reales.

Principal ventaja profesional
La reducción drástica de la superficie de ataque mediante el endurecimiento del kernel y un sandboxing (aislamiento) avanzado. A diferencia de otros sistemas, permite ejecutar aplicaciones de Google de forma totalmente aislada dentro de un sandbox de usuario, impidiendo que accedan a datos del sistema o rastreen la actividad del dispositivo sin permisos explícitos.

Para quién no es
No es adecuado para usuarios que buscan una experiencia de consumo convencional "llave en mano", ni para entornos corporativos que dependan de herramientas de gestión de dispositivos (MDM) incompatibles con sistemas operativos personalizados. Profesionales que no estén dispuestos a sacrificar ciertas comodidades automáticas por seguridad o que no posean un dispositivo compatible (Google Pixel) lo infravalorarán.

Funcionalidades clave
- **Sandboxed Google Play:** Permite instalar servicios de Google como apps normales, sin privilegios especiales de sistema, manteniendo el aislamiento total.
- **Hardened Malloc:** Un asignador de memoria propio diseñado para detectar y prevenir de forma proactiva ataques de corrupción de memoria y exploits de día cero.
- **Control de sensores y red:** Toggles específicos para revocar el acceso a sensores (acelerómetro, giroscopio) y permisos de red a nivel de aplicación.
- **Verificación de hardware (Auditor):** Capacidad de realizar una atestación local y remota para asegurar que el hardware y el software no han sido manipulados.
- **Protección de puertos USB:** Configuración para deshabilitar la transmisión de datos por el puerto USB-C cuando el dispositivo está bloqueado.
- **PIN Scrambling:** Reordenación aleatoria de los números en la pantalla de desbloqueo para evitar el rastreo visual o por huellas térmicas.

Precios
- **Versión gratuita:** Open Source y totalmente gratuita. El proyecto se mantiene mediante donaciones y no comercializa datos de usuario.
- **Coste de hardware:** Requiere la compra de un dispositivo compatible (Google Pixel), ya que es el único hardware con el soporte necesario para el arranque verificado (Verified Boot) con claves personalizadas.

Perfil del usuario
- Empresas que requieren asegurar las comunicaciones de sus directivos y personal clave.
- Periodistas de investigación y profesionales del derecho que manejan fuentes confidenciales.
- Administradores de sistemas y expertos en ciberseguridad.
- Departamentos gubernamentales y ONGs en entornos de alto riesgo.

Nivel técnico requerido
- **Para su uso:** Bajo-Medio. La experiencia de usuario es muy similar a un Android limpio, aunque requiere familiarizarse con la gestión avanzada de permisos.
- **Para su configuración:** Medio-Alto. La instalación inicial se realiza preferiblemente mediante un instalador web basado en WebUSB, pero requiere conocimientos básicos sobre desbloqueo de bootloader.
- **Soporte:** No existe soporte técnico oficial de pago; la resolución de incidencias depende de la documentación oficial y la comunidad.
- **Tecnologías:** Conocimientos básicos en seguridad móvil y gestión de claves de cifrado.

Ejemplos de uso profesional
- **Gestión de activos críticos:** Uso del dispositivo como token de autenticación física y gestión de contraseñas en un entorno aislado.

- **Comunicaciones seguras:** Implementación de dispositivos con GrapheneOS para llamadas cifradas punto a punto sin telemetría de fondo hacia fabricantes.
- **Aislamiento de aplicaciones corporativas:** Ejecución de suites de trabajo (Slack, Teams) en perfiles de usuario separados que no pueden interactuar con la información personal del dispositivo.

Uso y distribución
- **Instalador Web:** Herramienta oficial basada en navegador para la instalación simplificada.
- **OTA (Over-the-Air):** Actualizaciones automáticas de seguridad enviadas directamente por el proyecto.
- **CLI:** Herramientas de línea de comandos disponibles para usuarios avanzados y automatización de despliegues.

Open source
El proyecto es íntegramente de código abierto bajo licencia MIT, alojado en GitHub, lo que permite auditorías independientes de todo el sistema.

Integraciones
- **MCP:** Dispone de un servidor de atestación para verificar la integridad del dispositivo desde otros sistemas.
- **Sandboxed Play Services:** Integración nativa que permite que casi cualquier app de la Play Store funcione sin comprometer la seguridad del sistema base.
- **Seedvault:** Integración nativa para copias de seguridad cifradas en la nube personal o almacenamiento local (Nextcloud, USB).

Notas finales
Información legal, licencias y contratos
GrapheneOS se distribuye bajo la licencia MIT. Al ser un proyecto sin ánimo de lucro, no ofrece contratos de servicio (SLA) ni garantías comerciales. El usuario asume la responsabilidad de la instalación, la cual invalida técnicamente la garantía del software original del fabricante, aunque suele ser reversible.

Otros
Es fundamental destacar que GrapheneOS solo es compatible con dispositivos Google Pixel (desde el modelo 6 en adelante para soporte completo) debido a los requisitos específicos de seguridad de hardware (chip Titan M2) que otros fabricantes no permiten documentar o liberar.

Para más información:
- Sitio web oficial: https://grapheneos.org
- Guía de instalación: https://grapheneos.org/install
- Repositorio GitHub: https://github.com/GrapheneOS
- Documentación de características: https://grapheneos.org/features
- Licencia: https://grapheneos.org/LICENSE.txt

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
GrapheneOS está dirigido a empresas y profesionales que operan bajo modelos de amenaza elevados, como despachos jurídicos, periodismo de investigación, servicios de inteligencia y departamentos de ciberseguridad. Es ideal para organizaciones que aplican políticas de Zero Trust y necesitan eliminar la telemetría invasiva de los servicios móviles comerciales. Presupuestariamente, el coste se limita a la adquisición de hardware específico (Google Pixel modelos 6 a 9), ya que el software es gratuito. Los puntos clave son el aislamiento de procesos mediante sandboxing reforzado y la integridad del hardware verificada mediante atestación remota.

Madurez digital requerida
- **Usuarios y equipo:** Nivel medio. El uso diario es idéntico a Android, pero los usuarios deben comprender la gestión estricta de permisos y la ausencia de servicios en la nube preconfigurados por defecto.
- **Empresa y departamentos:** Nivel alto. Se requiere un departamento de IT capaz de gestionar dispositivos sin las herramientas de administración propietarias de Google (MDM estándar) y con capacidad para dar soporte interno sobre privacidad y seguridad.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Tiempos estimados de despliegue:** De 1 a 2 días para la configuración del protocolo inicial y aproximadamente 30 minutos por dispositivo individual.
- **Evaluación inicial:** Auditoría de las aplicaciones críticas necesarias para el flujo de trabajo y verificación de su funcionamiento en el entorno Sandboxed Google Play.
- **Prueba de concepto:** Despliegue en 2-3 dispositivos para verificar la compatibilidad con redes corporativas (VPN, certificados) y herramientas de comunicación interna.
- **Configuración y personalización:** Establecimiento de políticas de PIN Scrambling, restricciones de puertos USB y configuración de Seedvault para copias de seguridad cifradas.
- **Formación y adaptación:** Sesiones cortas para explicar el uso de perfiles de usuario separados (trabajo vs. personal) y el manejo de los interruptores de privacidad de hardware (sensores).
- **Seguimiento:** Revisión periódica de los registros de atestación mediante la aplicación Auditor para asegurar que la integridad del sistema no ha sido comprometida.

Necesidades de formación del equipo
El equipo necesita comprender el concepto de Sandboxed Google Play para no otorgar permisos innecesarios por hábito. Es vital formar en la gestión de copias de seguridad manuales o mediante Nextcloud/Seedvault, ya que no existe la sincronización automática nativa de Google Photos o Drive.

Perfiles necesarios
- **Perfiles técnicos:** Administradores de sistemas con conocimientos en seguridad móvil, gestión de bootloaders e infraestructura de clave pública (PKI) para la atestación.
- **Personal externo:** Consultores de ciberseguridad para la auditoría de riesgos inicial y la definición de políticas de endurecimiento.

Retorno de la inversión
- **Tiempos:** El ahorro se manifiesta en la reducción del riesgo de filtraciones de datos y espionaje industrial, cuya mitigación de daños suele ser extremadamente costosa.
- **KPIs:** Número de intentos de acceso bloqueados por el Hardened Malloc, reducción de la telemetría saliente del dispositivo (medible mediante DNS/Firewall) y tiempo de inactividad por exploits de día cero prevenidos por el sistema.

Otros
Es crucial considerar que la elección del hardware Google Pixel no es por preferencia de marca, sino por ser el único que permite el arranque verificado con claves de terceros y posee un enclave de seguridad (Titan M2) compatible con los estándares de GrapheneOS. El soporte de actualizaciones depende de la ventana de soporte oficial de Google para cada modelo.

PREGUNTAS FRECUENTES

¿Qué es GrapheneOS y en qué se diferencia de un Android convencional?

Es un sistema operativo móvil de código abierto basado en el Android Open Source Project (AOSP), pero reconstruido con un enfoque exclusivo en la seguridad proactiva y la privacidad. A diferencia del Android comercial, elimina la integración obligatoria de servicios de Google y la telemetría del fabricante, reforzando el kernel y el aislamiento de aplicaciones para minimizar cualquier vector de ataque.

¿Para qué perfiles profesionales está diseñado?

Está orientado a profesionales que gestionan información crítica, como periodistas de investigación, expertos en ciberseguridad, personal jurídico, directivos con riesgo de espionaje corporativo y administradores de sistemas en entornos de 'confianza cero'. Es ideal para cualquiera que necesite un dispositivo móvil con una superficie de ataque reducida al mínimo.

¿Cuánto cuesta y qué costes asociados tiene su implantación?

El sistema operativo es totalmente gratuito y no tiene costes de licencia por usuario. El principal coste profesional es la adquisición de hardware específico, concretamente dispositivos Google Pixel (preferiblemente de la serie 6 en adelante), que son los únicos con los requisitos de seguridad de hardware necesarios para su funcionamiento.

¿Es open source y se puede auditar su código?

Sí, es un proyecto íntegramente de código abierto distribuido bajo la licencia MIT. Todo su código fuente es público y está disponible en repositorios oficiales como GitHub, lo que permite a las organizaciones realizar auditorías de seguridad independientes para verificar la ausencia de puertas traseras.

¿Cómo garantiza la privacidad respecto a los servicios de Google?

GrapheneOS no incluye los servicios de Google de forma nativa. Sin embargo, permite instalarlos mediante un sistema de 'Sandboxed Google Play'. Esto significa que las herramientas de Google se ejecutan como aplicaciones normales sin privilegios especiales, impidiendo que recojan datos del sistema o rastreen la actividad del usuario de forma oculta.

¿Cumple con las normativas de seguridad y privacidad europeas?

Debido a su arquitectura técnica que prioriza la soberanía del dato y la ausencia de telemetría no deseada, es una herramienta excelente para cumplir con el RGPD en entornos de alta sensibilidad. No obstante, al ser un proyecto comunitario sin una entidad comercial detrás, no ofrece certificaciones legales específicas ni acuerdos de nivel de servicio (SLA) para empresas.

¿Es una tecnología segura contra ataques de día cero?

Sí, implementa medidas avanzadas como 'Hardened Malloc' (un asignador de memoria diseñado para detectar corrupciones de memoria) y un endurecimiento integral del kernel. Estas protecciones dificultan significativamente la ejecución de exploits de día cero en comparación con otros sistemas operativos móviles comerciales.

¿Se puede gestionar mediante herramientas MDM corporativas?

Este es uno de sus puntos críticos: no es compatible con la mayoría de las soluciones comerciales de Mobile Device Management (MDM) de terceros. Aunque permite la gestión de perfiles de usuario y políticas de red, las organizaciones que dependan de un control centralizado estricto mediante software comercial podrían encontrar limitaciones técnicas durante su despliegue.

¿Cómo se gestionan las actualizaciones de seguridad?

El sistema recibe actualizaciones automáticas Over-the-Air (OTA) enviadas directamente por el proyecto. Estas actualizaciones suelen ser extremadamente rápidas, a menudo publicándose el mismo día en que se lanzan los parches de seguridad de Android, garantizando que el dispositivo esté protegido contra las vulnerabilidades más recientes.

¿Requiere conocimientos técnicos avanzados para su uso diario?

Para el usuario final, la interfaz es prácticamente idéntica a la de un dispositivo Android estándar, por lo que la curva de aprendizaje es baja. Sin embargo, la instalación inicial requiere conocimientos sobre el desbloqueo del bootloader y la gestión manual de permisos de sensores o red para aprovechar realmente sus capacidades de seguridad.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- Realizar una evaluación de impacto antes de su despliegue, ya que la ausencia de un contrato de servicio (SLA) traslada toda la responsabilidad del mantenimiento a la empresa.
- Verificar la compatibilidad con el software de gestión empresarial (MDM); muchas soluciones de control remoto corporativo no funcionan correctamente al no tener privilegios de sistema.
- Establecer protocolos internos para la gestión de actualizaciones, ya que el sistema depende exclusivamente del soporte comunitario y no de un proveedor comercial con responsabilidad legal.
- Adquirir exclusivamente hardware compatible (Google Pixel) para garantizar que el arranque verificado (Verified Boot) funcione con las claves de GrapheneOS, evitando vulnerabilidades en el inicio del sistema.
- Formar a los empleados en el uso del "Sandboxed Google Play" para evitar que instalen servicios que anulen las ventajas de privacidad del sistema mediante la concesión manual de permisos excesivos.

Privacidad y protección de datos
- El uso de GrapheneOS reduce drásticamente el flujo de telemetría, facilitando el cumplimiento del RGPD al minimizar la recogida de datos no deseada por parte de terceros (Google).
- Responsabilidades: La empresa española actúa como Responsable del Tratamiento de los datos contenidos en el dispositivo. Al no haber un proveedor de servicios detrás, no existe un Encargado del Tratamiento externo para el sistema operativo.
- Ubicación de los datos: El sistema prioriza el almacenamiento local. GrapheneOS no incluye servicios de nube propios, lo que evita transferencias internacionales de datos automáticas a EE.UU.
- Derechos ARCO: El sistema facilita el ejercicio de estos derechos al permitir un control granular y total sobre el borrado y acceso a la información almacenada en el terminal.

Propiedad intelectual
- Propiedad de datos: El usuario y la empresa mantienen la propiedad absoluta de todos los datos generados y almacenados.
- Propiedad del resultado/procesamiento: Dado que es un sistema operativo de código abierto (Open Source), no existen restricciones sobre la propiedad intelectual de los trabajos desarrollados o procesados dentro del dispositivo.
- Licencia: El código base se distribuye mayoritariamente bajo la Licencia MIT, lo que permite su uso, copia y modificación con mínimas restricciones, siempre que se incluya el aviso de copyright original.

Usos y prohibiciones
- Usos admitidos: Uso profesional para el manejo de información clasificada, protección de fuentes periodísticas, secreto profesional legal y comunicaciones corporativas seguras.
- Usos prohibidos: No debe utilizarse para eludir sistemas de protección de derechos de autor (DRM), ya que GrapheneOS puede no ser compatible con ciertos niveles de certificación requeridos por aplicaciones de contenido protegido.

Seguridad y certificaciones
- Seguridad: Incluye "Hardened Malloc" para evitar ataques de memoria y aislamiento total (Sandboxing) de aplicaciones a nivel de núcleo.
- Certificaciones: No posee certificaciones comerciales estándar (como Common Criteria) debido a su naturaleza comunitaria, pero implementa atestación de hardware mediante el chip Titan M2, permitiendo verificar que el sistema no ha sido manipulado.
- Protección USB: Permite bloquear la transferencia de datos por cable mientras el dispositivo está bloqueado, previniendo extracciones forenses de datos.

Otros
- Es importante destacar que GrapheneOS no es un producto comercial, sino un proyecto de investigación y desarrollo. Una empresa española debe ser consciente de que no existe un "soporte técnico" al que reclamar en caso de fallo crítico, lo que sitúa el impacto legal y operativo de su uso en un nivel Medio/Alto dependiendo de la criticidad de la operación.

Fuentes consultada:
- Contratos: https://grapheneos.org/LICENSE.txt
- Condiciones: https://grapheneos.org/faq

- Licencias: https://github.com/GrapheneOS/platform_manifest/blob/14/README.md
- Documentación técnica: https://grapheneos.org/features

Para más información y herramientas:

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

Inicio Todas las herramientas Categorías