



“En un mundo donde la privacidad ya no es opcional, nosotros la convertimos en un activo.”

ScrutinyX Phone, un dispositivo diseñado para quienes necesitan **comunicarse sin riesgos**.



AS SEEN ON



scrutinyx.com

Problema Global

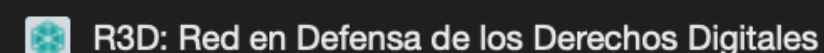
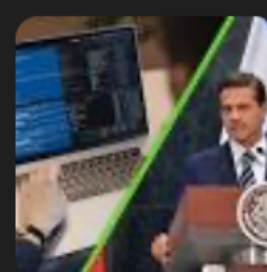
El espionaje móvil es una amenaza real y creciente



Un pago de 25 mdd a Peña Nieto habría abierto la puerta a Pegasus en México, según empresarios israelíes

De acuerdo con un medio de información israelí, el expresidente Enrique Peña Nieto habría recibido sobornos por 25 millones de dólares a...

Jul 7, 2025



El hackeo al teléfono de la presidenta Sheinbaum requiere una investigación seria

"Sí, sí hackearon mi teléfono", admitió la presidenta Claudia Sheinbaum en la conferencia matutina del 17 de marzo de 2025, un par de días...

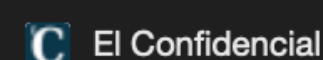
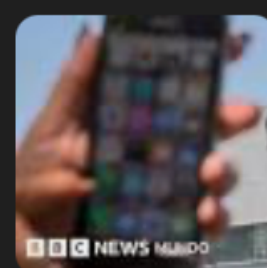
Mar 20, 2025



El "hackeo a gran escala" con un programa espía israelí a periodistas y activistas de El Salvador

Casi tres docenas de periodistas y activistas habrían sido espiados a través del sofisticado programa Pegasus, creado por la empresa israelí...

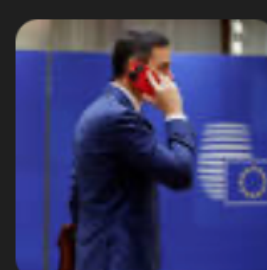
Jan 13, 2022



La imprudencia de Sánchez: siguió usando WhatsApp pese al 'hackeo' con Pegasus ya en 2021

La primera alerta llegó el 29 de octubre de 2019. Meta Platforms envió un mensaje a al menos 1.400 usuarios de WhatsApp, entre ellos un puñado...

May 16, 2025



The New York Times

Mundo EE. UU. América Latina Tiempo y clima Negocios Ciencia Cultura Estilos de vida

Políticos y funcionarios, blanco de vigilancia en México

La fiscalía de Ciudad de México solicitó los registros telefónicos de políticos y funcionarios, según consta en expedientes. Muchas de las personas vigiladas dicen que se les siguió por razones políticas.

EL ECONOMISTA

ÚLTIMAS NOTICIAS | TENDENCIAS: FINANZAS PERSONALES | JORNADA LABORAL | ALIANZA EDUCATIVA | MERC

TECNOLOGÍA

48% de mexicanos dice haber sufrido un ciberataque en su dispositivo móvil

México supera la media global en ciberataques móviles, con 48% de usuarios afectados frente al promedio de 40% mundial.

Diseñado para quienes más deben protegerse

Segmentos clave:

 Directores generales / C-levels

 Políticos y funcionarios

 Periodistas de investigación

 Artistas, influencers y figuras públicas

 Empresas de seguridad, despachos legales, notarias, embajadas, etc.

Dispositivo Seguro ScrutinyX Phone

“En un mundo donde la privacidad ya no es opcional, nosotros la convertimos en un activo.”

Un dispositivo diseñado para quienes necesitan **comunicarse sin riesgos**.

Basado en un equipo **Google Pixel**, cargado con el sistema operativo **GrapheneOS** —el sistema operativo móvil más seguro del mundo—, este equipo elimina por completo los rastreadores y vulnerabilidades de los sistemas convencionales (iOS y Android).

Incluye pre-instalado un entorno de aplicaciones cifradas de última generación:

- **Signal**, para mensajería y llamadas con cifrado de extremo a extremo.
- **Proton VPN, Mail y Drive**, que garantizan navegación, correo y almacenamiento totalmente privados.

Cada componente está libre de publicidad, rastreo o vínculos con grandes corporaciones.

El resultado: un ecosistema de comunicación impenetrable, confiable y 100% bajo tu control.



Dispositivo Seguro ScrutinyX Phone

Ventaja global del ecosistema

- **GrapheneOS protege** el sistema operativo y los datos locales.
 - **Signal protege** las comunicaciones en tránsito.
 - **Proton protege** la identidad y el entorno digital (correo, nube, red).
 - Todo bajo un hardware confiable (Google Pixel) y gestión profesional de configuración segura.
- 🧠 **El resultado: un “celular seguro” que** no espía, no filtra, no registra y no se deja infectar

COSTOS:

Google Pixel 9 Pro: \$6,000 USD+iva

Google Pixel 9 Pro XL: \$6,200 USD+iva



GrapheneOS — Sistema operativo blindado

Android Open Source Project (AOSP), modificado con mejoras de seguridad a nivel kernel, memoria, sandboxing y control de permisos.

Ventajas principales:

1. Seguridad a nivel de hardware:

Aprovecha los chips Titan M2 de Google Pixel, asegurando el arranque verificado (*Verified Boot*), el cifrado completo del dispositivo y la protección contra manipulación física.

2. Aislamiento de procesos (Sandbox reforzado):

Cada aplicación se ejecuta en un entorno completamente aislado, reduciendo la posibilidad de que un fallo en una app comprometa el sistema entero.

3. Privacidad avanzada en permisos:

Control granular sobre ubicación, sensores, red, cámara y micrófono; incluso se pueden “fingir” ubicaciones o negar acceso a sensores cuando el usuario lo desee.

4. Memoria protegida:

Emplea técnicas avanzadas como *hardened_malloc* y *exec_spawning* para prevenir exploits de memoria usados por malware y spyware tipo Pegasus.

5. Modo de red aislada:

Permite desactivar el acceso a red de cualquier aplicación individualmente, ideal para analizar o aislar procesos sospechosos.

◆ **En resumen: GrapheneOS convierte un Pixel en un entorno militar de comunicaciones, manteniendo la funcionalidad de un teléfono moderno.**

Signal — Comunicación cifrada sin rastreo

Protocolo Signal, considerado el estándar más seguro del mundo en mensajería privada.

Características clave:

1. Cifrado de extremo a extremo (E2E):

Todos los mensajes, llamadas y videollamadas están cifrados punto a punto mediante el protocolo **Double Ratchet**, que renueva las claves en cada mensaje.

2. Sin almacenamiento en servidores:

Signal no guarda copias de tus mensajes ni metadatos. Los mensajes viejos se borran del servidor en cuanto son entregados.

3. Código abierto y auditado:

El código del cliente y del servidor está disponible públicamente, auditado por expertos y universidades de ciberseguridad.

4. Protección de metadatos:

Implementa técnicas como *Sealed Sender*, que ocultan la identidad del remitente incluso del propio servidor de Signal.

5. Mensajes autodestructivos y PIN de registro:

Permite establecer temporizadores para eliminar mensajes y proteger la identidad del usuario si el dispositivo se pierde o es robado.

◆ En resumen: Signal garantiza que solo el emisor y el receptor pueden leer la comunicación, **nadie más** (ni siquiera Signal).

Aplicaciones Proton — Ecosistema cifrado integral

Infraestructura desarrollada por **Proton AG (Suiza)**, bajo estrictas leyes de privacidad europeas y el **GDPR**.

Componentes principales:

1. Proton VPN:

- Cifrado AES-256 y túneles VPN basados en **OpenVPN y WireGuard**.
- No registra actividad (*no-logs policy* certificada).
- Rutas seguras (*Secure Core*) a través de servidores en Suiza e Islandia antes de salir a internet pública.

2. Proton Mail:

- Cifrado de extremo a extremo entre usuarios Proton.
- **Zero-access encryption**: ni Proton puede leer tus correos.
- Firma digital PGP incorporada de forma automática.
- Todos los servidores se encuentran en centros de datos suizos con protección constitucional de privacidad.

3. Proton Drive:

- Archivos cifrados en el cliente antes de subir a la nube.
- Nadie (ni Proton) puede acceder al contenido ni a los nombres de los archivos.
- Compatible con compartición segura de enlaces protegidos por contraseña.

◆ **En resumen: el ecosistema Proton crea una burbuja digital suiza, blindando correo, archivos y conexión con estándares de cifrado militar.**

Presencia en medios internacionales

ScrutinyX en CEO Times



ScrutinyX by Vonman: Liderando la innovación en ciberseguridad móvil

“En un mundo donde los teléfonos móviles son parte integral de la vida personal y profesional, la privacidad nunca ha sido tan vulnerable. Para quienes corren el riesgo de ser atacados, como periodistas, ejecutivos, políticos y figuras públicas, hay mucho en juego. Aquí es donde ScrutinyX by Vonman entra en acción, ofreciendo una solución inigualable para proteger la privacidad digital y brindar tranquilidad.” CEO TIMES – ceotimesmag.com