TOOLKIT

Estrategias y recursos para mitigar el riesgo de Spyware

NOE TAZA

Toolkit: Estrategias y recursos para mitigar el riesgo de Spyware

Manual de autodefensa digital diseñado específicamente para perfiles en riesgo de vigilancia estatal (periodistas, activistas y defensores de derechos humanos). Su objetivo es explicar qué es el spyware comercial (como Pegasus o Predator) , cómo diferenciarlo de los virus comunes y qué acciones técnicas concretas se pueden tomar para protegerse.

Financiamiento

Esta es una publicación realizada dentro del marco del proyecto "Spyware under scrutiny: Research, incidence, and prevention within the Peruvian context", desarrollado por la asociación civil Hiperderecho. Agradecemos a New Venture Fund por financiar esta investigación.

Autoría

Noe Taza

Diagramación

Lorena Marks

Ilustraciones de portada

Jugo gástrico

Diagramación de portada

Lorena Marks

Iconos

The Noun Project

Ilustraciones Interiores a color

Didi Colores y Miyuki Tuyuki

Asociación Civil Hiperderecho

hola@hiperderecho.org

CONTENIDOS

00. NOS PREPARAMOS: INTRODUCCIÓN Y EVALUACIÓN 5

Invadiendo nuestra intimidad en silencio: ¿Qué es el spyware? 5

Diferencias importantes: Spyware comercial vs. Malware ordinario 6

Casos documentados en América Latina 7

¿Soy un objetivo? 8

Glosario Básico 8

01. HIGIENE DIGITAL : IOS 10

Bloqueo y cifrado del dispositivo 10

Modo Aislamiento (Lockdown Mode) 12

Gestión de permisos de aplicaciones 13

Actualizaciones del Sistema 14

Copias de Seguridad y iCloud 14

Checklist rápido — iOS 15

02. HIGIENE DIGITAL : ANDROID 16

Bloqueo y cifrado del dispositivo 16

Advanced Protection Mode y Android 16+ 17

Gestión de permisos y aplicaciones 18

Actualizaciones y elección de dispositivo 18

Checklist rápido — Android 19

03. COMUNICACIONES Y REDES 20

Aplicaciones de mensajería: qué usar y qué evitar 20

Correo electrónico 22

Redes Wi-Fi y conexiones 23

Ubicación y sensores del teléfono 24

04. SEÑALES DE ALERTA Y AUTODIAGNÓSTICO 25

Señales de comportamiento del dispositivo 26

Revisión manual básica 26

Intrusion Logging — Android 16+ (novedad 2026) 27

05. DIAGNÓSTICO CON HERRAMIENTAS 29

MVT — Mobile Verification Toolkit 30

AndroidQF — Quick Forensics 31

Consideraciones éticas y legales del análisis forense 33

PROTOCOLO DE RESPUESTA A INCIDENTES 34

06. Cómo actuar en caso de infección 34

Redes de Apoyo: Organizaciones de ayuda y referencia 35

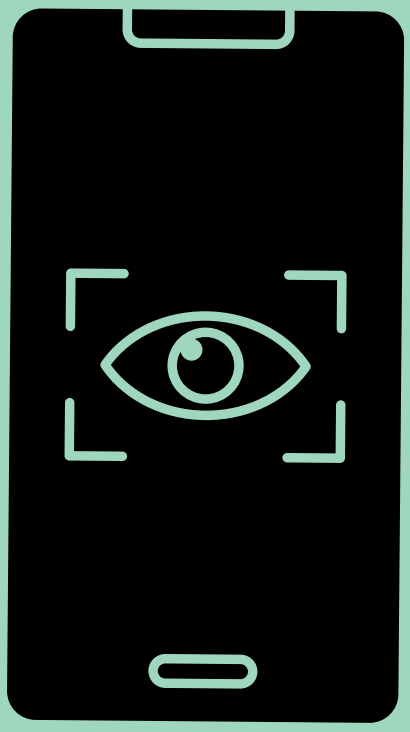
Recursos de referencia 37

00. NOS PREPARAMOS: INTRODUCCIÓN Y EVALUACIÓN

Antes de empezar: entender que es el spyware, quien lo usa y si tu eres un objetivo probable.

INVADIENDO NUESTRA INTIMIDAD EN SILENCIO: ¿QUÉ ES EL SPYWARE?

El ***spyware*** es un tipo de software malicioso que se instala en un dispositivo, a menudo sin que la persona lo sepa, y permite a terceros acceder a su contenido de forma remota. Esto puede incluir llamadas, mensajes de texto, correos electrónicos, fotos, conversaciones de aplicaciones cifradas, la cámara y el micrófono en tiempo real, y la ubicación GPS.



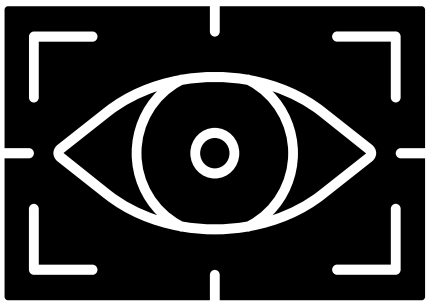
A diferencia del malware criminal común (diseñado para robar datos bancarios o extorsionar), el spyware de tipo vigilancia está construido específicamente para espiar a cualquier tipo de personas y, **entre ellas, pueden estar como objetivo:** periodistas que investigan a gobiernos o crimen organizado, activistas de derechos humanos, abogados de casos sensibles, sindicalistas, y líderes de oposición política.

Lo más preocupante de estas herramientas es que son casi invisibles, es decir no alteran el comportamiento del teléfono de manera obvia, no aparecen como apps en la pantalla, y en sus versiones más avanzadas se instalan sin que la víctima haga click en ningún enlace.

DIFERENCIAS IMPORTANTES: SPYWARE COMERCIAL VS. MALWARE ORDINARIO

(O de cómo diferenciar cuando van a por todos o todas y cuando nos buscan a nosotros o nosotras)

¿Qué cambia?	Spyware comercial (Vigilancia dirigida)	Malware criminal ordinario
¿Quién lo usa?	Gobiernos, agencias de inteligencia, actores estatales	Cibercriminales, grupos de fraude
¿A quién ataca?	Objetivos específicos y de alto perfil	Usuarios masivos, sin discriminacion
Método de infección	Zero-click (sin accion del usuario) o enlaces dirigidos	Phishing masivo, apps falsas, descargas
Capacidades	Acceso total: cámara, micrófono, apps cifradas	Contraseñas, datos bancarios, ransomware (secuestro de datos)
Visibilidad	Casi indetectable: diseñado para pasar desapercibido	Generalmente más ruidoso y detectable
Costo	Millones de dólares: vendido a Estados	Accesible y ampliamente disponible



CASOS DOCUMENTADOS EN AMÉRICA LATINA

El spyware comercial está presente en la región y existen casos comprobados y publicados por organizaciones como Citizen Lab y Amnesty Tech. La herramienta más documentada es **Pegasus**, desarrollada por la empresa israelí NSO Group: un software de vigilancia vendido exclusivamente a gobiernos que permite acceso total al dispositivo —mensajes, cámara, micrófono y ubicación— sin que la víctima haga nada. No es la única: en la región también se han documentado el uso de **Predator** (de la empresa Intellexa) y herramientas de **Hacking Team**, entre otras.

- **México:** Pegasus fue utilizado contra periodistas, activistas y figuras de la sociedad civil en múltiples casos entre 2012 y 2022. Entre los afectados se documentaron reporteros de investigación, defensores de derechos humanos, abogados de víctimas y personas cercanas a figuras políticas. Al menos 25 casos fueron documentados solo entre 2012 y 2018.
- **El Salvador:** en 2022, Citizen Lab documentó infecciones de Pegasus en 35 periodistas y personas de la sociedad civil, incluyendo redacciones enteras —22 de 34 integrantes del medio El Faro fueron infectados.
- **Brasil, Panamá, Chile y otros países:** se han documentado casos de adquisición y uso de herramientas de vigilancia similares contra periodistas y activistas.

PARA LEER MÁS

Todos los informes técnicos están disponibles en citizenlab.ca/publications y en securitylab.amnesty.org. Son la fuente de referencia más completa sobre casos documentados de spyware en el mundo.

¿SOY UN OBJETIVO?

El spyware de tipo estatal tiene un costo muy elevado y se usa de forma selectiva. No se despliega contra cualquier persona. Sin embargo, si tu trabajo o actividad implica cualquiera de los siguientes factores, tu riesgo es significativamente mayor que el de la población general.

Riesgo bajo-moderado	Riesgo moderado-alto	Riesgo alto
Activismo local o regional Participación en causas sociales sin exposición pública significativa. Riesgo real, pero herramientas más accesibles y menos sofisticadas.	**Periodismo, ONG, defensa de DDHH** Trabajo de investigación, contacto con fuentes sensibles, publicaciones críticas a actores con poder. Las herramientas usadas pueden ser spyware comercial.	**Periodismo crítico a estados y políticos de oposición** Investigaciones de corrupción, crimen organizado con nexos estatales, cobertura en contextos de conflicto, y figuras opositoras y sus equipos cercanos. El spyware tipo Pegasus es una amenaza concreta y documentada.

GLOSARIO BÁSICO

Zero-click (Infección sin clics): Método de infección que no requiere ninguna acción del usuario, el spyware se instala solo con recibir un mensaje o llamada, sin necesidad de abrirlo. Aprovecha las vulnerabilidades del software de tu dispositivo. Es la forma más peligrosa y difícil de prevenir.

One-click (Infección con un clic): El dispositivo se infecta cuando el usuario hace click en un enlace malicioso, generalmente enviado por mensaje o correo. Se puede prevenir con buenos hábitos digitales.

Sandbox (caja de arena/zona aislada): Mecanismo de aislamiento del sistema operativo que impide que una app acceda a los datos de otras apps. iOS y Android lo implementan, aunque un spyware sofisticado

puede eludirlo aprovechando vulnerabilidades.

Jailbreak / root: Proceso por el cual se elimina el sistema de protección del dispositivo para instalar software no autorizado. Un teléfono con jailbreak o root pierde prácticamente todas sus defensas de seguridad.

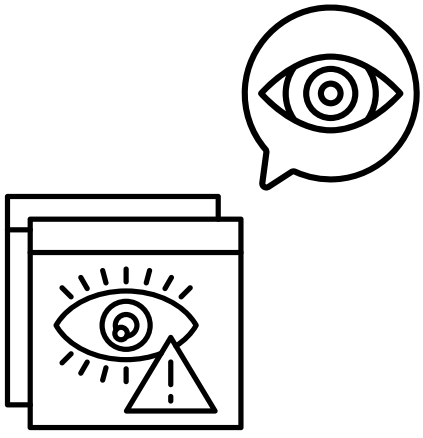
Cifrado (E2EE): Cifrado de extremo a extremo, los mensajes solo pueden leerlos quien los envía y quien los recibe. Ni el servicio (como Signal, WhatsApp, etc.) puede leerlos. Es el estándar que se debe buscar para comunicaciones sensibles.

Metadatos: "Datos sobre otros datos". Son información que describe, explica o facilita la comprensión de un recurso o archivo. Entre estos datos que pueden albergar encontramos localización, duración de una llamada, dispositivo que utilizaste, fecha y hora, etc.

Forense digital: Análisis técnico de un dispositivo para detectar rastros de spyware u otras actividades maliciosas. Requiere herramientas especializadas y, en casos de spyware comercial, conocimiento técnico avanzado.

IOC (Indicador de compromiso): Rastro técnico que indica que un dispositivo fue infectado por un spyware específico. Las herramientas como MVT (Mobile Verification Toolkit) buscan indicadores comparando el dispositivo con bases de datos de casos conocidos.

APK malicioso: Archivo de instalación de app para Android (.apk) que contiene software malicioso. Una forma común de infectar teléfonos Android es convencer al usuario de instalar un APK fuera de la tienda oficial.



01. HIGIENE DIGITAL : IOS

Para quienes usamos equipos Apple, existe la falsa creencia de que estamos 100% a salvo de cualquier ataque. Si bien iOS tiene muros fuertes, el spyware avanzado sabe cómo saltárselos si dejamos las ventanas abiertas.

Vamos a configurarlo juntas y juntos paso a paso:

BLOQUEO Y CIFRADO DEL DISPOSITIVO

- iOS cifra automáticamente todo el almacenamiento del dispositivo. Sin embargo, la fortaleza de ese cifrado depende directamente de qué tan bueno sea tu código de acceso: el sistema usa tu contraseña combinada con una clave única del chip del dispositivo para generar la clave de cifrado. Un PIN corto hace ese cifrado mucho más débil.

- Usa **un código alfanumérico de al menos 8 caracteres** (letras y números). Ve a ajustes > Face ID y código > Cambiar código > Opciones de código > Código alfanumérico personalizado.

- Los PINs de 4 o 6 dígitos son vulnerables

a **ataques de fuerza bruta y a "*smudge attacks*"** (marcas de grasa en la pantalla vlan los números usados). Evítalos si tienes un perfil de riesgo elevado.

- Activa la opción **"Borrar datos**" después de 10 intentos fallidos: Ajustes > Face ID y código > desplazarse hasta abajo > activar "Borrar datos".

- El **Secure Enclave** (chip independiente en todos los iPhone modernos) impone un retraso de 80 milisegundos entre cada intento de contraseña, lo que hace que descifrar un código alfanumérico tome décadas incluso para atacantes sofisticados.

OJO CON LA BIOMETRÍA:SOBRE FACE ID y TOUCH ID

La biometría es conveniente, pero tiene limitaciones de seguridad. En contextos de alto riesgo –cruzar fronteras, detenciones, protestas– considera desactivarlos temporalmente.

MODO AISLAMIENTO (LOCKDOWN MODE)

Apple introdujo el Modo de Aislamiento en iOS 16 específicamente para proteger a personas con alto riesgo de ser objetivos de spyware sofisticado. Bloquea muchas funciones que han sido explotadas por herramientas como Pegasus, a costa de algunas limitaciones de uso.

Lo que bloquea o limita:

- La mayoría de tipos de adjuntos en iMessage (excepto imágenes). Esto elimina uno de los vectores de ataque zero-click más usados por Pegasus.
- Tecnologías web complejas como la compilación JavaScript JIT (Just-in-Time). Reduce el riesgo de exploits desde el navegador.
- Llamadas FaceTime entrantes de personas que no están en tus contactos.
- Perfiles de configuración externos y acceso MDM (gestión de dispositivos corporativos).
- Conexiones por cable a computadoras u otros accesorios cuando el dispositivo está bloqueado.

Cómo activarlo: Ajustes > Privacidad y seguridad > Modo de aislamiento > Activar modo de aislamiento. El dispositivo se reinicia.

¿DEBO ACTIVARLO?

Si eres periodista de investigación, defensor/a de derechos humanos, o activista con perfil de riesgo alto: sí, actívalo. Algunas apps pueden funcionar de forma limitada, pero la protección que ofrece supera con creces esa incomodidad. Si tu perfil de riesgo es moderado, considera activarlo en momentos específicos de mayor exposición.

GESTIÓN DE PERMISOS DE APLICACIONES

Cada app que instalas puede pedir acceso a recursos del teléfono: cámara, micrófono, ubicación, contactos, fotos, etc. iOS es bastante estricto en pedir permiso explícito, pero muchas personas aceptan sin revisar. Una app que no necesita tu micrófono no debería tenerlo.

- **Revisa todos los permisos en Ajustes** > Privacidad y seguridad. Verás cada recurso (cámara, micrófono, ubicación, contactos) y qué apps tienen acceso. Revoca lo que no sea necesario.
- **Para la ubicación**, prefiere "Al usar la app" sobre "Siempre". Muy pocas apps necesitan tu ubicación en segundo plano.
- **Desinstala apps que no usas**. Cada app instalada es una superficie potencial de ataque.
- **Sospecha de apps que piden permisos** que no tienen sentido para su función: una app de linterna no necesita tus contactos; una app de recetas no necesita el micrófono.

CÓMO FUNCIONA LA SEGURIDAD DE APPS EN iOS

Todas las apps de iOS se ejecutan en un "sandbox": un entorno aislado que impide que lean los datos de otras apps. Tampoco pueden comunicarse entre sí directamente. Esto es una protección importante, pero no es absoluta: el spyware sofisticado puede eludirla explotando vulnerabilidades del sistema operativo.

ACTUALIZACIONES DEL SISTEMA

La mayoría de los ataques zero-click conocidos aprovechan vulnerabilidades que Apple ya ha solucionado en versiones posteriores del sistema. Estar desactualizado equivale a dejar la puerta abierta a ataques que ya tienen solución.

- **Activa las actualizaciones automáticas**: Ajustes > General > Actualización de software > Actualizaciones automáticas > activar todas las opciones.
- Cuando Apple publica **una actualización de seguridad de emergencia** (Rapid Security Response), instálala lo antes posible. Estas actualizaciones responden a vulnerabilidades que ya están siendo explotadas activamente.
- No uses dispositivos sin soporte de Apple para trabajos sensibles. Un iPhone 6 o anterior no recibe actualizaciones de seguridad y es significativamente más vulnerable.

COPIAS DE SEGURIDAD Y ICLOUD

Las copias de seguridad son esenciales para recuperarse ante un incidente, pero también pueden ser un vector de vulnerabilidad si no están protegidas correctamente.

- Si usas iCloud, activa la **Protección de datos avanzada**: Ajustes > tu nombre > iCloud > Protección de datos avanzada. Esto cifra end-to-end tus backups en iCloud (Apple no puede acceder a ellos).
- Para **copias locales** en computadora, usa iTunes/Finder con la opción “Cifrar copia de seguridad del iPhone” activada. Elige una contraseña fuerte y guárdala en un gestor de contraseñas.
- Recuerda que algunos datos del llavero (contraseñas) son “non-migratory”: solo pueden restaurarse en el mismo dispositivo físico. Si cambias de teléfono, tendrás que volver a agregar esas credenciales.

CHECKLIST RÁPIDO – IOS

- ☐ Código alfanumérico de 8+ caracteres activado
- ☐ Borrado automático tras 10 intentos activado
- ☐ iOS actualizado a la versión más reciente
- ☐ Modo de aislamiento activado (alto riesgo) o evaluado
- ☐ Permisos de apps revisados: cámara, micrófono, ubicación, contactos
- ☐ Apps desconocidas o sin uso desinstaladas
- ☐ Protección de datos avanzada en iCloud activada
- ☐ Actualizaciones automáticas habilitadas

02. HIGIENE DIGITAL : ANDROID

Android presenta más variedad entre fabricantes y versiones, lo que implica riesgos distintos. Estas medidas aplican a la mayoría de dispositivos modernos.

BLOQUEO Y CIFRADO DEL DISPOSITIVO

Los dispositivos Android modernos (Android 6+) cifran el almacenamiento por defecto, pero la seguridad real de ese cifrado depende de la calidad del método de desbloqueo que uses.

- **Usa un PIN largo (8+ dígitos) o una contraseña alfanumérica**. Ve a Ajustes > Seguridad > Bloqueo de pantalla.
- **Evita el patrón de puntos.** Los patrones son vulnerables de dos maneras: las marcas de grasa en la pantalla revelan el trazo, y la mayoría de personas usa patrones simples (menos de 1.600 combinaciones son las más comunes). Un PIN de 8 dígitos es exponencialmente más seguro.
- Si usas reconocimiento facial, ten en cuenta que en muchos dispositivos Androiddegamamediaesmenosseguro que en iPhone: puede desbloquearse con una foto. Complementa siempre con PIN.

ADVANCED PROTECTION MODE Y ANDROID 16+

Google introdujo el **Advanced Protection Mode** en Android como equivalente al Modo de Aislamiento de Apple. Actualmente está disponible en dispositivos Pixel con Android 16 y se espera que se extienda a otros fabricantes. Si tienes un Pixel actualizado, es una de las medidas más importantes que puedes tomar.

- Para activarlo en Pixel: Ajustes > Seguridad y privacidad > Protección avanzada. El dispositivo pedirá una clave de seguridad (hardware key) o configurará otras medidas de autenticación fuertes.
- Entre otras protecciones, limita la instalación de apps desde fuera de Google Play y activa protecciones adicionales contra exploits.
- Es un requisito previo para activar el **Intrusion Logging** (ver sección 04), la nueva herramienta forense de Android 2026.

¿POR QUÉ ANDROID HA SIDO HISTÓRICAMENTE MÁS DIFÍCIL DE ANALIZAR?

Hasta 2026, los casos públicos documentados de Pegasus en Android eran significativamente menos que en iOS, no porque Android sea más seguro, sino porque existían menos herramientas forenses para detectar el spyware en este sistema. El lanzamiento de **Intrusion Logging** por parte de Google —diseñado en colaboración con Amnesty Tech— cambia esta situación de forma importante.

GESTIÓN DE PERMISOS Y APLICACIONES

El modelo de permisos de Android da a cada app un UID (identificador de usuario) único y la ejecuta en su propio sandbox. Sin embargo, Android históricamente ha sido más flexible que iOS con la instalación de apps externas, lo que amplía la superficie de ataque.

- **Revisa los permisos en Ajustes** > Privacidad > Gestor de permisos. Igual que en iOS: revoca lo que no sea necesario.
- **No instales APKs fuera de Google Play** a menos que sepas exactamente qué estás instalando y confíes plenamente en la fuente. Esta es la vía de infección más común en Android.
- En Ajustes > Seguridad, busca "Instalar apps desconocidas" y asegúrate de que ninguna app tenga ese permiso activado.
- **No hagas root** a tu dispositivo. El proceso elimina el sandbox y las protecciones de aislamiento que Android usa para contenerte el daño de apps maliciosas.

ACTUALIZACIONES Y ELECCIÓN DE DISPOSITIVO

A diferencia de Apple, que controla todas las actualizaciones para todos sus dispositivos, en Android el ciclo de actualizaciones depende del fabricante. Esto crea una brecha de seguridad importante: muchos dispositivos asequibles solo reciben actualizaciones durante 2-3 años.

- **Activa las actualizaciones automáticas del sistema:** Ajustes > Acerca del teléfono > Actualización del sistema.
- Si tu dispositivo ya no recibe actualizaciones de seguridad, considera reemplazarlo para trabajo sensible. Un teléfono sin parches es un objetivo fácil.
- **Los dispositivos Pixel de Google** reciben actualizaciones directamente de Google durante más tiempo y son los únicos que hoy pueden usar Intrusion Logging. Para perfiles de alto riesgo, son la opción Android más recomendable.

CHECKLIST RÁPIDO – ANDROID

- ☐ PIN de 8+ dígitos o contraseña alfanumérica activada (sin patrón)
- ☐ Android actualizado a la versión más reciente disponible
- ☐ Instalación de apps de fuentes desconocidas desactivada
- ☐ Permisos de apps revisados desde el Gestor de permisos
- ☐ Apps sin uso desinstaladas
- ☐ Advanced Protection Mode activado (si usas Pixel con Android 16+)
- ☐ Intrusion Logging activado antes de cualquier incidente (Pixel / Android 16+)
- ☐ Dispositivo con soporte activo del fabricante confirmado

03. COMUNICACIONES Y REDES

La seguridad del dispositivo es solo una parte. Cómo te comunicas y a qué redes te conectas determina qué información puede ser interceptada.

APLICACIONES DE MENSAJERÍA: QUÉ USAR Y QUÉ EVITAR

No todas las apps de mensajería ofrecen el mismo nivel de protección. La diferencia clave es el cifrado de extremo a extremo (E2EE): que los mensajes viajen cifrados de tal manera que nadie —ni el proveedor del servicio— pueda leerlos en tránsito.

Aplicación	Cifrado E2EE	Metadatos	Recomendación
Signal	Sí, siempre y por defecto	Mínimos; Signal no los almacena	Recomendado para comunicaciones sensibles
iMessage	Sí, entre usuarios Apple	Visibles para Apple (con quién, cuándo)	Aceptable; preferir con Protección avanzada activada
WhatsApp	Sí, para mensajes	Ampliamente recolectados por Meta	Aceptable para contenido; evitar para redes sensibles
Telegram	Solo en "Chats Secretos"	Recolectados por Telegram	Los chats normales NO están cifrados E2EE
SMS/llamadas de voz	No	Recolectados por operadora	Evitar para información sensible

SOBRE TELEGRAM: UN ERROR COMÚN

Telegram es ampliamente usada en comunidades de activistas por su facilidad de uso y sus grupos grandes. Sin embargo, **los chats normales y los grupos de Telegram NO tienen cifrado de extremo a extremo.** Telegram puede leer esos mensajes. Solo los "Chats Secretos" (disponibles únicamente en chats individuales, no en grupos) usan cifrado E2EE. Para grupos sensibles, Signal o Element (Matrix) son opciones más seguras.

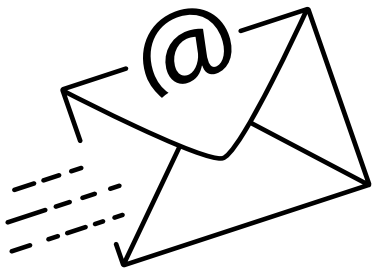
SIGNAL COMO OPCIÓN RECOMENDADA:

- Activa el **bloqueo con código en Signal:** Signal > Ajustes > Privacidad > Bloqueo de pantalla. Así, incluso si alguien accede a tu teléfono desbloqueado, no puede leer tus conversaciones de Signal.
- Configura la **desaparición automática de mensajes en Signal:** dentro de cada conversación, activa los mensajes que desaparecen. Para conversaciones sensibles, 1 semana o menos.
- Verifica el **número de seguridad** de tus contactos clave en Signal: esto confirma que la comunicación no ha sido interceptada por un ataque de persona-en-el-medio (man-in-the-middle).

CORREO ELECTRÓNICO

El correo electrónico convencional (Gmail, Outlook, etc.) no está cifrado de extremo a extremo. El proveedor puede leer los mensajes, y están expuestos a solicitudes legales. Para comunicaciones muy sensibles:

- Usa **Proton Mail** (proton.me): ofrece cifrado E2EE entre cuentas Proton y cifrado del almacenamiento. Tiene apps para iOS y Android.
- Para comunicaciones con personas fuera de Proton, considera usar **PGP** (Pretty Good Privacy). Requiere más configuración, pero permite cifrar correos con cualquier destinatario.
- Para correos normales (no sensibles), activa la autenticación en dos pasos en tu cuenta y usa una contraseña única y fuerte.



REDES WI-FI Y CONEXIONES

Las redes Wi-Fi públicas —hoteles, aeropuertos, cafeterías— son entornos donde el tráfico puede ser interceptado más fácilmente. Aunque HTTPS protege el contenido de la mayoría del tráfico web, hay otras formas de ataques en redes locales.

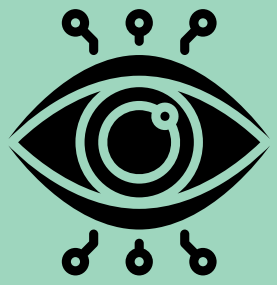
- Usa una **VPN confiable** cuando te conectes a Wi-Fi público. Como regla general, las VPN de pago son más confiables que las gratuitas: las gratuitas frecuentemente financian su servicio recolectando y vendiendo datos de navegación, que es exactamente lo que se intenta proteger. Opciones recomendadas por la comunidad de seguridad por su política de no-registro (no-log) verificada: **Mullvad y ProtonVPN** (tiene versión gratuita con limitaciones). Antes de elegir cualquiera, verifica que haya tenido auditorías de seguridad independientes publicadas.
- Verifica que los sitios que visitas usan **HTTPS** (el candado en la barra del navegador). Nunca ingreses contraseñas o información sensible en sitios HTTP.
- Desactiva la función de **conexión automática a redes Wi-Fi conocidas:** tu teléfono puede conectarse a redes maliciosas que imitan el nombre de una red que usaste antes.
- Apaga el **Bluetooth** cuando no lo estés usando. Algunos ataques históricos (BlueBorne, KNOB) han explotado Bluetooth para comprometer dispositivos cercanos.

UBICACIÓN Y SENSORES DEL TELÉFONO

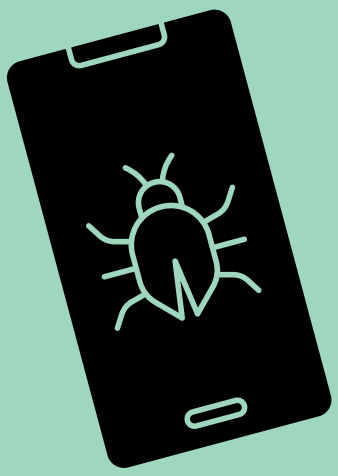
Tu teléfono tiene múltiples sensores que pueden revelar tu ubicación y hábitos, incluso sin acceso explícito al GPS.

- **Desactiva la ubicación para apps que no la necesitan de forma activa.** Revisa cada app en Ajustes > Privacidad > Localización (iOS) o Gestor de permisos (Android).
- El **acelerómetro y el sensor de batería** no requieren permiso explícito en Android y han sido usados en investigación académica para inferir rutas de viaje. Esto no es un riesgo cotidiano, pero es un recordatorio de que los sensores tienen implicaciones de privacidad.
- **El portapapeles del sistema** (donde van las cosas que copias) es accesible por todas las apps instaladas en muchos sistemas. Evita copiar contraseñas o información sensible en el portapapeles y déjala ahí durante mucho tiempo.
- iOS 14+ muestra un indicador naranja cuando el micrófono está en uso y verde cuando la cámara está activa. Presta atención a estas alertas cuando estén activadas por apps que no debería usarlas.

04. SEÑALES DE ALERTA Y AUTODIAGNÓSTICO



El spyware sofisticado está diseñado para ser invisible. Sin embargo, puede dejar rastros. Esta sección te muestra qué buscar, sin necesidad de herramientas técnicas.



IMPORTANTE ANTES DE EMPEZAR

Las señales que se describen aquí son indicios, no pruebas definitivas. Muchas pueden tener explicaciones inocentes. Lo que importa es el patrón: varias señales apareciendo juntas, especialmente después de un evento de riesgo (una reunión importante, una publicación, un viaje a un país de alto riesgo), debe tomarse en serio.

SEÑALES DE COMPORTAMIENTO DEL DISPOSITIVO

Estas son señales que puedes notar sin necesidad de conocimientos técnicos:

- **La batería se agota mucho más rápido de lo habitual** sin que hayas cambiado tus hábitos de uso. El spyware ejecuta procesos en segundo plano que consumen energía.
- **El dispositivo se calienta en reposo**, cuando no estás haciendo nada con él. Esto puede indicar procesamiento intensivo en segundo plano.
- **Consumo de datos móviles inusualmente alto**, especialmente de noche o cuando no estás usando el teléfono activamente. El spyware transmite datos al servidor del atacante.
- **La pantalla se enciende sola**, sin que toques el dispositivo ni llegue una notificación visible.
- **Apps que se cierran solas** o el sistema se comporta de forma errática sin razón aparente.
- **Ruidos extraños durante llamadas:** ecos, clicks, interferencias que no escuchabas antes.
- **Capturas de pantalla que no tomaste** o fotos en tu carrete que no recuerdas haber sacado.

REVISIÓN MANUAL BÁSICA

Estas revisiones toman menos de 10 minutos y no requieren herramientas especiales:

- **Revisa las apps instaladas.** Busca apps que no reconoces. En iOS: mantén presionado un ícono > Editar pantalla de inicio para ver todo. En Android: Ajustes > Apps. Googlea el nombre de cualquier app desconocida.
- **Revisa el consumo de datos por app.** iOS: Ajustes > Datos móviles. Android: Ajustes > Red > Uso de datos. Busca apps que consumen datos de fondo de forma inesperada.

- **iOS: verifica los perfiles de configuración instalados.** Ajustes > General > VPN y gestión del dispositivo. Si ves perfiles que no reconoces y no vienen de tu empleador o empresa, es una señal preocupante.
- **Android: revisa apps con permisos de administrador de dispositivo.** Ajustes > Seguridad > Apps de administración de dispositivo. Solo deberían aparecer apps que tú hayas configurado explícitamente (como gestión empresarial).
- **Revisa los permisos de micrófono y cámara** (ver sección 01 y 02). Cualquier app con acceso que no lo justifique merece atención.

INTRUSION LOGGING – ANDROID 16+ (NOVEDAD 2026)

En mayo de 2026, Google lanzó **Intrusion Logging**, una nueva función de registro forense dentro del Advanced Protection Mode de Android. Fue desarrollada en colaboración directa con el Security Lab de Amnesty International y el Digital Security Lab de RSF, quienes identificaron la necesidad hace más de dos años.

Es la primera vez que un fabricante de dispositivos construye un sistema de registro diseñado específicamente para apoyar investigaciones forenses consensuadas sobre ataques sofisticados.

- **Qué registra:** acceso a recursos del sistema (cámara, micrófono, ubicación, datos), actividad de red inusual, cambios en la configuración del sistema. Genera logs que pueden analizarse con herramientas especializadas para detectar patrones de spyware.
- **Requisitos:** dispositivo Pixel con Android 16, Advanced Protection Mode activo, y la función habilitada manualmente. Actualmente se está extendiendo a más dispositivos con Android 16.
- **Cómo activarlo:** Ajustes > Seguridad y privacidad > Protección avanzada > Registro de intrusiones > Activar. Debe activarse antes de cualquier incidente: no genera información retroactiva.
- **Cómo usar los logs:** los logs se pueden recolectar con AndroidQF

y analizarse con MVT. El Security Lab de Amnesty publicó una guía técnica completa en securitylab.amnesty.org (mayo 2026).

POR QUÉ ESTO IMPORTA

Históricamente, casi todos los casos documentados públicamente de Pegasus y otros spyware comerciales han sido en iPhones, no porque Android sea más seguro sino porque iOS ofrecía mejores herramientas forenses. Intrusion Logging cambia esa ecuación y debería permitir documentar muchos más casos en Android, especialmente en dispositivos de gama media —los más usados en el sur global.

05. DIAGNÓSTICO CON HERRAMIENTAS

Para ir más allá del autodiagnóstico visual, existen herramientas de análisis forense. Estas fueron desarrolladas por organizaciones especializadas en seguridad digital para la sociedad civil.

ANTES DE USAR CUALQUIER HERRAMIENTA

Si sospechas activamente que tu dispositivo está comprometido en este momento, no lo apagues. Algunos spyware borran rastros al reiniciar. Contacta primero a un equipo especializado (sección 06) para que te orienten sobre cómo proceder sin destruir evidencia.

MVT – MOBILE VERIFICATION TOOLKIT

mvt · Mobile Verification Toolkit

iOS + Android | Línea de comandos | Código abierto | github.com/mvt-project/mvt

MVT fue desarrollado por el Security Lab de Amnesty International y es la herramienta estándar de referencia para detectar spyware en dispositivos móviles. Funciona analizando el dispositivo en busca de **Indicadores de Compromiso (IOCs)** —rastros técnicos específicos dejados por spyware conocido como Pegasus, Predator y otros. Fue lanzado en julio de 2021 en el contexto del Proyecto Pegasus y es mantenido activamente por Amnesty International y colaboradores. La versión actual es mvt-2026.5.12 (mayo 2026).

La versión de mayo 2026 incorpora soporte para analizar automáticamente los **Intrusion Logs de Android 16+**, lo que abre nuevas posibilidades de detección en ese sistema.

PARA IOS:

- Analiza el backup del dispositivo hecho con iTunes o Finder, o el sistema de archivos completo (si el dispositivo fue previamente jailbreakeado por investigadores para ese fin).
- Busca procesos sospechosos, dominios de red maliciosos, y modificaciones inusuales en el sistema.
- Requiere hacer primero un backup cifrado del iPhone en la computadora.

PARA ANDROID:

- Analiza backups de Android, APKs instalados, y ahora también los Intrusion Logs de Android 16+.
- Detecta apps maliciosas conocidas y comportamientos de red asociados a spyware documentado.

NIVEL DE DIFICULTAD

MVT requiere usar la línea de comandos (terminal) con Python/pipx instalado, y solo tiene soporte oficial para Linux y macOS (Windows tiene soporte parcial via WSL). No está diseñado para autodiagnóstico de usuarios finales. Si no tienes experiencia técnica, lo mejor es contactar con un equipo especializado. Advertencia crítica sobre los resultados: los IOCs públicos son insuficientes para concluir que un dispositivo está "limpio". Un resultado negativo no descarta la infección —un spyware nuevo o una variante no documentada podría no ser detectada. El análisis forense confiable requiere indicadores no públicos y expertise profesional.

ANDROIDQF – QUICK FORENSICS

`androidqf · Android Quick Forensics`

Android | Línea de comandos | Código abierto | github.com/mvt-project/androidqf

Herramienta portable desarrollada originalmente por Claudio Guarnieri y mantenida activamente como fork por el Amnesty International Security Lab en `mvt-project/androidqf`. Permite la **recolección rápida de evidencia forense** en dispositivos Android sin necesidad de hacer root. Disponible como binario ejecutable para Linux, Windows y macOS. Los datos recolectados se analizan con MVT.

Desde mayo de 2026, cuando el dispositivo tiene Intrusion Logging activo, AndroidQF descarga, descifra y recolecta automáticamente los Intrusion Logs como parte de la adquisición, y MVT los analiza al correr `check-androidqf`.

REQUISITOS PRÁCTICOS (IMPORTANTES):

- Requiere conectar el dispositivo Android a la computadora con **cable USB**.
- Es necesario activar el **modo desarrollador y USB Debugging** en el dispositivo antes de iniciar la adquisición (Ajustes > Acerca del teléfono >Número de compilación, toca 7 veces). Tras la adquisición, se deben desactivar.
- El dispositivo mostrará un aviso pidiendo autorizar la conexión USB de la computadora. Debe autorizarse para continuar.

QUÉ RECOLECTA:

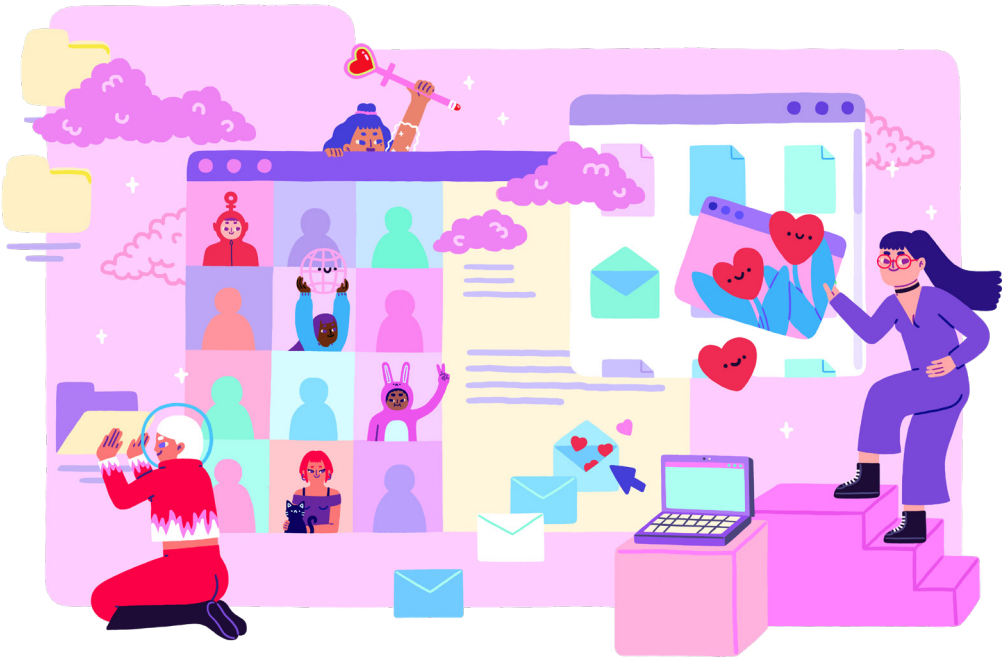
- Lista completa de apps instaladas y sus APKs (opcional).
- Logs del sistema (bugreport), información de red, archivos temporales del sistema.
- Intrusion Logs de Android 16+ (si está activado en el dispositivo).
- Backup de SMS (opcional) y backup de apps que lo permiten.

ADVERTENCIA: SEGURIDAD DEL ARCHIVO DE ADQUISICIÓN

El archivo generado puede contener datos muy sensibles: historial de apps, SMS, y si se recolectaron Intrusion Logs, historial de navegación. Si vas a trasladar ese archivo, usa una unidad cifrada. AndroidQF permite cifrar la adquisición con una clave pública para proteger los datos en tránsito hacia el analista.

CONSIDERACIONES ÉTICAS Y LEGALES DEL ANÁLISIS FORENSE

- **Consentimiento siempre:** el análisis forense de un dispositivo ajeno sin autorización explícita puede ser ilegal. Estas herramientas son exclusivamente para analizar tu propio dispositivo o el de alguien que te ha dado permiso expreso y documentado.
- **Los Intrusion Logs contienen datos sensibles:** incluyendo historial de navegación. Antes de compartirlos con cualquier persona o equipo, asegúrate de que sea una organización de confianza y que la persona dueña del dispositivo haya dado consentimiento informado.
- **Confidencialidad de los resultados:** si encuentras indicios de compromiso, la información es potencialmente sensible. Compártela solo con organizaciones especializadas de confianza (ver sección 06).
- **Los resultados negativos no son garantía:** estas herramientas buscan IOCs conocidos y publicados. Un spyware nuevo, una variante sin documentar, o indicadores no públicos no serán detectados. El análisis forense profesional con indicadores privados da resultados más completos.



06. CÓMO ACTUAR EN CASO DE INFECCIÓN

Si las señales apuntan a una posible infección, actuar con calma y en el orden correcto hace la diferencia entre preservar evidencia y perderla.

PROTOCOLO DE RESPUESTA A INCIDENTES

01 No apagues ni reinicies el dispositivo todavía

Algunos spyware eliminan rastros de sí mismos cuando el dispositivo se reinicia. Si hay evidencia forense, está en la memoria del sistema ahora. Antes de apagar, consulta con un equipo especializado si debes hacer alguna recolección de datos.

02 Documenta y anota cuándo empezaron las señales

Escribe en papel o en otro dispositivo: qué señales notaste, cuándo empezaron, qué eventos ocurrieron antes (reuniones, viajes, mensajes inusuales recibidos, contacto con personas nuevas). Esta cronología es valiosa para los analistas.

03 Contacta a un equipo especializado antes de hacer cambios

Las organizaciones de la lista a continuación tienen experiencia en este tipo de casos. Pueden orientarte sobre los pasos exactos para tu situación, evitar la destrucción de evidencia, y apoyar el proceso de análisis si decides seguir adelante. **Si estás en Perú, puedes contactar a Hiperderecho como primer punto de contacto local especializado en derechos digitales.**

04 Aísla el dispositivo

Activa el modo avión. No lo conectes a ninguna red Wi-Fi ni Bluetooth. Si el spyware está activo, el aislamiento limita su capacidad de transmitir datos nuevos. No lo conectes a ninguna computadora todavía sin instrucción de los expertos.

05 Desde otro dispositivo, cambia contraseñas críticas

Si el dispositivo comprometido tenía acceso a correo, redes sociales, servicios de mensajería, o herramientas de trabajo, cambia esas contraseñas desde un dispositivo diferente y limpio. Activa la autenticación en dos pasos donde no la tengas.

06 Considera reportar el caso

Los casos documentados de spyware contribuyen a investigaciones globales que protegen a otras personas. Organizaciones como Citizen Lab o Amnesty Tech pueden ayudarte a reportar si decides hacerlo. Nunca es obligatorio, pero tiene un valor real para la comunidad.

REDES DE APOYO: ORGANIZACIONES DE AYUDA Y REFERENCIA

Access Now — Digital Security Helpline

Ayuda directa de seguridad digital para activistas, periodistas y ONGs. Disponible 24/7, en español y múltiples idiomas. Atienden casos de spyware, vulneración de cuentas y otros incidentes.

accessnow.org/help-es

Amnesty International — Security Lab

Equipo técnico especializado en detección de spyware comercial. Desarrolladores de MVT y AndroidQF. Publican investigaciones sobre casos documentados de Pegasus y otros.

securitylab.amnesty.org

Citizen Lab (Universidad de Toronto)

Laboratorio de investigación interdisciplinaria especializado en vigilancia digital y derechos humanos. Documentaron la mayoría de los casos conocidos de Pegasus en América Latina.

citizenlab.ca

Frontline Defenders
Apoyo integral a defensoras y defensores de derechos humanos en riesgo, incluyendo seguridad digital. Especializados en casos de alto riesgo.

frontlinedefenders.org

RSF — Digital Security Lab
Reporteros Sin Fronteras. Apoyo de seguridad digital específicamente para periodistas. Colaboraron con Amnesty y Google en el desarrollo de Intrusion Logging.

rsf.org/en/digital-security-lab

EFF — Electronic Frontier Foundation
Recursos, guías y herramientas de autoprotección digital. Su sitio Surveillance Self-Defense es una referencia completa y accesible en español.

ssd.eff.org

Hiperderecho (Perú)
Organización peruana sin fines de lucro dedicada a la promoción de derechos y libertades en entornos digitales. Referente de seguridad digital y derechos digitales en el país.

hiperderecho.org - hola@hiperderecho.org

¡Hagamos comunidad! La información nos quita el miedo y nos permite resistir de manera segura tanto en las calles como en los entornos virtuales. No olvides compartir estas pautas de cuidado mutuo con tus amigues, compañeres de colectivos y redes de confianza.

RECURSOS DE REFERENCIA

- **Guía técnica de Intrusion Logging (Amnesty, mayo 2026):** cómo recolectar y analizar los nuevos logs forenses de Android.

  securitylab.amnesty.org/latest/2026/05/android-intrusion-logging-as-a-new-source-of-data-for-consensual-forensic-analysis

- **Apple iOS Security Guide:** documentación oficial de Apple sobre las protecciones de seguridad del sistema.

  support.apple.com/es-es/guide/security/welcome/web

- **Android Security Bulletin:** lista de parches de seguridad de Google, actualizada mensualmente.

  source.android.com/security/bulletin

- **Surveillance Self-Defense (EFF):** guías prácticas de autoprotección en español, por plataforma y nivel de riesgo.

  ssd.eff.org/es/module-categories/guías-herramientas

- **Security in a Box:** herramientas y tácticas de seguridad digital para activistas y defensores de DDHH.

  securityinabox.org

- **Repositorio de MVT:** herramienta de análisis forense móvil de Amnesty Tech, con documentación y actualizaciones.

  github.com/mvt-project/mvt

HIPERDERECHO