AUTORIA

Amarelu y Martu Isla (Amartu)

AGRADECIMIENTOS

Muchas gracias a las compañeras de Navegando Libres, Fembloc, Luchadoras y Maria d'Ajuda por su tiempo y por compartir tantas ideas. Esperamos que este material sirva de devolución y esté a la altura de su tremendo trabajo.

Muchas gracias a la Rede Transfeminista de Cuidados Digitais por compartir su infraestructura digital.

Muchas gracias también a Ariel, Lux, Foz, Tes, Inés y todas las personas que tomaron su tiempo para revisar el contenido y darnos su feedback.

Muchas gracias al Center for Digital Resilience por confiar en nosotres para el desarrollo de este proyecto.

VERSION WEB Y DESCARGAS

es.celularhackeado.net (en Español)

pt.celularhackeado.net (en Portugués)

CONTACTO

amartu-zine@riseup.net

<TU PAREJA NO ES HACKER>

Parte 2: Desmitificando el análisis de celulares

Licencia

24 https://labekka.red/licencia-f2f/

También te animamos a revisar tu propio Google Takeout[20], con paciencia y considerando que quizás no sepas interpretar toda la información ¡pero mucha otra sí!

Si quieres aprender a hacer análisis más técnicos te recomendar visitar la documentación de SocialTic sobre análisis forense consentido en beneficio de la sociedad civil[21] y contactar con líneas de atención feminista[22]. y organizaciones de derechos digitales de tu región[23] Elles seguro te pueden recomendar más recursos para aprender y resolver dudas sobre tus análisis.

¡Esperamos que toda esta información te haya sido útil y ahora te sientas con más fortaleza y conocimiento para enfrentar cualquier supuesto "hackeo"!

20 Ver apartado 4 (Cómo generar un Google Takeout).
21 https://forensics.socialtic.org/
22 https://feministhelplines.org/es/
23 https://securitylab.amnesty.org/digital-resources/

Contenidos

Introducción

Al colaborar con líneas de ayuda feministas dedicadas a los cuidados digitales, notamos que existen muchos mitos en torno al tema de la invasión de celulares, lo que genera ideas erróneas que alimentan sentimientos de impotencia, angustia y paranoia entre personas que atraviesan situaciones de violencia. A partir de esta experiencia, desarrollamos un contenido que busca desmitificar estas creencias y ofrecer información accesible sobre hackeo y análisis de celulares, procurando un equilibrio entre la gravedad de los riesgos y un enfoque cuidadoso y realista. Esperamos que este material sea útil tanto para quienes enfrentan la violencia digital como para sus redes de apoyo y para las propias líneas de ayuda, que constantemente enfrentan y desmontan estos mitos.

Para producir este contenido, realizamos entrevistas con cuatro líneas de apoyo feministas en cuidados digitales: **Navegando Libres**, de Ecuador; **Luchadoras**, de México; **Maria d'Ajuda**, de Brasil; y **Fembloc**, de Cataluña. En estos encuentros conversamos sobre los mitos que cada línea identificaba, los motivos por los cuales exis-

Te recomendamos volver a revisar el apartado 2 de este cuadernillo y empezar por hacer un análisis manual de tu celular.

> *No paniquees con cada app que no sepas lo que es, seguramente es una aplicación de sistema que tu celular necesita para funcionar. Busca en internet, hay mil foros con personas haciéndose la misma pregunta ;)*

Antivirus como Malwarebytes[17] o Koodous[18] también pueden ser muy útiles a la hora de detectar configuraciones inseguras y software espía no sofisticado. Sin embargo, recuerda que **no van a detectar aplicaciones o funcionalidades que se consideran legítima**s, como por ejemplo: *Family Link* (el control parental de Google) o si estás compartiendo la ubicación a través de la aplicación "Buscar" de iPhone.

> *Evita otros antivirus o aplicaciones que prometen revisar tu dispositivo en busca de software espía. Pueden ser incluso peligrosas. Por ejemplo, desaconsejamos el uso de Incognito[19].*

17 https://www.malwarebytes.com/es/
18 https://koodous.com/product/koodous-mobile
19 https://play.google.com/store/apps/details?id=com.arcane.incognito

do 10 de la Parte 1) y en las que te pueden acompañar las líneas de atención. Aunque estas medidas parezcan aburridas y no tan glamurosas como un análisis forense, tienen mucha más efectividad a la hora de proteger tu vida digital.

→ La **medidas más técnicas**, como puede ser un análisis forense, **no solucionan situaciones de violencia o vigilancia complejas**. Revisa la el apartado 3 de este cuadernillo para ajustar tus expectativas antes de solicitar un análisis.

> *Asegúrate de hacer estos análisis en **servicios de confianza** reconocidos por **organizaciones feministas y que defienden los derechos digitales**. Ten precaución con las estafas. Ninguna línea de atención feminista o para defensores de derechos humanos pide dinero por sus servicios.*

7. Algunas referencias en caso de que el análisis lo quieras hacer tú

Si después de leer este fanzine te quedaste con las ganas de hacer tu propio análisis **¡nos alegramos mucho! ¡Estamos segures de que le hacker puedes ser tú!**

tían esos mitos, los imaginarios que los sostienen, y qué contenidos podrían ser útiles para ayudar a desmontarlos.

Finalmente, decidimos **organizar el contenido en dos partes distintos**, una dedicada a **desmitificar el hackeo de celulares** y otra enfocada en **desmitificar el análisis de celulares**, es decir, el análisis que se hace para detectar señales de hackeo.

El cuadernillo que tienes en tus manos es la parte 2, donde señalamos posibles caminos a seguir en caso de que tu celular haya sido hackeado. También brindamos información sobre en qué consiste un análisis de celular, cuándo debería realizarse, qué puedes esperar de un análisis, cómo generar informes para un análisis más técnico, cómo documentar sospechas y a quién puedes pedir apoyo.

Este fanzine nace como proyecto final de la Fellowship del Center for Digital Resilience de la que fuimos parte entre agosto de 2024 y julio 2025. Fue un trabajo a cuatro manos, con cuatro horas de diferencia ho-

raria, desde dos orillas muy alejadas del océano Atlántico, entre Río de Janeiro y las Islas Canarias.

En este material utilizamos lenguaje neutro y la letra "e" para referirnos a cualquier persona que pueda estar enfrentando una situación de violencia mediada por la tecnología. Esta es una apuesta feminista inclusiva hacia personas trans y no binarias. Esperamos que te sientas cómode al leerlo.

También procuramos evitar el término "análisis forense" porque es un término técnico poco familiar. Preferimos decir "análisis de celulares" para referirnos a cualquier técnica o procedimiento que sirva para detectar un software o configuraciones que permitan espiar o rastrear a una persona.

Esperamos que te guste y te sea útil ♥

Amarelu y Martu

→ **Capturas de pantalla, fotos o vídeos:** Intenta hacer una captura de pantalla, tomar una foto o grabar un vídeo del comportamiento extraño. Guarda esos archivos en un lugar seguro, fuera del celular sospechoso.

6. A quién puedes pedir un análisis de tu celular

Existen varias colectivas que pueden apoyarte en este sentido. Puedes pedir ayuda a cualquiera de las líneas de atención que te mencionamos en el apartado 9 de la Parte 1 de esta fanzine.

Sin embargo, recuerda que:

→ Llevar a cabo un análisis forense de tu celular implica el tiempo y trabajo de personas con conocimiento técnico especializado en este tipo de análisis. **Antes de pedirlo reflexiona si realmente lo necesitas y qué estás esperando de ello**.

→ Ante un incidente seguridad digital, la mayoría de las veces lo que se necesita son **medidas básicas de protección digital** (como las que recomendamos en el aparta-

y haciendo que el **proceso sea más rápido, objetivo y cuidadoso**.

Información importante que deberías documentar:

→ **Cuándo ocurrió:** Anotar cuándo ocurrió cada situación es esencial. Incluso si no recuerdas la hora exacta, una idea aproximada ya ayuda mucho. Esto permite que, en un análisis técnico, se busque en los registros del celular los eventos que ocurrieron en ese período.

→ **Qué ocurrió:** Describe de forma concisa lo que llamó tu atención: comportamientos extraños del celular, notificaciones inesperadas, etc. No es necesario usar lenguaje técnico, lo importante es registrar lo que viste o te pareció raro.

→ **Dónde ocurrió:** Describe en qué aplicación o cuenta notaste algo inusual.

→ **Con qué frecuencia:** Saber si fue un evento aislado o si se volvió recurrente ayuda a identificar el tipo de control o monitoreo. Anota si los síntomas se repitieron y con qué frecuencia.

1. ¿Qué puedo hacer si realmente está pasando algo?

Aunque muchas veces sobrevaloramos el poder y las habilidades tecnológicas de las personas con las que nos relacionamos, mientras subestimamos nuestra propia capacidad de comprender y reaccionar, no podemos ignorar que **vivimos en una estructura social machista y patriarcal**. Esta estructura normaliza el acceso no consentido a la intimidad de mujeres cis y personas trans, atravesando relaciones afectivas, familiares e incluso institucionales. Marca profundamente muchas vivencias, produciendo abusos, vigilancia y formas sistemáticas de control sobre nuestros cuerpos y subjetividades. Es decir, aunque espiar a alguien a través un dispositivo no sea algo tan simple o inmediato, esta es la realidad de muchas personas, ya sea a través de software espía diseñado para contextos afectivos, herramientas de control parental usadas de forma abusiva, o accesos indebidos a cuentas como Google o Apple.

Ante la sospecha de que “algo pasó” en el celular, es común que surjan sentimientos de miedo, inseguridad, vergüenza y confusión. Muchas personas se preguntan:

"¿Estaré exagerando?" o "¿Cómo puedo estar segure?". En ese momento, es importante reflexionar cuidadosamente sobre los **síntomas**[1] que has podido observar en el celular y revisar la **pirámide de probabilidad**[2] de lo que podría haber sucedido. Si después de eso sigues con sospechas e indicios de que "algo pasó", es necesario actuar para preservar tu privacidad y seguridad. Sin embargo, **no hay una única forma de actuar ni un único camino a seguir**, todo dependerá de tus objetivos, tu necesidad emocional, tu urgencia, etc.

Si sientes la necesidad de obtener respuestas más objetivas y deseas **intentar confirmar si realmente hubo espionaje** (por ejemplo, si alguien tuvo acceso remoto a tu celular, instaló apps de monitoreo o accedió a tu cuenta), una posibilidad es buscar apoyo para realizar un **análisis del celular** (análisis forense), que implica una serie de procedimientos orientados a identificar señales de intervención, rastros de actividad, vulnerabilidades de seguridad y otros indicios. La realización de este análisis puede ayudarte a reconstruir lo que ocurrió y entender el nivel de exposición.

1 Ver Parte 1 (6. Qué síntomas son preocupantes y cuáles no)
2 Ver Parte 1 (7. ¿Qué pudo pasar?)

En el caso de necesitar un análisis más profundo del dispositivo se puede pedir: una extracción de apps y SMS con Androidqf, acceso físico al teléfono para hacer una revisión más profunda, u otros métodos de análisis de red que exceden el alcance de este fanzine.

5. Cómo documentar

Documentar sospechas y hechos extraños puede parecer un detalle menor, pero es una herramienta fundamental tanto para quien está viviendo la situación como para quienes van a brindar apoyo. En momentos difíciles, nuestra memoria puede fallar, y anotar lo que ocurrió, con fecha, hora y descripción, permite **registrar los detalles mientras aún están frescos**, organizar los hechos y construir una línea de tiempo. Esto no solo **te ayuda a entender mejor lo que está pasando**, sino que también brinda a los equipos técnicos y de apoyo el **contexto necesario para investigar** de forma más precisa, sin tener que acceder a todo ni revisar datos innecesarios. Además, evita que tengas que repetir muchas veces la misma historia, **reduciendo la exposición emocional**

Cómo generar un Google Takeout

Paso 1. Haz *login* en tu cuenta de Google y accede a *takeout.google.com.*

Paso 2. Haz clic en "Desmarcar todo" y marca sólo las opciones que consideres necesarias. Generalmente son interesantes:

- Alertas,
- Actividad de registro de acceso,
- Auenta de Google,
- Google Play,
- Aronología,
- Mi actividad, y
- Perfil.

Paso 3. Haz clic en "Siguiente paso" y selecciona:

- Enviar enlace de descarga por correo electrónico.
- Exportar una vez.
- Tipo de archivo: .zip.

Paso 4. Después de unos minutos te llegará un correo electrónico con el enlace para descargar el archivo.

Si sientes que no necesitas analizar técnicamente lo que pasó, ya sea por agotamiento emocional, miedo a escalar la situación o simplemente porque **solo quieres seguir adelante**, puedes saltarte la parte del análisis y **centrarte en medidas de seguridad**. Muchas veces, lo más importante es recuperar tu seguridad y autonomía, independientemente de obtener una prueba concreta de lo ocurrido.

> *No hay un camino mejor que otro. Y sea cual sea, te recomendamos buscar ayuda de profesionales y activistas con experiencia en el área y, de preferencia, que trabajen desde una perspectiva feminista, con un enfoque centrado en el cuidado, la privacidad de los datos, además de sensibilidad para tratar contextos de violencia de género. Al buscar ayuda, ten cuidado con supuestos hackers y servicios técnicos[3] genéricos. En el apartado 9 de la Parte 1 y en el apartado 6 de este cuadernillo compartimos información sobre* ***cómo y dónde pedir ayuda de forma confiable****.*

Si deseas tomar **medidas de emergencia básicas de forma independiente**, antes de buscar ayuda, aquí van algunas recomendaciones:

3 Ver Parte 1 (8. Precauciones con supuestos hackers y servicios técnicos)

1. Cambia tus contraseñas y revisas los métodos de recuperación: Desde un dispositivo seguro, cambia las contraseñas de tus cuentas más importantes, como el correo electrónico —especialmente el que usas en tu celular (Android)—, tu cuenta de Apple, tus redes sociales y tus bancos. Usa **contraseñas complejas y únicas** para cada servicio, y utiliza un gestor de contraseñas confiable como KeepassXC[4] o Bitwarden[5] para guardarlas. No olvides revisar los métodos de recuperación de contraseñas (utiliza correos y números de celular a los que tengas acceso y sean seguros).

2. Configura la autenticación de dos factores: Activa la autenticación en dos o más pasos en todas las plataformas que ofrezcan esta opción, añadiendo una capa extra de seguridad que dificulta accesos no autorizados. Como método de autenticación, **prioriza usar aplicaciones** (como Aegis[6], por ejemplo) en lugar de SMS, siempre que sea posible. El SMS es una opción más vulnerable, ya que puede ser interceptado o inaccesible si no tienes red o estás en otro país.

4 https://keepassxc.org/
5 https://bitwarden.com/
6 https://getaegis.app/

También puedes generar el sysdiagnose con la funcionalidad **“Tocar”** o **“AssistiveTouch”**:

- **Paso 1**. Ajustes > Accesibilidad > Tocar > AssistiveTouch > Activar. Ahora verás un nuevo botón blanco en tu pantalla que tiene funcionalidades de accesibilidad.
- **Paso 2**. En Personalizar menú flotante > Añadir ícono. Presionar en el ícono añadido que ahora se ve con un “+”. Selecciona de la lista “Análisis” > OK
- **Paso 3**. Ahora si le das al nuevo botón blanco verás que tiene una nueva funcionalidad: “Análisis” > presiona en ella y verás una notificación que dice “Recopilando análisis”. Espera unos seguros a que termine.
- **Paso 4**. Si después de generar el sysdiagnose quieres quitar el nuevo botón blanco, vuelve a Ajustes > Accesibilidad > Tocar > AssistiveTouch > Desactivar.

La documentación de Apple ofrece una guía visual[16] de cómo hacerlo.

*Los archivos de sysdiagnose y bug report **no** contienen información personal como fotos, vídeos, contactos, mensajes, etc., pero sí información sobre las aplicaciones instaladas y otros detalles de tu dispositivo. **Envíalos a través de un medio seguro**.*

16 https://it-training.apple.com/tutorials/support/sup075/

***En Xiaomi es diferente**, tendrás que ir a Ajustes > Sobre el teléfono > Todas las especificaciones > pulsar cinco veces sobre los detalles de la CPU > Verás una notificación de que se está generando el informe (puede tardar varios segundos).*

*Al terminar el proceso **no olvides desactivar las "Opciones para desarrolladores"** en Ajustes > Opciones para desarrolladores > Desactivar.*

Como generar un sysdiagnose (iPhone)

En el caso de iPhone el informe de errores para el análisis se llama "sysdiagnose" y se genera y extrae así:

- **Paso 1**. Presiona a la vez los **botones de volumen y encendido** (los tres a la vez) por uno o dos segundos.
- **Paso 2**. Cuando dejes de apretar **sentirás una vibración corta**, significa que el sysdiagnose se empezó a generar.
- **Paso 3**. **Espera unos segundos** hasta que el archivo se termine de generar.

Para encontrar tu sysdiagnose ve a Ajustes > Privacidad y Seguridad > Análisis y mejoras > Datos de análisis > Buscar: sysdiagnose. Debes ver un archivo que se llame **sysdiagnose-año-mes-día-hora-xxxx.tar.gz**.

3. Revisa y revoca accesos en tus cuentas: Es importante verificar desde dónde y en qué dispositivos están conectadas tus cuentas, y cerrar el acceso de cualquier dispositivo sospechoso, desconocido o innecesario. Si alguien accedió indebidamente a tu cuenta, es posible que siga conectado en segundo plano incluso si cambiaste la contraseña. Por eso es esencial **revocar directamente los accesos**.

4. Activa y usa Google Play Protect (Android): Google Play Protect es un sistema de seguridad nativo de Android diseñado para detectar apps potencialmente maliciosas instaladas desde la Play Store o fuentes externas. Ve a la **Play Store**, entra en "**Play Protect**" y realiza un escaneo manual del dispositivo. Asegúrate de que la **opción de verificación de amenazas esté activada**, permitiendo que el sistema monitorice el comportamiento de las apps y alerte sobre actividades sospechosas.

5. Revisa detalladamente las apps instaladas: Haz una revisión minuciosa de la lista de apps en tu dispositivo, identificando y eliminando las que sean **desconocidas o innecesarias**. Además, examina cuidadosamente los **permisos concedidos** a cada aplicación, especial-

mente los sensibles como acceso a ubicación, cámara y micrófono. **Revoca cualquier permiso** que no sea estrictamente necesario para el funcionamiento legítimo de la app.

6. Actualiza el sistema y las aplicaciones: Asegúrate de que el **sistema operativo** y **todas las apps** estén actualizadas con los últimos **parches de seguridad**. Las actualizaciones corrigen **fallos de seguridad que podrían ser utilizados para vulnerar el dispositivo**.

7. Restablece valores de fábrica: Cuando restableces el celular se eliminan todas las aplicaciones y datos del celular, vuelve al estado inicial, igual a cuando salió de la fábrica. Esto implica que **cualquier aplicación o configuración utilizada para espiar se eliminará** del celular. Es una forma "radical" pero muy efectiva de eliminarlo todo.

- En Android: Ajustes > Sistema > Opciones de recuperación > Volver al estado de fábrica (puede variar según el fabricante)
- En iOS: Ajustes > General > Transferir o restablecer el iPhone > Borrar contenidos y ajustes

del software > pulsa siete veces seguidas el "Número de compilación" hasta que veas "You are now a developer!" (la manera de llegar a ver el "Número de compilación" puede ser diferente, dependiendo del modelo de celular[15]).

- **Paso 2**. Vuelve a Ajustes y ahora verás una nueva opción llamada "Opciones de desarrollador". Presiona **"Informe de errores"** o "*Bug report*".
- **Paso 3**. Selecciona **"Informe completo"** y presiona "Informar".
- **Paso 4**. **Después de unos segundos** se te notificará que está listo el informe de errores. Para compartirlo, **presiona la notificación** o búscalo en tu gestor de archivos. Debería tener el nombre "**bugreport-año-mes-día-hora.zip**".

Este método funciona para **Google Pixel, Motorola, Samsung y algunos otros fabricantes**. Si para tu teléfono no funciona, busca en internet "*how to generate bug report* [tu modelo de celular]"

15 https://developer.android.com/studio/debug/dev-options?hl=es-419

pueden ofrecer un análisis inicial, orientaciones técnicas y, sobre todo, acompañamiento y apoyo.

4. Cómo generar los archivos necesarios para un análisis

Para hacer análisis (forenses) a celulares se necesitan, principalmente, los siguientes archivos:

- **Bug report** (en el caso de Android),
- **Sysdiagnose** (en el caso de iPhone), o
- **Google Takeout** (en el caso de Android o cuentas de Google).

A continuación te explicamos cómo generar y extraer estos archivos.

Cómo generar un *bug report* (Android)

En Android el informe de errores para el análisis se llama "*bug report*" o "informe de errores". Hay varias formas de extraerlo. Dependiendo del fabricante, la forma más habitual es:

- **Paso 1. Habilita las "Opciones para desarrolladores"**: Ve a Ajustes > Información del teléfono > Información

Pero **recuerda**:

- Se **eliminarán todas tus fotos, vídeos, conversaciones y otros datos** que tengas en el celular, elige lo que quieras conservar y guárdalo en un ordenador o nube segura, pero no uses las opciones de "copia de seguridad" ya que en ella se podría conservar el posible *malware* u otras configuraciones;
- Se perderá cualquier prueba de cara a un proceso judicial (si no tienes pensado iniciar este proceso, no consideres esta advertencia);
- Restablecer el celular **no bloquea posibles accesos no autorizados a tus cuentas de Google o Apple**, para ello tendrás que cambiar la contraseña, activar 2FA, configurar métodos de recuperación seguros y revocar los inicios de sesión.

Fíjate también en los consejos rápidos que damos en el apartado 10 de la Parte 1 para que la persona hacker seas tú ;)

2. En qué consiste un análisis del celular

Aquí venimos a contarte qué se suele hacer para revisar un celular y tratar de descubrir si tiene *software* espía, u otras aplicaciones o configuraciones que se pueden usar para espiar.

Revisiones manuales

En **primer lugar**, se suele hacer una **revisión manual de aplicaciones**. Es decir, ir al listado de aplicaciones del celular y verificar una por una:

- ¿Es una aplicación del fabricante del teléfono o fue instalada por la persona usuaria del celular?
- ¿Para qué sirve la aplicación?
- ¿Qué permisos tiene? ¿Tiene sentido para la funcionalidad de la aplicación?

Cuando hay dudas se busca en internet el nombre de la aplicación, también se pueden usar las webs *immuniweb.com* y *reports.exodus-privacy.eu.org* para tener más información.

Cuándo el análisis puede ayudar — y cuándo no es recomendable

Puede ser útil cuando...	Puede que no sea el mejor camino si...
Sospechas que instalaron una app espía en tu celular.	Estás en riesgo inmediato.
Tienes indicios sólidos de que alguien accede a tus cuentas de Google sin autorización (revisión de Google Takeout).	No te sientes emocionalmente preparade para lidiar con el proceso y con lo que pueda surgir.
Necesitas recuperar registros que puedan ayudarte a recordar o probar algo.	Solo quieres seguir adelante sin revivir detalles de la situación.
Quieres entender mejor lo que ocurrió para tomar decisiones con mayor claridad.	Esperas que el análisis traiga "pruebas definitivas" (no siempre es posible).
Estás considerando hacer una denuncia o buscar apoyo legal y quieres fortalecer tu caso con más información.	Ya tomaste medidas de seguridad y te sientes segure con eso.

Importante recordar:

No todas las líneas de ayuda feminista hacen peritajes oficiales con informes que puedan usarse como pruebas en juicios, pero

Por eso, es fundamental que la decisión de realizar o no el análisis sea tomada con cuidado, de manera informada, tomándose el tiempo necesario y respetando las necesidades emocionales. **No siempre este es el paso más urgente o necesario**, y siempre se debe tener en cuenta el bienestar y la autonomía. El análisis del celular es solo una herramienta más dentro de un conjunto más amplio de estrategias para enfrentar la violencia digital. La mayoría de veces, fortalecer las medidas básicas de seguridad digital y recibir apoyo son los pasos prioritarios para retomar el control de la situación.

En resumen, el análisis técnico es más indicado cuando las sospechas son sólidas, cuando los intentos básicos de protección (cambiar contraseñas, revisar permisos, actualizar el sistema) no resolvieron el problema, cuando hay un objetivo claro de documentar lo que está ocurriendo, o cuando se quiere obtener pruebas de cara a un proceso judicial. Fuera de estos casos, enfocarse en fortalecer la seguridad digital y emocional suele ser más importante, más efectivo y menos desgastante.

En Android, también se verificará si Google Play Protect[7] está activado y si la instalación de apps desconocidas no está activada para ninguna aplicación, en especial para el navegador o gestor de archivos.

Además, se suele preguntar a la persona si recibió enlaces sospechoso por SMS , Whatsapp u otra plataforma y revisarlo. Para comprobar enlaces se suele usar *virustotal.com.*

También se revisan las funcionalidades de control parental (como Google Family Link) o de compartir ubicación, que no se identificarían como software espía o virus pero que se podrían usar para vigilar a una persona.

Escaneo con antivirus

En **segundo lugar**, se puede hacer un **escaneo del celular con un antivirus recomendado**, como Malwarebytes[8] o Koodous[9]. Estos antivirus son capaces de detectar fácilmente software espía utilizado en relaciones afectivas y configuraciones inseguras como la "instalación de apps de fuentes desconocidas" activada.

7 https://support.google.com/android/answer/2812853?hl=es
8 https://www.malwarebytes.com/es/
9 https://koodous.com/product/koodous-mobile

Análisis de informes de errores

En **tercer lugar**, si se sigue teniendo sospechas de una posible intervención del dispositivo, se puede hacer un **análisis del informe de errores del dispositivo**. En Android al informe de errores se le llama *bug report* y en iPhone se le dice *sysdiagnose*.

Para hacer este análisis, el equipo de atención te dará las instrucciones para sacar el informe de errores de tu dispositivo y enviarlo. Estos informes contienen información sobre las aplicaciones instaladas, los permisos que tienen, cuándo se instalaron, cuándo se iniciaron, los procesos del sistema, el uso de batería, errores que han ocurrido y detalles técnicos sobre el dispositivo y sus configuraciones. Estos informes no tienen fotos, vídeos, mensajes o chats, ni tampoco configuraciones específicas de cada aplicación.

El análisis de estos informes no es magia y sus **resultados no son mágicos**. La herramienta que se suele usar para analizar estos informes de errores es MVT[10] (Mobile Verification Toolkit), desarrollada por Amnistía Internacional, como funciones de protección desactivadas, por ejemplo.

- Si la cuenta vinculada al celular está siendo accedida desde otro dispositivo, posibilitando así el monitoreo de diversas actividades, como el uso de aplicaciones, búsquedas en Internet, ubicación, etc. En este caso no se analizaría el celular sino los datos que nos pueda ofrecer esa cuenta. Para cuentas de Google será muy útil revisar el contenido de "Google Takeout".

A pesar de estos beneficios potenciales, es importante recordar que el análisis técnico del celular **no garantiza respuestas definitivas en todos los casos**. Las tecnologías de vigilancia pueden ser muy sofisticadas y dejar pocos rastros, y **el hecho de no encontrar nada no significa que no esté ocurriendo algo**, lo que puede generar frustración, causar paranoia, o incluso una falsa sensación de seguridad. El proceso también puede ser **emocionalmente desafiante**, e intensificar sentimientos de ansiedad, inseguridad e incluso miedo, especialmente si los resultados del análisis son inconclusos o difíciles de interpretar.

10 https://docs.mvt.re/en/latest/

caso será único y cada línea de atención tendrá su abordaje a la hora de llevar a cabo análisis de celulares.

3. Qué puede hacer un análisis del celular por mí (y qué no)

El análisis del celular puede ser un recurso valioso para **identificar señales de violencia digital**, y cuando se realiza con cuidado, por personas o colectivos que actúan con responsabilidad y un enfoque feminista, puede ofrecer más que pruebas: puede traer alivio, confirmar sospechas o simplemente ayudar a ponerle nombre a una sensación de inseguridad que hasta entonces parecía demasiado vaga como para explicarla. Técnicamente, el análisis puede revelar una serie de cosas, como por ejemplo:

- Si se instaló algún *software* con capacidades de espionaje y cuándo sucedió. En algunos casos, incluso es posible determinar quién desarrolla el software y los servidores que utiliza para operar.
- Si se realizaron modificaciones o configuraciones que puedan indicar intentos de vulnerar el dispositivo.

cional y orientada a la detección de software espía en celulares de personas defensoras de derechos humanos. Estos análisis pueden detectar software espía utilizado en relaciones afectivas (no sofisticado) - a través de una revisión automatizada de apps - y también algunos programas espías sofisticados, pero con limitaciones.

MVT funciona con "Indicadores de Compromiso" (en Inglés *Indicators of Compromise*, IOC), que básicamente son elementos que se consideran sospechosos y que se asocian a un posible software malicioso (por ejemplo urls, nombres de procesos, errores, etc). Amnistía Internacional y otras organizaciones se dedican a definir estos IOC después del estudio del software espía que van encontrando en investigaciones y que la comunidad va reportando. Sin embargo, el ecosistema del software espía, especialmente el más sofisticado, es bastante opaco. Por lo tanto los IOCs que valía paran detectar un *Pegasus* hace unos meses quizás no valgan hoy.

En algunas ocaciones, después de un análisis del informe de errores del dispositivo se puede considerar necesario un análisis más profundo del dispositivo que im-

plique acceso físico o el uso de herramientas de extracción de aplicaciones como Androidqf[11].

Análisis de Google Takeout

En **cuarto lugar**, en casos de dispositivos Android y/o sospecha de acceso a cuentas de Google puede ser muy pertinente el **análisis de datos de Google Takeout**[12]. Este análisis consistirá en pedir a Google datos sobre la cuenta que se quiera analizar, a través de su formulario en *takeout.google.com.*

Google envía un archivo .zip con toda la información que se le haya solicitado sobre la cuenta (como cambios de contraseña o recuperación de cuenta), Google Play (como aplicaciones instaladas y suscripciones), dispositivos en los que se configuró la cuenta, dispositivos que iniciaron sesión (incluyendo IP y región), datos de navegación en Chrome (búsquedas y urls visitadas), búsquedas y descargas de Google Drive y mucho más.

11 https://github.com/mvt-project/androidqf/
12 https://es.wikipedia.org/wiki/Google_Takeout

Este análisis puede ser muy extenso, por eso es muy importante **definir franjas de tiempo**, días u horas concretas a revisar.

Análisis de tráfico

Finalmente, queremos contarte que para casos de sospecha de software espía sofisticado también se hacen **análisis de red del dispositivo**. Básicamente consiste en capturar el tráfico de red dispositivo y analizarlo para ver si se están enviando datos a servidores que se consideran sospechosos. Para ello se te puede pedir conectarte a una red o VPN determinada (que capturará tu tráfico para ser analizado) o capturar el tráfico tu misme con alguna herramienta como **PCAPdroid**[13] y luego mandarlo a analizar. **PiRogue**[14] es una herramienta que sirve para hacer este tipo de análisis.

> ***Aquí solo pretendemos ofrecer una visión general sobre el análisis de celulares y hacerlo algo más comprensible***. *Por supuesto, esto no es una guía sobre cómo hacer análisis forense de celulares, ni pretende definir cómo se tienen que hacer. Cada*

13 https://play.google.com/store/apps/details?id=com.emanuelef.remote_capture&hl=es_VE
14 https://pts-project.org/docs/pirogue/overview/