BIBLIOTECA
ACCCF

13
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Sospecha de vigilancia digital: guía de comprobación y preservación con Zero Breach Toolkit

Crisis, falsos indicios, descarga verificada, privacidad, lectura del reporte y entrega pericial

Ayudar a una persona preocupada a comprobar indicios sin destruir evidencia ni instalar otro riesgo, con pasos simples y un anexo reproducible para quien revise el caso.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

Guía técnica general. Ejemplos y cifras de demostración son ficticios.

Contenido

Índice navegable. Los títulos enlazan a su ubicación dentro del documento.

1. Antes de tocar nada: seguridad y calma . . . 4

2. Comportamientos normales que pueden parecer espionaje . . . 5

2.1 Una señal no es una explicación . . . 5

2.2 Falso positivo no significa imaginación . . . 5

3. Qué hace Zero Breach y cuándo no usarlo . . . 6

3.1 Una comprobación local de indicios publicados . . . 6

3.2 Cuándo detenerse y pedir ayuda . . . 6

4. Descarga y verificación del paquete . . . 7

4.1 Repositorio oficial, no enlaces reenviados . . . 7

4.2 Verificación del ejecutable de Windows . . . 7

4.3 Alternativa: código fuente y comparación reproducible . . . 8

5. Privacidad y preparación antes de ejecutar . . . 8

5.1 Local no significa inofensivo . . . 8

5.2 Preparación de la carpeta y del alcance . . . 8

5.3 Vista previa y descripción . . . 9

6. Ejecución paso a paso . . . 9

6.1 Primero: practica sin examinar un dispositivo real . . . 9

6.2 Después: revisión local autorizada . . . 9

6.3 Si eliges un teléfono . . . 10

7. Cómo leer el reporte antes de compartirlo . . . 10

7.1 Resultado, grado, alcance y huecos . . . 10

7.2 Códigos y significado operativo . . . 11

7.3 “Worth a look” no es una sentencia . . . 11

8. Los cuatro escenarios del laboratorio . . . 12

8.1 `spyware`: seis hallazgos, ninguna conclusión apresurada . . . 12

8.2 `worth-a-look`: elementos para preguntar, no para acusar . . . 12

8.3 `clean`: ausencia de coincidencias con cuatro huecos . . . 13

8.4 `cellebrite`: acceso forense, no spyware . . . 13

9. Entrega segura al perito o al equipo de respuesta . . . 17

9.1 Primero el resumen, después el expediente completo . . . 17

9.2 Hash y EML para una entrega verificable . . . 18

9.3 La explicación que evita una segunda crisis . . . 18

Anexo A. Protocolo reproducible para el perito . . . 18

A.1 Registro del entorno y de la procedencia . . . 19

A.2 Ficha para una ejecución real autorizada . . . 19

A.3 Matriz de interpretación . . . 19

Anexo B. Marco jurídico, privacidad y control final . . . 20

1. Antes de tocar nada: seguridad y calma

Si crees que alguien vigila tu teléfono o tu computadora, lo primero no es descargar un programa. Es evitar que la prisa te haga perder información o crear otro problema. No borres archivos, no restablezcas el dispositivo, no instales suites milagrosas y no permitas que un desconocido controle el equipo por acceso remoto. Una preocupación puede nacer de algo legítimo, de una configuración o de un incidente real. Todavía no lo sabemos y no necesitamos decidirlo en este minuto.

Si hay amenaza física, riesgo para menores, una persecución activa o una persona que puede descubrir que estás pidiendo ayuda, prioriza la seguridad y los canales de emergencia de tu localidad. No ejecutes una comprobación solo porque esta guía existe. Un análisis puede cambiar registros, ocupar espacio o avisar indirectamente a alguien que controla el entorno. Pide ayuda desde un dispositivo y un canal seguros antes de seguir.

Haz una lista pequeña: qué observaste, cuándo empezó, qué cambió, qué instalaste, quién tuvo acceso físico y qué cuentas podrían estar comprometidas. Usa horas aproximadas si no recuerdas las exactas. No captures ni reenvíes contenido íntimo para pedir ayuda. Un mensaje, una URL, una configuración, un nombre de aplicación y una fecha suelen ser más útiles que una carpeta entera de tu vida privada.

Lo necesario antes de lo posible

Respira. No borres, no persigas al supuesto atacante y no compartas contraseñas ni códigos. Si hay peligro, pide ayuda ahora. Si hay tiempo, conserva lo mínimo y comprueba sin dramatizar. Duriva te hará esta pregunta varias veces: ¿qué puedes demostrar y qué solamente parece posible?



Figura 1. Antes de comprobar, evita perder la fuente. La prioridad no es demostrar que tenías razón Reconstrucción editorial; no constituye evidencia real.

2. Comportamientos normales que pueden parecer espionaje

2.1 Una señal no es una explicación

Una dirección MAC distinta, una desconexión, una batería que baja rápido, una notificación inesperada, una aplicación desconocida o una dirección IP nueva no demuestran por sí solos que alguien te vigila. Pueden tener causas de privacidad, actualización, cobertura, sincronización, una aplicación legítima o una cuenta compartida. También pueden formar parte de algo más serio. El error es escoger la explicación más alarmante antes de revisar la fuente.

Apple documenta que sus dispositivos pueden utilizar direcciones Wi-Fi privadas distintas por red y, con el modo Rotating en sistemas compatibles, cambiarlas cada dos semanas. Esta función busca reducir seguimiento, no demostrar espionaje. Una desconexión es otra pregunta: puede involucrar router, cobertura, actualización, compatibilidad, energía, software o configuración empresarial. No le atribuyas una sola causa sin revisar.[1]

Lo que observas	Primera comprobación tranquila	Qué conservar para revisar
La MAC cambió	Revisa la configuración de dirección privada por red y el modelo/sistema.	Captura de configuración, red y fecha; no el historial entero.
Se desconecta	Anota frecuencia, otros dispositivos, cobertura, hora y cambios recientes.	Modelo, sistema, router, patrón y errores; no contraseña Wi-Fi.
Batería baja rápido	Revisa consumo por app, señal, temperatura y actualizaciones.	Estadísticas del sistema y período, no contenido de chats.
Mensaje duplicado	Comprueba sincronización, otros dispositivos y cuentas vinculadas.	Aplicación, versión, hora, cuentas y mensaje de contexto.
Alerta de seguridad	Lee qué archivo o conducta detecta y qué versión de la herramienta existe.	Alerta completa, ruta, fecha y explicación; no ejecutes el archivo.
Actividad nocturna	Distingue actualizaciones, respaldos, tareas y acceso físico.	Registros, estado de bloqueo y quién tenía el dispositivo.

2.2 Falso positivo no significa imaginación

Un falso positivo es una alerta que no representa el problema que se temía, pero no toda conducta extraña es un falso positivo y no todo resultado sin hallazgos lo es. La persona no necesita que le digan que imagina cosas: necesita saber qué comprobación cambiaría la interpretación. Si una configuración explica el dato, se documenta. Si no la explica, se sigue investigando sin culpa ni conclusiones apresuradas.

> **La frase correcta**
>
> “Esto puede tener una explicación normal. Voy a comprobarla antes de llamarlo espionaje.” Y también: “Si la explicación no encaja, conservaré la fuente para que alguien cualificado la revise.”

Una señal no es una explicación

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Primero se comprueba; después se interpreta

Observación	Explicación posible	Comprobación
MAC distinta	Dirección privada por red o rotación.	Configuración, modelo y fecha.
Desconexión	Cobertura, router o actualización.	Patrón, otros equipos y registros.
Batería baja	Aplicaciones, señal o temperatura.	Consumo por app y período.
Mensaje duplicado	Sincronización o dispositivos vinculados.	Cuenta, versión y otras sesiones.
Alerta de seguridad	Falso positivo o indicio relevante.	Objeto, versión y fuente original.

La figura explica decisiones y relaciones; no representa evidencia de un caso real.

Figura 2. Una señal no es una explicación. Primero se comprueba; después se interpreta Reconstrucción editorial; no constituye evidencia real.

3. Qué hace Zero Breach y cuándo no usarlo

3.1 Una comprobación local de indicios publicados

Zero Breach Toolkit es una herramienta gratuita y de código abierto que busca indicadores documentados de ciertos spywares en computadoras, colecciones Android y respaldos de iPhone. Puede revisar archivos, navegadores, registros de persistencia y otros artefactos soportados. No es una pericial completa, no descubre cualquier vigilancia y no demuestra que una persona esté segura por no encontrar nada.[23]

La herramienta es especialmente útil cuando quieres una primera lectura local de indicios conocidos y una lista explícita de lo que no pudo revisar. Su valor no es decir “no hay duendes”, sino separar coincidencias, referencias débiles, huecos y preguntas para un especialista. Las fuentes nuevas o desconocidas no aparecen mágicamente en una base de indicadores publicados, y algunos rastros desaparecen con el tiempo.

3.2 Cuándo detenerse y pedir ayuda

No ejecutes una comprobación si puede ponerte en peligro, si no tienes autorización sobre el dispositivo o los archivos, si otra persona puede observar el proceso o si no puedes proteger el reporte. Tampoco la uses para revisar el equipo de tu pareja, empleado, cliente o familiar sin permiso. La capacidad de leer un archivo no te convierte en titular autorizado de su contenido.

Si ya existe una notificación de seguridad creíble, una extracción confirmada o una preocupación de targeting, busca ayuda especializada sin terminar antes tu propia revisión. Periodistas, activistas, defensores de derechos humanos y sociedad civil pueden acudir a la línea de ayuda de Access Now o a

Amnesty International Security Lab, cuyos enlaces aparecen en el propio reporte. Para cualquier otra persona, un respondedor de incidentes o un perito cualificado es la ruta adecuada.[4]

Situación	Qué hacer primero	Qué evitar
Curiosidad por comportamiento extraño	Revisar configuración y cronología antes de escanear.	Instalar muchas herramientas al azar.
Sospecha razonable y entorno seguro	Comprobación local con alcance y privacidad definidos.	Compartir el reporte completo en un grupo.
Peligro o vigilancia activa	Ayuda especializada y dispositivo/canal seguro.	Ejecutar pruebas que puedan delatar la consulta.
Equipo de otra persona	Autorización expresa y alcance documentado.	Leer contenido solo porque está accesible.
Prueba de una guía o curso	Escenarios sintéticos incorporados, no dispositivos reales.	Presentar entrenamiento como detección real.

> **No necesitas convertirte en hacker**
>
> No hay que hacer un test point, entrar por procesador ni realizar chip-off. Si una comprobación sencilla no responde, se preserva y se escala. La complejidad técnica no es un requisito para pedir ayuda.

4. Descarga y verificación del paquete

4.1 Repositorio oficial, no enlaces reenviados

El origen utilizado en esta guía es `github.com/interplains/Zero-Breach-Toolkit`. Desde ahí se abre la sección Releases para descargar el paquete correspondiente a Windows, macOS o Linux o el código fuente. No descargues un archivo con el mismo nombre desde un video, un acortador, una captura o un comentario. Un nombre idéntico no demuestra que sea el mismo contenido.[5]

La documentación del proyecto indica que el programa de Windows no está firmado con un certificado de código. Por eso SmartScreen o un antivirus puede advertirte. No desactives protecciones ni aceptes el archivo por fe ciega. El proyecto ofrece atestación del flujo de construcción y, para programas recientes, manifiestos SHA-256 firmados. Verifica antes de ejecutar.[6]

4.2 Verificación del ejecutable de Windows

Con GitHub CLI instalado y el ejecutable descargado en la carpeta actual, la documentación propone esta comprobación de procedencia:

Verificación de atestación, no de ausencia de malware

```
gh attestation verify zero-breach-toolkit-windows-x64.exe --repo interplains/Zero-Breach-Toolkit
```

Una atestación correcta relaciona esos bytes con un flujo público de construcción y un commit. No demuestra que el programa esté libre de errores ni que sea adecuado para tu situación. También puedes usar los manifiestos SHA-256 firmados descritos por el proyecto. No uses un hash encontrado en otra página como si fuera el de tu archivo: calcula el tuyo y compáralo con la fuente oficial correspondiente a esa versión.

4.3 Alternativa: código fuente y comparación reproducible

La otra ruta es clonar el repositorio, revisar el código y comparar el archivo Python generado con la versión esperada. El proyecto describe la compilación determinista del archivo único y las verificaciones de publicación. Para una persona no técnica no es obligatorio compilar: puede pedir ayuda para verificar el paquete o usar la opción de práctica del menú. Lo que no debe hacer es saltarse la identidad del origen por tener prisa.

Ejemplo de obtención del código oficial

```
git clone --depth 1 https://github.com/interplains/Zero-Breach-Toolkit.git
```

> **Duriva pregunta**
>
> ¿De dónde salió exactamente ese ejecutable? Si no puedes responder con repositorio, versión y verificación, todavía no es momento de ejecutarlo.

5. Privacidad y preparación antes de ejecutar

5.1 Local no significa inofensivo

El análisis ordinario está diseñado para no subir tus datos ni visitar indicadores. La actualización de listas sí usa red y la adquisición de Android descarga un colector separado con consentimiento y cambia el estado del teléfono. Además, el bloqueo interno de red no es un sandbox del sistema operativo: montajes de red, otras aplicaciones y sincronización siguen existiendo. Si necesitas aislamiento estricto, decídelo con un especialista.[7]

El reporte puede contener nombre de usuario, perfiles, rutas, historial, remitentes de SMS y extractos de mensajes. El resumen para compartir contiene menos información, pero no es una pericial completa ni debe publicarse sin revisión. Elige una carpeta local no sincronizada, evita OneDrive, iCloud, Dropbox y carpetas compartidas y decide quién podrá abrir el informe. No envíes claves, cookies, contraseñas ni archivos personales al repositorio.

5.2 Preparación de la carpeta y del alcance

Decisión	Qué elegir	Por qué
Carpeta de salida	Local, nueva, no sincronizada y de acceso restringido.	Evita filtrar historial y rutas.
Primera ejecución	Escenario de práctica o alcance limitado.	Aprende el reporte sin inventar un caso real.
Actualización de indicadores	Paso separado y consciente, no confundir con escaneo.	La red y las fuentes cambian.
Aplicaciones abiertas	Cierra navegadores y mensajería si el procedimiento lo pide.	Reduce archivos bloqueados y cambios concurrentes.
Permisos	Solo los necesarios; no elevar por costumbre.	Evita revisar otras cuentas o cambiar configuración.
Persona que recibe resultados	Destinatario y canal seguro antes de crear el archivo.	Evita compartir por impulso después.

5.3 Vista previa y descripción

Antes de analizar datos reales puedes pedir una vista del alcance y de las comprobaciones disponibles. `--preview` presenta el alcance sin escanear; `--describe` devuelve en JSON qué lecturas existen y cuáles son sus límites. Estos pasos ayudan a decidir si una comprobación responde a la pregunta y si existe una alternativa menos intrusiva.[8]

Descripción del alcance y de las lecturas

```
python -X utf8 scan/zero-breach-toolkit.py --preview
python -X utf8 scan/zero-breach-toolkit.py --describe
```

> **Antes de continuar**
>
> Si el alcance incluye datos que no necesitas compartir, reduce la selección. Si la preocupación exige ayuda, no la pospongas por completar estos pasos. La herramienta es una opción, no una obligación.

6. Ejecución paso a paso

6.1 Primero: practica sin examinar un dispositivo real

El proyecto incluye escenarios creados para aprender: `spyware`, `worth-a-look`, `clean` y `cellebrite`. Usan un teléfono e indicadores inventados, con dominios `.invalid` que no pueden pertenecer a una infraestructura real. El informe lleva una advertencia visible de entrenamiento y el directorio temporal se elimina al terminar. No generan un resumen para compartir ni un paquete de evidencia porque nadie debería confundirlos con un caso real.[9]

Cuatro escenarios de práctica

```
python scan/zero-breach-toolkit.py --training spyware
python scan/zero-breach-toolkit.py --training worth-a-look
python scan/zero-breach-toolkit.py --training clean
python scan/zero-breach-toolkit.py --training cellebrite
```

Si usas el lanzador de Windows, busca la opción de práctica en el menú; la documentación la identifica como `Practise`. Si usas código fuente, ejecuta los comandos desde la carpeta del repositorio. No combines `--training` con archivos, teléfonos, actualizaciones ni listas reales: el programa lo rechaza por diseño. Aprende primero dónde aparecen el resultado, los grados de evidencia y los huecos.

6.2 Después: revisión local autorizada

Cuando la fuente esté verificada, la autoridad sea clara y la carpeta de salida esté protegida, puedes ejecutar una revisión del alcance elegido. No uses `--quick` si quieres evitar una cobertura incompleta deliberada. Si eliges un objetivo específico, selecciónalo conscientemente: una revisión específica no equivale a revisar todo el dispositivo.

Ejemplo de ejecución con reporte, JSON y resumen mínimo

```
python -X utf8 scan/zero-breach-toolkit.py --report reporte.txt --json reporte.json --share-json resumen.json
```

El informe de texto sirve para leer, el JSON para revisar estructura y el resumen para una primera conversación con menos exposición. Ninguno demuestra autenticidad del dispositivo ni prueba que todo el sistema haya quedado examinado. No combines el entrenamiento con `--share-json` ni con un

paquete de evidencia: solo se generan para una revisión real autorizada.

6.3 Si eliges un teléfono

Una colección Android y una revisión de respaldo de iPhone no son lo mismo. La herramienta lee artefactos disponibles y declara lo que no puede acceder. Una adquisición cambia el estado del teléfono y guarda información privada; no la realices sin consentimiento explícito, un destino seguro y comprensión de la cobertura. La copia local puede necesitar contraseña o descifrado separado; no la compartas ni la subas a servicios de análisis.[10][11]

> **No hay botón de verdad**
>
> Si no sabes qué alcance acabas de elegir, detente. La respuesta no está en pulsar “full”, sino en saber qué se revisó y qué no pudo revisarse.

7. Cómo leer el reporte antes de compartirlo

7.1 Resultado, grado, alcance y huecos

Lee cuatro cosas antes que cualquier cifra: qué afirma el resultado, qué grado de evidencia tiene, qué alcance se revisó y qué quedó fuera. El mismo número puede significar cosas distintas según la fuente. Seis hallazgos no son seis infecciones, cero hallazgos no es ausencia de vigilancia y una referencia no es un archivo malicioso en ejecución.

Elemento	Qué te dice	Error que evita
Resultado y código	Qué ocurrió en la ejecución seleccionada.	Convertirlo en una etiqueta absoluta.
Grado de evidencia	Si es archivo, registro, referencia, log o infraestructura.	Tratar todo como prueba de ejecución.
Alcance	Qué teléfono, archivos, cuentas y opciones incluye.	Generalizar al dispositivo completo.
Huecos	Qué no pudo leer o comprobar y por qué.	Llamar limpio a lo no revisado.
Indicadores y fechas	Qué fuentes se usaron y si están actualizadas.	Confundir copia reciente con indicador actual.
Siguiente paso	Preservar, cerrar huecos o pedir ayuda según el caso.	Borrar o “limpiar” por reflejo.

7.2 Códigos y significado operativo

Código / situación	Lectura correcta	Siguiente decisión
0: sin accionables ni huecos	No se encontraron coincidencias accionables en ese alcance.	No llamarlo dispositivo seguro; revisar alcance y motivo de preocupación.
1: error	La ejecución o la salida falló.	Corregir entrada o destino; no interpretar como ausencia.
2: coincidencias accionables	Hay indicios que requieren interpretación y preservación.	No borrar, ejecutar ni perseguir; buscar ayuda.
3: faltan datos o fuentes	Hay huecos; no es un resultado limpio.	Completar cobertura y volver a revisar.
4: salida sin escanear	No se produjo una revisión ni un veredicto.	No afirmar que no hay spyware.
Referencias o indicadores retirados	El origen del indicador cambia su significado actual.	Revisar contexto y fuente, no forzar una acusación.

Fuentes de la tabla: [12]

7.3 “Worth a look” no es una sentencia

Una aplicación instalada fuera de la tienda, acceso de accesibilidad, una versión antigua o una configuración de verificación desactivada puede merecer una pregunta. No es un hallazgo por sí solo. Las herramientas de accesibilidad, lectores de pantalla, gestores de contraseñas y aplicaciones de automatización pueden ser legítimas. La persona que conoce el dispositivo puede confirmar o descartar esas explicaciones con más información.

> **Duriva rompe la cuarta pared**
>
> Si solo lees “hay seis coincidencias”, parece una sentencia. Si lees también “hay cuatro comprobaciones sin ejecutar”, entiendes que el expediente sigue abierto. Esa es la diferencia entre reaccionar y revisar.



Figura 3. El reporte se lee por capas. El alcance y los huecos cambian el significado Reconstrucción editorial; no constituye evidencia real.

8. Los cuatro escenarios del laboratorio

8.1 `spyware`: seis hallazgos, ninguna conclusión apresurada

El escenario sintético `spyware` produjo seis coincidencias: cinco evidencias en el dispositivo y una en el registro. Incluye una aplicación, una huella de archivo, un certificado, una propiedad, una ruta y una referencia de infraestructura inventada. También dejó cuatro huecos: sin huellas de archivos, sin historial de batería, sin reporte de fallos y sin respaldo de SMS. El resultado fue `INDICATORS_FOUND`, código 2 y `scan_state: partial`.[13]

Lo que enseña no es “tienes spyware”, sino cómo se agrupan objetos distintos y por qué cada uno necesita interpretación. La propia salida recuerda que una coincidencia pide investigar, no declarar compromiso ni ejecutar una limpieza. La presencia de un archivo o configuración no demuestra por sí sola ejecución, y una referencia de infraestructura no demuestra contacto exitoso. Todo el teléfono y todos los indicadores son ficticios.

8.2 `worth-a-look`: elementos para preguntar, no para acusar

El escenario `worth-a-look` no encontró indicadores conocidos, pero mostró cuatro elementos para preguntar: una aplicación instalada directamente con acceso de accesibilidad, actualizaciones antiguas, un servicio de accesibilidad habilitado y verificación de aplicaciones desactivada. El resultado fue `NO_KNOWN_INDICATORS_WITH_GAPS`, código 3, con los mismos cuatro huecos de cobertura.[14]

Estos elementos no prueban infección ni falsedad. Son una invitación a preguntar: ¿reconoces la aplicación?, ¿para qué la instalaste?, ¿esperabas ese permiso?, ¿hay actualizaciones pendientes?, ¿qué

cambió antes del comportamiento? El manual no afirma que el dueño esté equivocado ni que todo sea normal. Aprender a preguntar antes de acusar es el objetivo.

8.3 `clean`: ausencia de coincidencias con cuatro huecos

El escenario `clean` no produjo coincidencias conocidas, pero conservó cuatro huecos y código 3. La salida dice expresamente que no es un certificado de buena salud. Enseña que “nada encontrado” solo puede referirse a lo revisado y a los indicadores conocidos. No prueba ausencia de spyware nuevo, oculto, dirigido o no documentado, ni que todos los lugares fueron examinados.[15]

Si una persona tiene una razón concreta para preocuparse, el resultado no elimina esa preocupación. El siguiente paso puede ser completar cobertura, revisar registros, consultar un especialista o simplemente documentar que la primera comprobación no aportó indicios accionables. No hay que forzar un falso positivo para que la persona se sienta comprendida.

8.4 `cellebrite`: acceso forense, no spyware

El escenario `cellebrite` produjo una coincidencia en el registro USB y código 2. Su propósito es mostrar cómo la herramienta reconoce una pista de acceso forense y cómo cambian las recomendaciones: preservar, revisar aplicaciones cercanas a ese momento y cambiar contraseñas desde otro dispositivo si el contexto lo justifica. El registro y el número de serie son inventados; no hay ninguna persona ni dispositivo real detrás.[16]

Este caso no es spyware y tampoco permite afirmar por sí solo toda una extracción completa. La pregunta pericial es quién tuvo acceso al teléfono, durante cuánto tiempo, con qué autoridad y qué ocurrió antes y después. La conclusión debe distinguir una pista de conexión con el significado que el contexto puede acreditar.

> **Cuatro aprendizajes diferentes**
>
> Coincidencias no equivalen a infección; elementos para revisar no equivalen a falso positivo; cero coincidencias no equivale a seguridad; y una pista forense no equivale a prueba de extracción total. El reporte es un comienzo de revisión, no una sentencia.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · spyware

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: spyware. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       org.example.training.spyapp  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       e36c3fee5d43ffb61b91fbee792cd8b7b4ebd9076f77e9002a9eaa0ea5648a84  [sample]
          The file fingerprint of a published spyware sample (its family
          is named where the source gives one). A match here is
          conclusive, not circumstantial.
          Where: app org.example.training.spyapp (/data/app/training-spyapp/base.apk)

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       d472b7c9d957a9e55ce56bd80388b97be9e2132644c0a51cac03aa618905e6d2  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       persist.training.spy.flag  [artifact]
          Where: system property persist.training.spy.flag

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       /data/local/tmp/training-spy-daemon  [artifact]
          Where: /data/local/tmp/training-spy-daemon

    >> THE PHONE'S SYSTEM LOGS NAME THIS SPYWARE INFRASTRUCTURE
       training-spyware-server[.]invalid  [infrastructure]
          A server the cited researchers attribute to the named spyware
          family. Its exact role - delivering an exploit, controlling an
          implant or receiving stolen data - is not stated in the source,
          so treat contact as serious but unspecified. A domain can change
          hands after a campaign ends: compare the date of the evidence
          with the date of the research.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log dumpsys.txt, line 1

  WHAT TO DO
    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figura 4. Reporte real de entrenamiento del escenario spyware. Fragmento literal; todos los datos son sintéticos. Reconstrucción editorial; no constituye evidencia real.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · worth-a-look

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: worth-a-look. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  ALSO: 4 items under "WORTH A LOOK" further down. They are NOT
  a finding; each comes with its usual, ordinary explanation.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================

Indicator set : 6 indicators, unknown age
  ** WARNING: one or more source dates are unknown; copying files does not refresh indicators. **

DETAIL  —  what was examined, and the evidence behind the summary

--- android-intrusion check  [NOT_APPLICABLE] ---
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figura 5. Reporte real de entrenamiento del escenario worth-a-look. Fragmento literal; todos los datos son sintéticos. Reconstrucción editorial; no constituye evidencia real.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · clean

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: clean. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figura 6. Reporte real de entrenamiento del escenario clean. Fragmento literal; todos los datos son sintéticos. Reconstrucción editorial; no constituye evidencia real.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · cellebrite

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: cellebrite. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SIGNS THIS PHONE WAS UNLOCKED WITH A PHONE-FORENSICS TOOL (CELLEBRITE)
       cellebrite usb 04f2:b071  [forensic]
          A trace of Cellebrite, the phone-forensics tool police and
          security services use to unlock seized phones and copy their
          contents. It is not spyware: it shows the phone was unlocked, or
          an unlock was attempted, while it was out of its owner's hands.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log logcat.txt, line 2

  WHAT TO DO
    Someone unlocked this phone, or tried to, with Cellebrite: the
    phone-forensics tool police and security services use to copy
    everything on a seized phone. Assume what was on the phone then -
    messages, photos, contacts, saved passwords and the accounts
    signed in - was copied. Change the passwords of important accounts
    from another device, sign out other sessions, and tell the people
    whose conversations were on it. In documented cases spyware was
    installed after such an unlock, so check the apps installed around
    that time and get expert help.

    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.

    Do NOT open, visit or look up indicator addresses. Keep the [.]
    spelling when sharing them.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figura 7. Reporte real de entrenamiento del escenario cellebrite. Fragmento literal; todos los datos son sintéticos. Reconstrucción editorial; no constituye evidencia real.

9. Entrega segura al perito o al equipo de respuesta

9.1 Primero el resumen, después el expediente completo

Antes de enviar todo, pregunta a la persona que recibirá el caso qué necesita y por qué canal. Una primera conversación puede limitarse a motivo de preocupación, dispositivo, alcance, fecha, resultado y huecos. El resumen mínimo ayuda a decidir si se necesita el informe completo y evita transmitir historial o mensajes que no aportan a la pregunta.

Cuando se necesita el informe completo, se entrega por canal seguro, no como archivo público. La versión de trabajo y la versión para compartir se separan. La persona receptora puede necesitar objetos originales, pero eso se acuerda expresamente. No se suben colecciones Android, respaldos iOS ni reportes a servicios desconocidos, grupos de chat o sitios de análisis genéricos.[17]

9.2 Hash y EML para una entrega verificable

Si el informe se envía por correo, conserva el EML completo con cuerpo, encabezados y adjuntos. El cuerpo puede incluir el algoritmo y el hash de cada archivo. El receptor calcula sus propios valores y compara. La coincidencia acredita igualdad con el archivo declarado en esa entrega, no la autenticidad del dispositivo ni la verdad de los hallazgos. Un hash calculado después solo acredita integridad desde ese momento.

El cifrado del correo, la firma y el hash resuelven problemas distintos. El cifrado limita quién puede leer; la firma ayuda a comprobar origen y alteración; el hash compara objetos. Ninguno demuestra que la persona que escribió el mensaje sea quien afirma ni que el contenido sea verdadero. No envíes la clave privada ni la contraseña del archivo en el mismo mensaje. Usa un canal separado acordado.

Objeto	Qué se registra	Qué no demuestra
EML de entrega	Cuerpo, encabezados, adjuntos y recepción.	Que el remitente humano escribió el contenido.
Reporte TXT / JSON	Nombre, tamaño, hash, fecha y versión.	Que el alcance fue total o el dispositivo auténtico.
Resumen para compartir	Resultado, alcance, huecos y siguiente paso.	Una pericial completa o una ausencia de riesgo.
Clave o contraseña	Canal separado y destinatario confirmado.	Que la entrega fue autorizada por cualquier receptor.
Colección original	Autoridad, cobertura, custodia y hash por objeto.	Que cualquier herramienta pueda leer todos los artefactos.

9.3 La explicación que evita una segunda crisis

Texto breve para entregar el caso

```
Motivo de preocupación: [conducta observada y fecha]
Dispositivo y autorización: [tipo, titular y permiso]
Herramienta y versión: [origen y verificación]
Alcance: [qué se revisó y qué no]
Resultado: [coincidencias, referencias y huecos]
Acciones ya realizadas: [sin borrar ni limpiar]
Objetos entregados: [resumen / informe / originales]
Hash de cada archivo: [algoritmo y valor]
Lo que necesito: [revisión de alcance, interpretación y siguiente paso]
Datos que no incluí: [claves, contraseñas, contenido íntimo o irrelevante]
```

> **No se trata de ganar una discusión**
>
> El perito no necesita que la persona demuestre que tenía razón. Necesita una fuente, una cronología y una explicación de lo que se hizo. La incertidumbre bien conservada es más útil que una certeza fabricada.

Anexo A. Protocolo reproducible para el perito

A.1 Registro del entorno y de la procedencia

Registro usado para producir los ejemplos de esta guía

```
Repositorio: https://github.com/interplains/Zero-Breach-Toolkit
Commit: 10ceaba497e40da1f327916a0a3fe0af0ff5994f
Versión mostrada: Zero Breach Toolkit 2.0.6
Esquema JSON: 1.6
Archivo: scan/zero-breach-toolkit.py
SHA-256: 4f7294b0d72ae901552e3ac44f64148c0059d43d587a1638654ab00e7c80e627
Escenarios: spyware, worth-a-look, clean y cellebrite
Tipo de datos: completamente sintéticos
Información personal: no examinada
Dispositivos reales: no utilizados
```

Este registro describe una clonación del repositorio y ejecuciones de entrenamiento; no es una atestación del ejecutable de Windows ni una verificación de la versión más reciente. La comprobación del ejecutable descargado debe hacerse contra su propia versión y flujo de construcción. Los cuatro escenarios sí se ejecutaron y produjeron TXT y JSON, además de una salida JSON de `--describe`.

A.2 Ficha para una ejecución real autorizada

Plantilla de registro pericial

```
Caso y autorización: [identificador, titular, alcance y exclusiones]
Razón de la comprobación: [conducta y pregunta]
Dispositivo y estado inicial: [modelo, sistema, fecha, zona]
Paquete: [repositorio, versión, archivo y verificación]
Hash del paquete y de indicadores: [valores y fecha]
Entorno: [equipo de análisis, aislamiento y sincronización]
Alcance: [default / full / targeted / browser / phone]
Comando y parámetros: [sin secretos]
Inicio y fin con zona: [literales]
Salidas: [TXT, JSON, resumen, manifest y hashes]
Resultado y código: [literal]
Hallazgos: [grado, objeto, fuente y contexto]
Huecos: [checks no ejecutados y razones]
Incidencias: [errores, límites y archivos no disponibles]
Preservación y custodia: [ubicación, acceso y transferencias]
Revisión: [persona, fecha y siguiente comprobación]
```

A.3 Matriz de interpretación

Pregunta	Fuente que responde	Qué no se puede afirmar
¿Qué encontró?	Hits, grado y objeto.	Infección automática o identidad del atacante.
¿Qué no pudo revisar?	Coverage.not_checked y scan_state.	Que los lugares omitidos estén limpios.
¿Qué fuentes usó?	Indicadores, versiones y fechas.	Que una copia reciente sea evidencia actual.
¿Qué puede ser normal?	Configuración, aplicación y contexto del dueño.	Falso positivo sin corroboración.
¿Qué falta para atribuir?	Autoridad, sesiones, dispositivo y cronología.	Persona física por una IP, app o MAC.
¿Qué se comparte?	Resumen o informe completo según necesidad.	Que publicar el informe sea inocuo.

Criterio de aceptación

El informe debe permitir que otra persona reproduzca el alcance, localice cada hallazgo, entienda cada hueco y sepa qué sigue sin demostrarse. Si solo contiene una etiqueta “limpio” o “infectado”, todavía no es una revisión completa.

Anexo B. Marco jurídico, privacidad y control final

Una comprobación de seguridad también trata datos personales. En México se aplican principios de finalidad, proporcionalidad, seguridad, confidencialidad y vulneraciones de la LFPDPPP actual. Perú, Chile, Argentina, Colombia, Ecuador y España/UE contienen funciones equivalentes, no idénticas, de minimización, seguridad, derechos y proveedores. En Chile, la modernización de la Ley 21.719 tiene inicio diferido al 1 de diciembre de 2026 y no debe anticiparse como régimen plenamente vigente. No hay una autorización universal para leer un dispositivo ajeno.[18][19][20][21][22][23][24]

Control antes de cerrar	Respuesta exigida
¿La persona estaba segura y autorizada?	No se ejecutó ninguna prueba por curiosidad ni sin permiso.
¿El paquete fue verificado?	Repositorio, versión y procedencia documentados.
¿La salida quedó protegida?	Carpeta local, acceso y sincronización controlados.
¿Se distinguió hallazgo de referencia y hueco?	No se llamó infección ni seguridad por una etiqueta.
¿Se explicó lo normal sin descartar lo grave?	Configuración y contexto fueron comprobados.
¿El reporte se compartió con minimización?	Resumen primero; expediente completo por canal seguro.
¿El perito puede reproducir?	Versión, alcance, comandos, hashes, huecos y custodia presentes.

Cierre

La buena pregunta no es “¿soy paranoico?”, sino “¿qué puedo comprobar sin hacerme más daño?”. La respuesta puede ser una configuración, una coincidencia, un hueco o una revisión profesional. Todas son más útiles que una acusación sin fuente.

Referencias citadas

Cada número remite a la fuente consultada en el cuerpo. La fecha general de revisión documental es el 10 de noviembre de 2026; el uso en un expediente exige comprobar la versión aplicable al hecho, materia, sujeto y jurisdicción.

[1] Apple Support. Use private Wi-Fi addresses on Apple devices: la dirección privada puede variar por red y, con Rotating, cada dos semanas en sistemas compatibles. La función busca reducir seguimiento; no constituye evidencia de espionaje ni explica todas las desconexiones. Fuente oficial en línea

[2] Zero Breach Toolkit, repositorio interplains/Zero-Breach-Toolkit. Comprobaciones locales de indicadores publicados de spyware, con código bajo Apache 2.0 y documentación de alcance y límites. Fuente oficial en línea

[3] Zero Breach Toolkit. Cobertura por familia de comprobaciones y límites: archivos, navegadores, persistencia, registros, Android y respaldos de iPhone. No mide tasas de detección ni de falsos positivos. Fuente oficial en línea

[4] Zero Breach Toolkit. Guía de escenarios sintéticos de entrenamiento: spyware, worth-a-look, clean y cellebrite. Los indicadores son inventados y los ejemplos no leen el equipo ni listas reales; no permiten inferir el estado de un dispositivo real. Fuente oficial en línea

[5] Zero Breach Toolkit, repositorio interplains/Zero-Breach-Toolkit. Comprobaciones locales de indicadores publicados de spyware, con código bajo Apache 2.0 y documentación de alcance y límites. Fuente oficial en línea

[6] Zero Breach Toolkit. Guía de verificación de versiones: atestación de programas construidos por GitHub Actions, manifiestos SHA-256 y firma; el paquete Windows no tiene firma de código de Windows. Fuente oficial en línea

[7] Zero Breach Toolkit. PRIVACY: el análisis ordinario no realiza cargas por diseño; actualización y adquisición Android son actividades distintas. Los reportes pueden contener datos sensibles y el resumen para compartir no sustituye al informe completo. Fuente oficial en línea

[8] Zero Breach Toolkit. Contrato de resultados y cobertura: códigos 0, 1, 2, 3 y 4; distinción entre hallazgo, referencia, hueco, salida sin escaneo y alcance limitado. Un resultado sin coincidencias nunca es garantía de seguridad. Fuente oficial en línea

[9] Zero Breach Toolkit. Guía de escenarios sintéticos de entrenamiento: spyware, worth-a-look, clean y cellebrite. Los indicadores son inventados y los ejemplos no leen el equipo ni listas reales; no permiten inferir el estado de un dispositivo real. Fuente oficial en línea

[10] Zero Breach Toolkit. Cobertura por familia de comprobaciones y límites: archivos, navegadores, persistencia, registros, Android y respaldos de iPhone. No mide tasas de detección ni de falsos positivos. Fuente oficial en línea

[11] Zero Breach Toolkit. PRIVACY: el análisis ordinario no realiza cargas por diseño; actualización y adquisición Android son actividades distintas. Los reportes pueden contener datos sensibles y el resumen para compartir no sustituye al informe completo. Fuente oficial en línea

[12] Zero Breach Toolkit. Contrato de resultados y cobertura: códigos 0, 1, 2, 3 y 4; distinción entre hallazgo, referencia, hueco, salida sin escaneo y alcance limitado. Un resultado sin coincidencias nunca es garantía de seguridad. Fuente oficial en línea

[13] Laboratorio local ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, ejecución de los cuatro escenarios sintéticos. Archivos spyware, worth-a-look, clean y cellebrite en TXT/JSON. No se examinó información personal ni dispositivos reales.

[14] Laboratorio local ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, ejecución de los cuatro escenarios sintéticos. Archivos spyware, worth-a-look, clean y cellebrite en TXT/JSON. No se examinó información personal ni dispositivos reales.

[15] Laboratorio local ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, ejecución de los cuatro escenarios sintéticos. Archivos spyware, worth-a-look, clean y cellebrite en TXT/JSON. No se examinó información personal ni dispositivos reales.

[16] Laboratorio local ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, ejecución de los cuatro escenarios sintéticos. Archivos spyware, worth-a-look, clean y cellebrite en TXT/JSON. No se examinó información personal ni dispositivos reales.

[17] Zero Breach Toolkit. PRIVACY: el análisis ordinario no realiza cargas por diseño; actualización y adquisición Android son actividades distintas. Los reportes pueden contener datos sensibles y el resumen para compartir no sustituye al informe completo. Fuente oficial en línea

[18] México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[19] Perú. Ley 29733 y su Reglamento aprobado por DS 016-2024-JUS. Principios de finalidad, proporcionalidad, seguridad y confidencialidad; el nuevo Reglamento desarrolla incidentes, evaluación preventiva y funciones progresivas del oficial de datos. Fuente oficial en línea

[20] Chile. Ley 21.719, que modifica la Ley 19.628 sobre protección de datos personales. La versión con el nuevo régimen tiene inicio de vigencia diferido al 01-12-2026; antes de esa fecha debe revisarse la norma entonces aplicable y no anticipar obligaciones futuras como

vigentes. Fuente oficial en línea

[21] Argentina. Ley 25.326, texto actualizado. Artículos 4–6, 9–10, 14–16 y 25: calidad, información, seguridad, confidencialidad, derechos de titulares y prestación de servicios de tratamiento por cuenta de terceros. Fuente oficial en línea

[22] Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

[23] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[24] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

Aviso editorial: guía técnica general y material educativo. No constituye asesoría legal, dictamen pericial ni autorización para acceder a sistemas o información. Los ejemplos y cifras de demostración son ficticios; las figuras son reconstrucciones editoriales.