Selective Logical Acquisition Model for Low-Intrusion Mobile Devices with Integrity and Traceability Guarantees in Field Contexts

Maximiliano Facundo Telmo Gonzalez[1], Natalia Vanesa Diego[2] and Ramón Americo Wills[3]

[1] Dirección de Investigación Operativa / Ministerio Público Fiscal de Córdoba
mtelmo@justiciacordoba.gob.ar
[2] Dirección de Investigación Operativa / Ministerio Público Fiscal de Córdoba
ndiego@justiciacordoba.gob.ar
[3] Instituto de Formación / Ministerio Público Fiscal de Córdoba/Universidad Nacional de Córdoba
rwills@justiciacordoba.gob.ar

Abstract. Mobile device forensic acquisition in field contexts poses challenges regarding integrity, traceability, and methodological control, particularly when decentralized methods or manual documentation are used. These limitations introduce overwrite risks and affect the probative validity of evidence collected outside laboratory environments. This paper proposes a low-intrusion acquisition model that addresses these risks through verifiable detectability rather than inviolability. The model defines a selective collection policy for high-value artifacts, combined with cryptographic integrity mechanisms (SHA-256 per artifact), sequential event chaining, and verifiable state manifests. It also analyzes the conditions under which this approach aligns with forensic standards and admissibility requirements in criminal proceedings. Finally, the paper discusses institutional dependence on proprietary tools and the potential of this approach as an auditable alternative within sovereign digital forensics, proposing guiding criteria for first responders and judicial actors.

Keywords: chain of custody, probative validity, technological sovereignty.

Modelo de adquisición lógica selectiva en dispositivos móviles de baja intrusión con garantías de integridad y trazabilidad en contextos de campo

Resumen. La adquisición forense de dispositivos móviles en campo presenta desafíos en integridad, trazabilidad y control metodológico, especialmente cuando se utilizan métodos descentralizados o documentación manual. Estas limitaciones introducen riesgos de sobreescritura y cuestionamientos sobre la validez probatoria de la evidencia recolectada fuera del laboratorio. Se propone

un modelo de adquisición de baja intrusión basado en detectabilidad verificable en lugar de inviolabilidad. El modelo establece una política de recolección selectiva de artefactos de alto valor probatorio, combinada con mecanismos de integridad criptográfica (hash SHA-256 por artefacto), encadenamiento de eventos y generación de manifiestos verificables. Se analizan las condiciones de compatibilidad con estándares forenses y requisitos de admisibilidad penal. Asimismo, se discute la dependencia de herramientas propietarias extranjeras y el potencial de este enfoque como alternativa auditable en el marco de una forensia digital soberana, proponiendo criterios orientadores para el primer interventor y operadores judiciales.

Palabras clave: cadena de custodia, validez probatoria, soberanía tecnológica.

1 Introducción

La creciente centralidad de la evidencia digital en el proceso penal argentino plantea desafíos que exceden lo técnico. Su validez probatoria depende no solo del procedimiento de adquisición, sino de la capacidad de demostrar su integridad, trazabilidad y sostenibilidad metodológica frente a impugnaciones. Esta exigencia es crítica cuando la adquisición ocurre fuera del laboratorio, allanamientos, entrevistas o inspecciones, donde el primer interventor actúa con recursos limitados y sin condiciones controladas.

En este contexto, los operadores judiciales requieren certeza sobre la integridad de la evidencia, mientras que los procedimientos de campo carecen frecuentemente de mecanismos para acreditarla.

Este trabajo examina CAPTA (Colecta Ágil de Potencial Elemento Probatorio Técnico Auditable), un modelo de adquisición lógica selectiva desarrollado por el Ministerio Público Fiscal de la Provincia de Córdoba a través de la Dirección de Investigación Operativa. Se analizan las condiciones en las que sus mecanismos (hash SHA-256 por artefacto, encadenamiento de eventos, licenciamiento vinculado al dispositivo y verificación independiente) resultan compatibles con estándares forenses y requisitos de admisibilidad.

Los métodos basados en Android Debug Bridge (ADB) son operativamente viables pero presentan debilidades probatorias: no garantizan solo lectura, lo que genera cuestionamientos sobre posibles alteraciones. La respuesta no es negar ese riesgo, sino gestionarlo de forma explícita y documentada. Casey y Turnbull (2011) establecieron los fundamentos del triage digital para escenarios con recursos limitados; Barmpatsalou et al. (2018) analizaron las limitaciones de los métodos de adquisición lógica en dispositivos móviles, destacando su menor intrusividad pero también sus restricciones en términos de completitud y control forense; y Carrier y Spafford (2003) propusieron la cadena de custodia digital como construcción procesal verificable. A diferencia de estos antecedentes, este trabajo examina ADB como componente de un modelo institucionalizado e introduce la detectabilidad verificable como criterio de validez probatoria en lugar de la inviolabilidad.

El trabajo realiza dos contribuciones: (i) analiza la compatibilidad entre adquisición de baja intrusión y principios jurídico-probatorios; (ii) discute la dependencia de herramientas propietarias y el potencial de enfoques auditables como

alternativa soberana. La Sección 2 presenta el modelo; la 3 analiza estándares; la 4 examina legalidad; la 5 aborda datos personales; la 6 discute soberanía; y la 7 concluye.

2 El modelo de adquisición examinado

2.1 Caracterización del modelo

CAPTA implementa un modelo de triaje lógico orientado al primer interventor en contextos de campo. Su premisa central es operativamente específica: la adquisición forense debe ser posible sin las condiciones que define el laboratorio, lo que implica redefinir los criterios de diseño no en función de la completitud de la extracción sino en función de la viabilidad operativa, la preservación de la integridad y la utilidad probatoria inmediata.

El modelo opera sobre dispositivos Android y afines mediante Android Debug Bridge (ADB), una interfaz de depuración estándar documentada públicamente, sin requerir privilegios de superusuario ni modificaciones persistentes del dispositivo. Requiere como condiciones mínimas que el dispositivo esté desbloqueado y con depuración USB o WiFi habilitada, condiciones que deben verificarse y documentarse antes del inicio de la sesión forense, constituyendo requisitos de aplicabilidad y no intervenciones del modelo.

Esta distinción es jurídicamente relevante: la habilitación de la depuración es una condición preexistente al relevamiento, no una modificación introducida por el operador durante la adquisición. El modelo de adquisición en sí mismo no altera las configuraciones del dispositivo.

2.2 Principios del modelo con relevancia jurídico-probatoria

Mínima intervención. Toda acción ejecutada durante la adquisición se limita estrictamente a lo necesario para la recolección de los artefactos objetivos. No se instalan aplicaciones, no se ejecutan comandos con impacto sobre el estado del dispositivo más allá de la lectura de datos, y las escrituras en el dispositivo quedan restringidas por política de lista blanca a operaciones estrictamente necesarias (grabación de pantalla y operaciones temporales de pull), con eliminación inmediata de los temporales y registro de cada excepción.

Integridad verificable. Cada artefacto recolectado recibe un hash SHA-256 calculado en el momento de la incorporación. Este valor queda registrado en el reporte forense, en el acta de recolección y en el manifiesto generado al bloquear el relevamiento, permitiendo verificar la integridad de cada elemento en cualquier momento posterior mediante cualquier implementación estándar del algoritmo, sin dependencia de CAPTA, ni de ninguna herramienta propietaria.

Trazabilidad completa. Cada acción ejecutada durante la sesión queda registrada en un log forense con encadenamiento criptográfico secuencial: cada evento depende criptográficamente del anterior, de modo que cualquier modificación, eliminación o inserción en cualquier posición de la cadena altera todos los hashes subsiguientes y resulta detectable. El log registra además la identidad del operador, los atributos del

kit de ejecución y el resultado de la verificación de integridad del ejecutable al inicio de cada sesión.

Detectabilidad como garantía explícita. El modelo no promete inviolabilidad (promesa técnicamente insostenible en ausencia de bloqueo físico de escritura), sino detectabilidad verificable de cualquier alteración respecto del estado al momento del bloqueo del relevamiento. Esta distinción conceptual es el núcleo del argumento jurídico-probatorio del trabajo: la solidez de la evidencia no descansa en la imposibilidad de su alteración sino en la capacidad de demostrar que no fue alterada.

2.3 **Mecanismos de integridad y su valor probatorio**

Los mecanismos de integridad CAPTA operan en tres niveles complementarios que, en conjunto, constituyen un sistema de garantías verificables:

Hash por artefacto: permite verificar que cada elemento recolectado es idéntico al que existía en el dispositivo al momento de la extracción. La verificación es reproducible, independiente del entorno original y matemáticamente comprobable.

Encadenamiento criptográfico del registro forense: permite verificar que la secuencia de acciones registrada durante el relevamiento no fue alterada con posterioridad. La cadena puede ser reconstruida y verificada por cualquier perito o tribunal sin acceso a CAPTA.

Manifiesto de hashes y bloqueo: al finalizar el relevamiento, el sistema genera un listado completo de todos los archivos con sus hashes y establece la carpeta en modo solo lectura. El manifiesto vincula el registro forense con el conjunto de evidencia, constituyendo el documento técnico central de la cadena de custodia.

2.4 **Sistema de licenciamiento y trazabilidad del operador**

CAPTA implementa un sistema de licenciamiento que ata criptográficamente cada kit al dispositivo físico de almacenamiento desde el cual opera, mediante cifrado AES-256-GCM con clave derivada de atributos del hardware y firma RSA de la clave pública embebida en el ejecutable. Este mecanismo tiene valor jurídico-probatorio directo: permite afirmar ante cualquier instancia judicial que la intervención fue realizada con el kit autorizado institucionalmente y que el ejecutable no fue modificado respecto del aprobado.

2.5 **Alcance y limitaciones técnicas relevantes para el análisis jurídico**

El modelo tiene un alcance deliberadamente acotado que es necesario precisar para el análisis jurídico-probatorio. CAPTA no accede a datos en particiones del sistema, contenido cifrado de aplicaciones con protección adicional, ni artefactos en el espacio privado de aplicaciones que no exponen interfaces de exportación. No certifica autenticidad de origen, no puede probar que un archivo existía en el dispositivo antes de la intervención si no fue recolectado durante ella. No impide modificaciones externas con privilegios administrativos sobre la carpeta de evidencia una vez generada, aunque garantiza su detectabilidad mediante el manifiesto.

Estas limitaciones no invalidan el modelo sino que definen su espacio de aplicación. El análisis jurídico-probatorio de las secciones siguientes parte de este alcance declarado: examina las condiciones bajo las cuales CAPTA, dentro de ese alcance, produce evidencia jurídicamente sostenible.

3 Compatibilidad con estándares forenses internacionales

3.1 Los estándares como marco de referencia jurídico-técnico

La compatibilidad con estándares internacionales cumple una función técnica y jurídica: define condiciones de confiabilidad y refuerza la defensa del procedimiento ante impugnaciones. En informática forense, las referencias principales son las normas ISO/IEC 27037, 27041, 27042 y 27043, junto con NIST SP 800-101 Rev.1 para dispositivos móviles. Si bien no tienen fuerza normativa directa en Argentina, estos estándares son ampliamente reconocidos como criterios de buenas prácticas y utilizados como referencia en peritajes y decisiones judiciales. El análisis evalúa la alineación de CAPTA identificando compatibilidades, brechas y mecanismos de compensación.

3.2 ISO/IEC 27037 – Identificación, recolección y preservación

La norma establece que la evidencia debe ser recolectada y preservada de forma verificable, con documentación completa del procedimiento. CAPTA cumple estos principios mediante: preservación del estado (las operaciones de lectura vía ADB no modifican el sistema ni los metadatos; las escrituras necesarias están restringidas, registradas y eliminadas); documentación (el log forense encadenado registra cada acción con precisión temporal, junto con el acta de recolección y la identificación del operador); e integridad verificable (el hash SHA-256 por artefacto y el manifiesto permiten verificación independiente). La principal limitación es la ausencia de bloqueo físico de escritura, compensada mediante controles por software y registro exhaustivo, en línea con el estándar.

3.3 ISO/IEC 27041 – Idoneidad del método

Esta norma exige que el método sea validado, reproducible y apropiado al caso. CAPTA cumple en tres aspectos: reproducibilidad (comportamiento determinista bajo mismas condiciones); auditabilidad (verificación independiente del log y de los hashes sin dependencia de la herramienta); adecuación contextual (idóneo para relevamiento preliminar en campo, no como sustituto de laboratorio). La idoneidad se evalúa según el propósito, no en abstracto, lo que respalda su uso como etapa inicial de investigación.

3.4 ISO/IEC 27042 – Análisis e interpretación

Aunque orientada al análisis, esta norma resulta parcialmente aplicable. CAPTA contribuye mediante registro de decisiones de recolección, que permite reconstruir criterios del operador, y documentación contextual (acta y reporte), necesaria para la interpretación posterior.

3.5 ISO/IEC 27043 – Marco general de investigación

Esta norma define un enfoque integral de investigación digital. CAPTA se integra en la fase de identificación y preservación preliminar, funcionando como etapa inicial dentro de una estrategia forense escalonada, no como reemplazo del laboratorio.

3.6 NIST SP 800-101 Rev.1 – Dispositivos móviles

El estándar del NIST establece buenas prácticas específicas para dispositivos móviles, enfatizando documentación, integridad y cadena de custodia. CAPTA se alinea en: documentación del estado del dispositivo; registro cronológico de acciones; verificación criptográfica de artefactos; generación de reportes estructurados. La ausencia de bloqueo físico de escritura es reconocida por el propio estándar como limitación posible, mitigable mediante controles por software y documentación.

3.7 Síntesis: compatibilidad brechas y compensaciones

El análisis permite distinguir:

- **Compatibilidad plena:** integridad verificable por artefacto, trazabilidad completa, reproducibilidad, documentación del contexto, identificación del operador y reportes estructurados.
- **Compatibilidad parcial (con compensación):** ausencia de bloqueo físico y escrituras mínimas, mitigadas mediante registro, control y verificación posterior.
- **Brechas dentro del alcance:** acceso a datos cifrados o particiones del sistema y certificación de autenticidad de origen.

En síntesis, CAPTA cumple los requisitos sustantivos de los estándares aplicables dentro de su alcance declarado. Sus limitaciones no se ocultan, sino que se explicitan y compensan por diseño, lo que sustenta su validez jurídico-probatoria.

4 Requisitos de legalidad del uso de CAPTA

El marco normativo habilitante es la Resolución FG N° 7/26 de la Fiscalía General de la Provincia de Córdoba, dictada en ejercicio de las facultades reglamentarias previstas en el art. 16 incs. 6 y 8 de la Ley N° 7826, que impone al MPF el principio de objetividad y la obligación de recabar los elementos de convicción disponibles. CAPTA es utilizada por los Detectives de la Dirección de Investigación Operativa de la Dirección General de Policía Judicial, a pedido de fiscalías (capital e interior) o del

juzgado interviniente, con autorización judicial motivada que consigne expresamente la finalidad y el alcance de la medida, intervención de personal capacitado, y documentación exhaustiva materializada en reporte forense y acta formal, en estricto respeto a los principios de proporcionalidad, especialidad y protección de derechos fundamentales.

El modelo opera en dos escenarios con regímenes de validez diferenciados.

En el contexto de entrevistas con testigos o víctimas, la incorporación de evidencia digital requiere consentimiento expreso documentado en acta, condición suficiente de legitimidad cuando el titular actúa libremente y con información sobre el alcance de la medida. En la práctica, el operador concurre con el dispositivo de almacenamiento que contiene el kit autorizado, conecta el celular de la víctima o testigo, selecciona los elementos indicados por la instrucción, y ejecuta la adquisición. Al finalizar, el sistema genera el reporte forense y el manifiesto de hashes, y el celular es devuelto a su titular en el mismo acto, sin retención. Este flujo preserva el principio de no revictimización y reduce la distancia entre el hecho denunciado y la fijación de la evidencia digital, minimizando el riesgo de sobreescritura o pérdida.

En el contexto de allanamientos, la adquisición se encuadra en la orden judicial que autoriza la medida. Dado que los dispositivos móviles contienen categorías amplias de datos personales sensibles, su acceso debe estar expresamente contemplado en la autorización, con indicación específica de la finalidad y el tipo de artefactos a relevar. El mero secuestro físico sin acceso al contenido puede resultar insuficiente desde el punto de vista probatorio, dado el uso generalizado de cifrado y mecanismos de borrado remoto. En la práctica, el modelo admite dos variantes: la principal consiste en aplicar CAPTA en el lugar del allanamiento sobre el dispositivo hallado, antes o en lugar de su secuestro físico, lo que permite asegurar los artefactos críticos de forma inmediata; la alternativa aplica cuando el dispositivo ya se encontraba secuestrado o no fue posible obtener la autorización a tiempo, realizándose la adquisición en sede judicial con posterioridad bajo las mismas condiciones de documentación y trazabilidad.

El acceso al dispositivo requiere la colaboración del titular o, ante su negativa, autorización judicial para el uso de datos biométricos. La Cámara de Acusación de Córdoba, en autos Quipildor, Armando Andrés (Auto N° 332, 08/09/2020), sostuvo que la utilización compulsiva de datos biométricos para el desbloqueo no vulnera el principio nemo tenetur se ipsum accusare, en tanto constituye el uso de un dato físico preexistente y no una declaración de voluntad del imputado. Este criterio ha sido elevado a norma positiva por la Ley XV N° 43 de Chubut (2026), que autoriza expresamente "el uso de la fuerza física indispensable para proceder al desbloqueo de los dispositivos electrónicos que posean patrón de huella dactilar o cualquier otro de tipo biométrico" (art. 7 inc. c), consolidando una tendencia interprovincial hacia la admisibilidad de esta medida en investigaciones de especial gravedad.

Proporcionalidad, límites y delimitación del uso del software

La adquisición debe estar estrictamente delimitada a la finalidad consignada en la autorización judicial. Si durante el relevamiento se identifican indicios de delitos no comprendidos en la orden original, el operador debe interrumpir la recolección sobre esos elementos e informar de inmediato a la instrucción para obtener una nueva

autorización. La expansión no autorizada constituye una vulneración del principio de proporcionalidad con potencial efecto invalidante sobre la evidencia obtenida. La trazabilidad completa del proceso garantiza que cualquier decisión adoptada durante el relevamiento sea reconstruible y auditable por todas las partes, resguardando el ejercicio efectivo del derecho de defensa en juicio.

5 Protección de datos personales en la adquisición forense móvil

Los dispositivos de almacenamiento, sobre todo los teléfonos celulares, han dejado de ser meros periféricos para convertirse en "...una extensión del cuerpo humano…" conforme al precedente Riley vs California[1], albergando lo que la doctrina denomina el "núcleo duro" de la privacidad. En este escenario, la recolección de PEPs se enfrenta a un doble desafío: la necesidad de garantizar la integridad de la evidencia para el proceso judicial y la obligación de respetar los derechos fundamentales de las personas titulares de los datos.

En este sentido CAPTA es robusto en materia de Protección de Datos Personales (PDP), ya que sigue los lineamientos que propone la legislación argentina en esta área: ley 25.326 de protección de datos personales, Ley 27.483 (convenio 108), Ley 27699 de Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (convenio 108+); y asimismo de la normativa de la Unión Europea (Reglamento General de Protección de Datos Personales).

- Los datos personales sensibles (art. 2 Ley 25.326, art. 6 Ley 27.483), como fotografías, conversaciones en plataformas de mensajería (P2P), cualquier archivo almacenado en el dispositivo, entre otros, exigen una mayor protección. En este sentido la recolección la realiza el primer interventor en un dispositivo de almacenamiento (pendrive) que solo utiliza personal del MPF afectado a dicha función. La herramienta es un archivo ejecutable que está contenido de antemano en el dispositivo que se utiliza en la recolección. Solamente -y específicamente- el personal afectado lleva consigo el hardware referido, nadie más.
- CAPTA implementa un mecanismo de control de integridad del ejecutable mediante el cálculo y registro del hash SHA-256 de cada versión generada, lo que permite verificar que el archivo utilizado en campo es idéntico al validado institucionalmente. En su versión actual (2.2), el sistema opera sin conexión a internet: no transmite datos ni se comunica con servidores externos. La única excepción es la firma digital del acta de recolección, instancia en la que el sistema redirige al navegador hacia la plataforma oficial firmar.gob.ar sin transmitir datos propios ni de la evidencia recolectada. El sistema admite también depuración remota mediante ADB sobre TCP/IP (ADB por WiFi), modalidad que no implica conexión a internet ni transmisión a servidores externos, sino comunicación directa en red local entre el dispositivo analizado y la terminal operativa.
- El pendrive, con la información recolectada, es guardado de forma inmediata en una bolsa, y se precinta para su traslado a las oficinas del MPF.

[1] U.S. Supreme Court. (n.d.). Riley v. California, 573 U.S. 373 (2014). Justia. Recuperado 25/02/2026, de https://supreme.justia.com/cases/federal/us/573/373/

- Los PEPs recolectados en los dispositivos de almacenamiento, luego son descargados en un servidor del Poder Judicial, al que solo tiene acceso la Sección de Cibercrimen de la Dirección de Investigación Operativa (DIO). A continuación se le da acceso al órgano requirente -Fiscalías de Instrucción, Fiscalía Penal Juvenil, Juzgado Penal Juvenil, entre otros-.
- Una vez descargados los PEPs en el servidor local, se procede a formatear el pendrive utilizado. Finalmente se copia el software desde el servidor local en el dispositivo de almacenamiento formateado y es operativo nuevamente. De esta forma se cumplen los principios de proporcionalidad y finalidad en materia de Protección de Datos (art. 11 ley 25.326).
- CAPTA garantiza el ejercicio de los derechos de acceso, rectificación y actualización (art. 14 ley 25.326), en tanto resulten compatibles con la investigación en la que se emplea el sistema.
- Asegurar la legalidad, lealtad y transparencia del tratamiento de datos en la operatividad de la herramienta (Convenio 108+, art. 5)

6 Capacidades forenses nacionales y soberanía tecnológica

La forensia móvil en Argentina depende en gran medida de soluciones comerciales propietarias de origen extranjero. Herramientas como Cellebrite UFED, Oxygen Forensic Detective o MSAB XRY concentran el mercado institucional, imponiendo condiciones de licenciamiento, actualizaciones y soporte que los organismos locales no controlan. Esta dependencia tiene consecuencias concretas: costos de adquisición y renovación elevados, restricciones de uso según jurisdicción o tipo de caso, y opacidad sobre los algoritmos de extracción que dificulta la verificación independiente de resultados en sede judicial.

Desde una perspectiva de soberanía tecnológica, la situación plantea tres problemas. Primero, la auditabilidad: cuando una herramienta propietaria genera un hash o un reporte de extracción, el perito no puede verificar de manera independiente cómo fue producido ese resultado, lo que expone la evidencia a cuestionamientos sobre su origen y método. Segundo, la accesibilidad institucional: organismos de menor escala frecuentemente acceden en cantidad insuficiente a estas herramientas, generando asimetría en las capacidades forenses según jurisdicción. Tercero, la dependencia geopolítica: las condiciones de exportación, actualización y soporte están sujetas a decisiones corporativas y regulaciones extranjeras ajenas al sistema judicial argentino.

En el ámbito nacional, existen desarrollos institucionales que comparten la premisa central de este trabajo y evidencian una tendencia emergente hacia la construcción de capacidades forenses propias. "Espejo Chubut", desarrollado por el Departamento de Informática Forense del Ministerio Público Fiscal de la Provincia del Chubut, implementa una metodología de extracción y preservación de evidencia digital desde dispositivos móviles orientada a víctimas y testigos que aportan elementos directamente en comisarías o fiscalías, sin necesidad de concurrir al laboratorio (MPF Chubut, 2023). "Captura Digital", ofrecida por el Gabinete de Pericias Informáticas del Poder Judicial de Neuquén, permite preservar contenido digital de dispositivos Android mediante Android Debug Bridge (ADB) con consentimiento del propietario,

para su incorporación a investigaciones penales o instancias de preconstitución de prueba, e incluye verificación de integridad del ejecutable mediante hash SHA-256 (Gabinete de Pericias Informáticas, s.f.). Ambos sistemas operan con alcance deliberadamente limitado, sin pretensión de reemplazar la actividad pericial de laboratorio, y facilitan una primera intervención de bajo impacto por personal no especializado. El sistema aquí examinado se inscribe en esta tendencia interprovincial y la desarrolla mediante mecanismos de integridad criptográfica por artefacto, encadenamiento del registro forense, licenciamiento vinculado al dispositivo de ejecución, y adquisición lógica de archivos, elementos y estructuras, que en conjunto amplían la capacidad de defensa probatoria ante impugnaciones.

El enfoque basado en ADB que implementa CAPTA opera sobre una interfaz estándar, abierta y documentada públicamente, mantenida por Google como parte del Android Open Source Project. Su uso no requiere licencias, no depende de actualizaciones comerciales y puede ser auditado en su totalidad por cualquier perito o tribunal que lo requiera. Representa no solo una alternativa técnica sino también una opción de menor dependencia tecnológica, alineada con los principios de transparencia y verificabilidad que el proceso penal exige a la prueba pericial.

Esto no implica que el enfoque reemplace a las herramientas especializadas en todos los contextos. Pero sí sugiere que la construcción de capacidades forenses nacionales debería contemplar, junto a la adquisición de herramientas comerciales, el desarrollo y estandarización de procedimientos basados en tecnologías abiertas, auditables y replicables, como condición para una forensia digital soberana y procesalmente robusta.

7 Conclusiones

La validez probatoria de la evidencia digital no es una propiedad técnica intrínseca sino una construcción procesal que depende de la verificabilidad del procedimiento de obtención. El análisis realizado permite formular tres conclusiones con alcance normativo y técnico diferenciado.

Primera. La adquisición lógica selectiva de baja intrusión es jurídicamente sostenible cuando se cumplen tres condiciones simultáneas: que las limitaciones técnicas sean declaradas explícitamente y no ocultadas; que existan mecanismos de verificación independiente del resultado (hash por artefacto, encadenamiento del registro, manifiesto verificable) accesibles sin dependencia de la herramienta original; y que el procedimiento esté respaldado por autorización judicial motivada y documentación exhaustiva del operador. CAPTA satisface estas condiciones dentro de su alcance declarado, lo que sustenta su compatibilidad con los estándares ISO/IEC 27037, 27041 y NIST SP 800-101 Rev.1 y con los requisitos de admisibilidad del sistema acusatorio argentino.

Segunda. El concepto de detectabilidad verificable, garantizar la identificación de cualquier alteración posterior en lugar de prometer inviolabilidad técnica, constituye el puente conceptual entre el modelo de adquisición en campo y las exigencias del proceso penal. Este enfoque es más honesto metodológicamente y más robusto ante impugnaciones que los modelos que afirman inviolabilidad sin bloqueo físico de

escritura, ya que sitúa la garantía en la verificación independiente y no en una promesa técnica indemostrable.

Tercera. La dependencia institucional de herramientas forenses propietarias de origen extranjero introduce riesgos concretos de auditabilidad, accesibilidad y soberanía que el sistema judicial argentino no controla. El enfoque basado en tecnologías abiertas y documentadas públicamente (como ADB) representa una dirección viable para la construcción de capacidades forenses nacionales procesalmente robustas, no como sustituto de las herramientas especializadas sino como componente auditable de una estrategia forense escalonada.

Referencias

Casey, E., & Turnbull, B. (2011). Digital evidence on mobile devices. En E. Casey (Ed.), Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3.a ed., pp. 339–385). Academic Press.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simões, P. (2018). Current and future trends in mobile device forensics: A survey. ACM Computing Surveys, 51(3), 1–34. https://dl.acm.org/doi/epdf/10.1145/3177847

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of Digital Evidence, 2(2), 1–20.

International Organization for Standardization. (2012). ISO/IEC 27037: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

International Organization for Standardization. (2015a). ISO/IEC 27041: Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods. ISO.

International Organization for Standardization. (2015b). ISO/IEC 27042: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. ISO.

International Organization for Standardization. (2015c). ISO/IEC 27043: Information technology — Security techniques — Incident investigation principles and processes. ISO.

National Institute of Standards and Technology. (2014). NIST Special Publication 800-101 Revision 1: Guidelines on mobile device forensics. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-101r1

Riley v. California, 573 U.S. 373 (2014).

Ministerio Público Fiscal de la Provincia de Córdoba. (2026). Resolución FG N° 7/26: Aprobación del uso de CAPTA para la recolección de evidencia digital en dispositivos móviles. Fiscalía General de Córdoba.

Provincia del Chubut. (2026). Ley XV N° 43: Regulación del uso de herramientas tecnológicas en la investigación, prevención y lucha contra los delitos complejos y de cibercriminalidad. Boletín Oficial de la Provincia del Chubut, N° 14817, 20 de marzo de 2026.

Cámara de Acusación de Córdoba. (2020). Quipildor, Armando Andrés (Auto N° 332, 08/09/2020). Poder Judicial de la Provincia de Córdoba.

República Argentina. (2000). Ley N° 25.326 de Protección de los Datos Personales. Boletín Oficial.

República Argentina. (2019). Ley N° 27.483: Aprobación del Convenio 108 del Consejo de Europa. Boletín Oficial.

República Argentina. (2023). Ley N° 27.699: Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108+). Boletín Oficial.

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). Diario Oficial de la Unión Europea.
Ministerio Público Fiscal de la Provincia del Chubut. (2023). Espejo Chubut, el software creado en Chubut que permite validar a los chats y audios de WhatsApp en juicios. https://www.mpfchubut.gov.ar/centro-de-noticias/puerto-madryn/espejo-chubut-el-software-creado-en-chubut-que-permite-validar-a-los-chat-y-audios-de-whatsapp-en-juicios
Gabinete de Pericias Informáticas del Poder Judicial del Neuquén. (s.f.). Captura Digital. https://gpineuquen.gob.ar/CapturaDigital.html

Durante la preparación de este trabajo, los autores utilizaron Claude (Anthropic) con el fin de mejorar el lenguaje y la legibilidad del manuscrito. Tras utilizar esta herramienta, los autores revisaron y editaron el contenido según fuera necesario y asumen plena responsabilidad por el contenido de la publicación.