

Autenticación y contradicción de capturas de WhatsApp impugnadas en el proceso penal: revisión sistemática

Authentication and Adversarial Safeguards for Challenged WhatsApp Screenshots in Criminal Proceedings: A Systematic Review

Mariana de Jesús Verduga Álvarez¹

Doctora en Jurisprudencia, Abogada de los Tribunales de Justicia
Pontificia Universidad Católica del Ecuador sede Esmeraldas
PUCESE
(marianajva@hotmail.com) <https://orcid.org/0009-0007-4045-8998>

Como Citar:

Verduga Álvarez, M. de J. (2026). Autenticación y contradicción de capturas de WhatsApp impugnadas en el proceso penal: revisión sistemática. *Saber Estratégico Internacional*, 4(3), 1134–1154. <https://doi.org/10.70577/s.e.v4i3.109>

RESUMEN

Las capturas o impresiones de WhatsApp reproducen una conversación, aunque no conservan la relación con la fuente, los metadatos y el dispositivo de origen. En consideración de ello, el objetivo fue analizar los criterios de autenticación y las garantías de contradicción aplicables cuando su autenticidad ha sido impugnada en el proceso penal. Se realizó una revisión sistemática de publicaciones comprendidas entre 2021 y 2026. La búsqueda se efectuó en Scopus, Web of Science Core Collection y SciELO; el riesgo de sesgo se valoró mediante MMAT y JBI, mientras que los hallazgos se integraron mediante síntesis narrativa debido a la heterogeneidad de los estudios. La búsqueda permitió identificar 33 registros, se eliminaron siete por duplicación y 26 continuaron al cribado, posteriormente se evaluaron nueve estudios y ocho conformaron la síntesis final. Los criterios relacionaron el originador y el dispositivo con la fuente, la adquisición forense, la cadena de custodia, el hash, los metadatos, el contexto y la corroboración. Cabe resaltar que cinco estudios presentaron algunas preocupaciones y tres un riesgo alto, mientras que la inspección visual permitió orientar el examen, aunque no sustituyó la verificación técnica, en virtud de que determinadas herramientas pueden generar conversaciones ficticias semejantes a la interfaz. La captura impugnada no debe aceptarse ni excluirse de manera automática, debido a que su admisión y valoración requieren una base de autenticación proporcional al cuestionamiento y condiciones que permitan examinar la procedencia, integridad, atribución y completitud de la conversación.

Palabras clave: Autenticidad; Cadena de custodia; Contradicción; Evidencia digital; Proceso penal; WhatsApp.

ABSTRACT

WhatsApp screenshots and printouts reproduce the visible content of a conversation, although they do not necessarily preserve its relationship with the source, metadata, and originating device. In consideration of this problem, the objective was to analyze the authentication criteria and adversarial safeguards applicable when authenticity is challenged in criminal proceedings. A systematic review of publications from 2021 to 2026 was conducted. The search was carried out in Scopus, Web of Science Core Collection, and SciELO, while risk of bias was assessed using MMAT and JBI; because the studies were heterogeneous, the findings were integrated through a narrative synthesis. The search identified 33 records, of which seven were duplicates and 26 proceeded to screening; subsequently, nine full-text articles were assessed and eight studies formed the final synthesis. The criteria were related to identification of the originator and device, preservation of the source, forensic acquisition, chain of custody, hash calculation, metadata, complete context, and corroboration. It should be noted that five studies raised some concerns and three were judged at high risk, while visual inspection helped guide the examination but did not replace technical verification, because certain tools can generate fictitious conversations that resemble the interface. A challenged screenshot should not be automatically accepted or excluded, because its admission and assessment require an authentication foundation proportionate to the challenge and conditions that allow the defense to examine provenance, integrity, attribution, and completeness.

Keywords: Adversarial proceedings; Authenticity; Chain of custody; Criminal procedure; Digital evidence; WhatsApp.

INTRODUCCIÓN

Las conversaciones sostenidas mediante aplicaciones de mensajería se incorporan con frecuencia a las investigaciones penales, en virtud de que pueden relacionar personas, ubicar decisiones dentro de una secuencia temporal o documentar acuerdos, amenazas y otras conductas relevantes. Esta utilidad no elimina el problema de su forma de presentación, debido a que el proceso no siempre recibe el dispositivo, la base de datos o el archivo exportado, sino una captura de pantalla o una impresión que reproduce únicamente aquello que una persona decidió mostrar. La expansión de la evidencia digital en causas penales ha obligado a distinguir la existencia de información potencialmente pertinente de su autenticación y de su fuerza demostrativa, mientras que la jurisprudencia comparada mantiene respuestas diferentes frente a la procedencia, la integridad y la atribución de los contenidos electrónicos (Ashouri et al., 2014; Novak, 2019; Rawashdeh, 2017).

Una captura conserva la apariencia de la conversación, aunque no incorpora necesariamente los elementos que permiten establecer cómo fue obtenida, qué datos la acompañaron o si el contenido se encuentra completo, mientras que en el dispositivo pueden mantenerse bases de datos, registros de llamadas, identificadores, fechas, archivos multimedia y otros artefactos capaces de relacionar los mensajes con una cuenta y un equipo. Cabe resaltar que estos componentes pueden perderse, recortarse o modificarse cuando la información se presenta mediante una imagen; por ello, los estudios forenses sobre WhatsApp han demostrado que el examen del dispositivo y de los artefactos de la aplicación permite recuperar información adicional al texto visible, aunque su alcance depende del sistema operativo, la versión, el acceso disponible y el tipo de adquisición (Al Mutawa et al., 2012; Anglano, 2014; Azfar et al., 2016).

La presencia de un nombre, un número o el diseño habitual de WhatsApp tampoco permite resolver por sí sola la autenticidad, en virtud de que los datos de red, la señalización de llamadas y las condiciones de interceptación evidencian que una comunicación puede ser examinada desde distintos puntos de la infraestructura; por consiguiente, la verificación debe establecer qué fuente respalda el contenido y cuál es el alcance de cada artefacto (Karpisek et al., 2015; Wijnberg & Le-Khac, 2021). Así mismo, la rapidez con la que cambian las aplicaciones y los dispositivos exige documentar el procedimiento empleado, debido a que una conclusión técnica solo puede ser revisada cuando la adquisición, el examen y la presentación permanecen vinculados dentro de un proceso identificable (Kohn et al., 2013).

Desde la perspectiva jurídica, la autenticidad, la admisibilidad, la legalidad y la valoración corresponden a decisiones diferentes, en virtud de que una conversación puede resultar pertinente y, al mismo tiempo, presentar dudas sobre la persona a quien se atribuye. Así mismo, una copia puede ser admitida, aunque su peso disminuya cuando no se explica la ausencia del original, mientras que una evidencia técnicamente íntegra puede resultar inadmisibile si fue obtenida mediante la vulneración de derechos. Cabe resaltar que la preservación y la cadena de custodia permiten establecer que la información no cambió después de su adquisición, pero no demuestran por sí solas quién escribió el mensaje; por consiguiente, también deben examinarse el origen, el contexto y la corroboración (Ganja & Rodríguez Rafael, 2017).

Cuando una impresión es impugnada, la parte afectada requiere conocer el archivo de origen, acceder a los metadatos y examinar el procedimiento mediante el cual se produjo la evidencia, debido a que la ausencia de estas condiciones impide controvertirla de manera efectiva. En virtud de ello, la contradicción no se limita a permitir una objeción verbal durante la audiencia, sino que comprende las condiciones materiales

necesarias para verificar la fuente, formular hipótesis alternativas, solicitar o presentar un peritaje y contrainterrogar a quien realizó la extracción. La literatura disponible se distribuye entre estudios jurídicos, análisis técnicos de dispositivos, evaluaciones de herramientas y trabajos sobre percepción de los mensajes, situación que dificulta determinar cuáles criterios se repiten y cómo deben relacionarse dentro del juicio. Esta dificultad adquiere mayor relevancia cuando el contenido se imprime, se incorpora como anexo y circula dentro del expediente sin conservar la relación con el archivo electrónico que le dio origen, en virtud de que la reproducción puede terminar valorándose como un documento convencional. Cuando se pierde la relación entre la captura y el archivo electrónico que le dio origen, la objeción puede formularse cuando la fuente ya ha sido modificada o no se encuentra disponible, a lo cual se suma que puede permanecer bajo el control exclusivo de quien incorporó la reproducción.

En virtud de esta problemática, resultó necesario integrar los criterios jurídicos y forenses que permiten diferenciar una reproducción visual de una evidencia cuya procedencia e integridad puedan ser examinadas. En este contexto, el objetivo de la revisión fue analizar las publicaciones comprendidas entre 2021 y 2026 relacionadas con los criterios de autenticación y las garantías de contradicción aplicables a capturas de pantalla o impresiones de conversaciones de WhatsApp cuya autenticidad ha sido impugnada. La pregunta de investigación se formuló así: ¿Qué criterios se aplican a su admisión, incorporación y práctica en el proceso penal?

MATERIALES Y MÉTODOS

Diseño y pregunta de revisión

La investigación se desarrolló mediante una revisión sistemática con síntesis narrativa. Para presentar el proceso de identificación y selección de los estudios se utilizaron las orientaciones de PRISMA 2020, mientras que las cadenas y las decisiones de búsqueda fueron organizadas de acuerdo con PRISMA-S (Page et al., 2021; Rethlefsen et al., 2021). Para delimitar la pregunta de investigación se utilizó una estrategia PCC, en la cual las capturas, impresiones, transcripciones y registros de conversaciones de WhatsApp representaron la población o unidad de evidencia; la autenticidad, integridad, admisión, incorporación, cadena de custodia, peritaje y contradicción correspondieron al concepto; mientras que la investigación y el proceso penal conformaron el contexto. También se admitieron reglas generales y experiencias comparadas cuando presentaran criterios transferibles al problema penal.

Antes de ejecutar la búsqueda definitiva se elaboró un protocolo de trabajo no registrado, en el cual se definieron la pregunta de revisión, los criterios de elegibilidad, las fuentes de información, las variables de extracción y el procedimiento de evaluación metodológica. Estas decisiones se mantuvieron durante la selección y síntesis de los estudios, en virtud de que permitieron conservar la correspondencia entre la pregunta, los criterios aplicados y los resultados presentados.

Fuentes de información y estrategia de búsqueda

La búsqueda se efectuó el 7 de septiembre de 2026 en Scopus, Web of Science Core Collection y SciELO. Se aplicó el periodo 2021-2026 y se consideraron publicaciones en inglés y español. Los términos se organizaron en tres grupos relacionados con WhatsApp; evidencia digital y capturas; y autenticación, integridad, admisibilidad, cadena de custodia, contradicción y proceso penal. PubMed no formó parte de la

búsqueda, debido a que su cobertura no correspondió con el objeto jurídico-probatorio de la revisión. Antes de ejecutar la búsqueda definitiva se comprobó la sensibilidad de la cadena de Scopus; el término libre trial recuperó ensayos clínicos ajenos al objeto de estudio, por lo que fue reemplazado por expresiones penales específicas.

Las expresiones utilizadas se presentan en la Tabla 1. La información recuperada en Scopus se conservó en formato RIS con los datos bibliográficos, resúmenes, palabras clave y DOI. Los tres resultados identificados en SciELO fueron cribados mediante el título y el resumen, mientras que las siete publicaciones recuperadas en Web of Science correspondieron a registros previamente identificados en las otras bases y, por consiguiente, fueron retiradas como duplicados.

Tabla 1.

Estrategias de búsqueda ejecutadas y resultados

Base	Fecha	Cadena y filtros	n
Scopus	7-09-2026	TITLE-ABS-KEY((whatsapp OR "WhatsApp chat*" OR "WhatsApp conversation*" OR "WhatsApp message*") AND ("digital evidence" OR "electronic evidence" OR screenshot* OR "screen capture*" OR printout* OR transcript* OR "prueba digital" OR "evidencia digital" OR "evidencia electrónica" OR "captura* de pantalla") AND (authenticat* OR authenticit* OR integrity OR admissib* OR "chain of custody" OR forens* OR evidentiary OR contradiction OR confrontation OR "cross-examination" OR "due process" OR impugna* OR autentic* OR integridad OR admisib* OR "cadena de custodia" OR criminal* OR penal OR prosecution OR "criminal trial" OR courtroom OR court* OR judicial OR "proceso penal" OR "juicio penal")) AND PUBYEAR > 2020 AND PUBYEAR < 2027 AND (LIMIT-TO(LANGUAGE, "English") OR LIMIT-TO(LANGUAGE, "Spanish"))	23
Web of Science Core Collection	7-09-2026	TS=((WhatsApp OR "WhatsApp chat*" OR "WhatsApp conversation*" OR "WhatsApp message*") AND ("digital evidence" OR "electronic evidence" OR screenshot* OR "screen capture*" OR printout* OR transcript* OR "prueba digital" OR "evidencia digital" OR "evidencia electrónica" OR "captura* de pantalla") AND (authenticat* OR authenticit* OR integrity OR admissib* OR "chain of custody" OR forens* OR evidentiary OR contradiction OR confrontation OR "cross-examination" OR "due process" OR impugna* OR autentic* OR integridad OR admisib* OR "cadena de custodia" OR criminal* OR penal OR prosecution OR "criminal trial"	7

Base	Fecha	Cadena y filtros	n
		OR courtroom OR court* OR judicial OR "proceso penal" OR "juicio penal")); filtros: 2021-2026; inglés o español.	
SciELO	7-09-2026	(WhatsApp OR "mensajes de WhatsApp" OR "conversaciones de WhatsApp") AND ("prueba digital" OR "evidencia digital" OR autenticidad OR admisibilidad OR "captura de pantalla" OR penal OR criminal); idioma: español; años elegibles presentes: 2021 y 2023.	3

Fuente: elaboración propia a partir de los registros de búsqueda.

Criterios de elegibilidad

Los criterios de inclusión consideraron artículos, revisiones, capítulos y trabajos de congreso publicados entre 2021 y 2026 en inglés o español, con un método o corpus normativo, jurisprudencial o técnico identificable, relacionados con mensajes, conversaciones, capturas, impresiones, transcripciones o artefactos de WhatsApp y con evidencia proveniente de servicios de mensajería directamente comparable, además, debían incorporar al menos un componente de autenticación, integridad, manipulación, cadena de custodia, admisión, incorporación, práctica, impugnación, confrontación, contrainterrogatorio o debido proceso. Así mismo, se admitieron trabajos técnicos cuando sus resultados permitieran examinar la procedencia, recuperación, trazabilidad o detección de alteraciones, mientras que los estudios pertenecientes a otras materias fueron incluidos cuando sus criterios resultaran transferibles al proceso penal.

Se excluyeron las publicaciones en las cuales WhatsApp fue utilizado únicamente como canal de salud, educación, encuesta o comunicación organizacional, las investigaciones sobre detección de delitos, minería de mensajes o análisis de contenido que no incorporaron una dimensión probatoria, los estudios técnicos ajenos a la autenticación, integridad o fiabilidad, y los documentos de materias no penales que no permitieron una transferencia al proceso penal, así mismo, se retiraron las notas de opinión, noticias, textos sin una unidad académica analizable, publicaciones fuera del periodo o idioma establecido y registros duplicados.

Selección de los estudios

Los registros fueron consolidados por título, autoría, año y DOI, mientras que, cuando la coincidencia no permitió establecer su correspondencia, se compararon el resumen, la fuente y el objeto de análisis. Las decisiones adoptadas mediante el título y el resumen se conservaron en una matriz con el fundamento de inclusión o exclusión; posteriormente, se recuperaron los estudios potencialmente elegibles y se aplicaron nuevamente los criterios a la publicación completa, manteniendo en este nivel los registros en los cuales persistió una duda razonable. Cabe resaltar que los siete resultados de Web of Science ya se encontraban en las otras bases y fueron retirados como duplicados, mientras que los registros considerados inicialmente como no recuperados fueron reexaminados y excluidos por título y resumen; por consiguiente, todos los estudios buscados para el análisis de elegibilidad fueron recuperados.

La selección de los registros, la extracción de los datos y la evaluación metodológica fueron realizadas por una investigadora, mientras que las decisiones de inclusión y exclusión fueron contrastadas con los criterios

definidos en el protocolo. Cabe resaltar que, cuando persistió una duda razonable durante la revisión del título y el resumen, el registro continuó hasta la evaluación de la publicación completa; por consiguiente, no se excluyeron en el primer nivel aquellos estudios cuya relación con la autenticación o la contradicción no podía establecerse con suficiente claridad.

Extracción y síntesis de los datos

Para cada estudio se registraron la autoría, el año, la jurisdicción, la finalidad, el diseño o enfoque, el corpus o escenario, el tipo de registro de WhatsApp, la forma de adquisición, el criterio de atribución, el mecanismo de integridad, la cadena de custodia, los metadatos, la forma de incorporación, la respuesta ante la impugnación y las garantías de contradicción. Posteriormente, los hallazgos fueron organizados en la matriz de incluidos y contrastados con los artículos conservados, de este modo, su correspondencia permitió diferenciar los resultados expuestos de las inferencias transferibles al proceso penal.

La heterogeneidad entre los análisis jurídicos, las simulaciones de laboratorio, las comparaciones de herramientas, los estudios de percepción y las revisiones doctrinales impidió combinar los resultados mediante un estimador común; por consiguiente, se desarrolló una síntesis narrativa organizada en tres ejes: procedencia y atribución, integridad y trazabilidad, y contradicción durante la incorporación y práctica de la prueba. Los porcentajes y las cantidades se conservaron conforme fueron informados en cada estudio, mientras que las propuestas relacionadas con la decisión judicial se formularon como una integración razonada y no como reglas demostradas en una única jurisdicción.

Evaluación del riesgo de sesgo

El riesgo de sesgo se examinó de acuerdo con el tipo de evidencia, en virtud de que los seis estudios con componentes empíricos o técnico-experimentales fueron valorados mediante MMAT 2018, utilizando la categoría correspondiente a estudios cuantitativos descriptivos, no aleatorizados o de métodos mixtos, mientras que los dos estudios exclusivamente doctrinales se examinaron con la lista JBI para evidencia textual narrativa (Hong et al., 2018; McArthur et al., 2025). Para integrar la presentación de los resultados, los criterios aplicables fueron organizados en cinco dominios relacionados con la claridad de la pregunta o fuente, la selección del corpus, la adecuación del procedimiento o medición, la coherencia del análisis e integración, y la transparencia de la interpretación. Las respuestas afirmativa, incierta y negativa se representaron como bajo riesgo, algunas preocupaciones y alto riesgo, respectivamente; cabe resaltar que no se calcularon puntuaciones numéricas, debido a que el juicio global consideró si las limitaciones identificadas podían modificar la confianza otorgada al aporte principal de cada estudio.

RESULTADOS

Selección de los estudios

El proceso de selección se presenta en la Figura 1. La búsqueda permitió identificar 33 registros. Se eliminaron siete duplicados y 26 continuaron al cribado; posteriormente, se evaluaron nueve estudios y ocho conformaron la síntesis final.

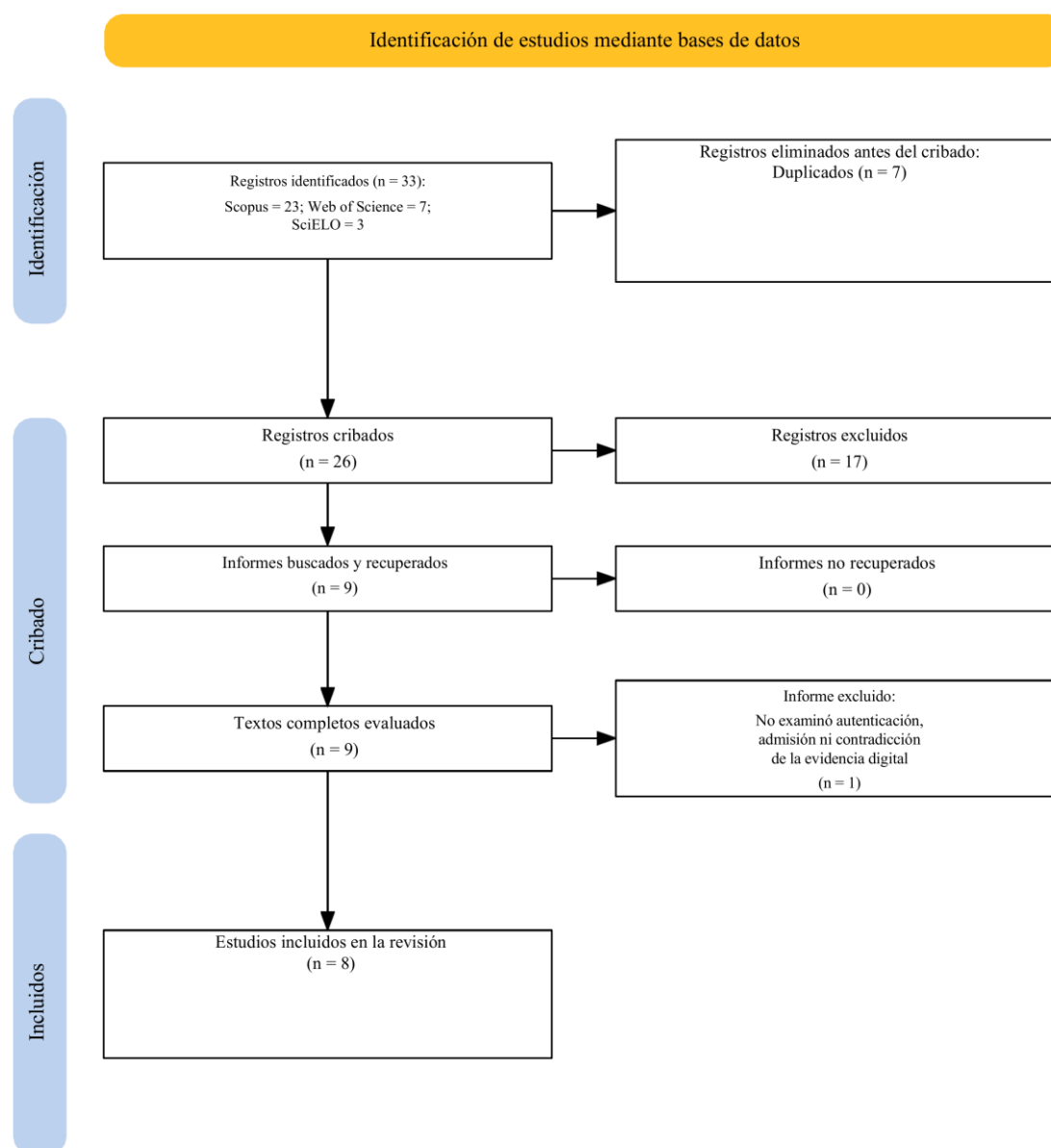
Los 17 registros excluidos mediante el título y el resumen no reunieron de manera conjunta la unidad de evidencia, la dimensión probatoria y el criterio de autenticidad o contradicción establecido en el protocolo, en virtud de que correspondieron a trabajos sobre falsificación de videos o imágenes, análisis de contenido,

detección de conductas, aplicaciones distintas de WhatsApp o procedimientos técnicos sin una transferencia suficiente a la admisión o práctica de la evidencia impugnada. Cabe resaltar que los registros en los cuales permaneció una duda razonable continuaron a la evaluación a texto completo, mientras que la decisión del primer nivel se sustentó en el título y el resumen disponibles.

Entre los nueve estudios evaluados se conservaron aquellos que formularon reglas jurídicas aplicables a las comunicaciones digitales o que permitieron examinar la fuente, la integridad, la recuperación o la detección de alteraciones. El único artículo excluido a texto completo utilizó grafos de conocimiento y procesamiento de lenguaje natural para analizar datos de mensajería dentro de una investigación, aunque no abordó la autenticación, la admisión ni las garantías de contradicción de la evidencia; por consiguiente, no se incorporaron categorías de exclusión que no presentaron casos observados.

Figura 1.

Diagrama de flujo de la selección de estudios



Fuente: elaboración propia con base en PRISMA 2020.

Características de los estudios incluidos

Los ocho estudios fueron publicados entre 2021 y 2024, correspondiendo uno a 2021, cuatro a 2022, dos a 2023 y uno a 2024. Tres investigaciones se desarrollaron en Indonesia, mientras que las demás procedieron de Sudáfrica, Reino Unido, India, Estados Unidos y Colombia. Los diseños comprendieron tres simulaciones o evaluaciones técnicas de laboratorio, dos estudios exclusivamente jurídico-doctrinales, una investigación sociojurídica de orientación empírica, un estudio experimental de percepción y un estudio de autenticidad visual de registros de comunicación, lo cual permitió relacionar criterios jurídicos con procedimientos de recuperación, aunque limitó la transferencia directa de una regla uniforme entre jurisdicciones.

El objeto de análisis tampoco fue homogéneo, en virtud de que cuatro estudios examinaron directamente artefactos, bases de datos o capturas de WhatsApp, dos abordaron evidencia electrónica o comunicaciones digitales dentro de reglas generales de admisibilidad, uno comparó la capacidad de herramientas para recuperar artefactos de redes sociales y otro evaluó la respuesta de personas no expertas ante distintas explicaciones sobre la posibilidad de falsificar una captura. Cabe resaltar que el estudio colombiano fue desarrollado en procesos de divorcio, aunque se incorporó porque examinó de manera expresa la autenticidad, el hash, la cadena de custodia y la contradicción de mensajes impresos, elementos transferibles al problema penal (Gómez Agudelo et al., 2021).

Tabla 2.*Características de los estudios incluidos*

Autor y año	Jurisdicción y contexto	Diseño o corpus	Procedimiento	Aporte principal
Cahyanto et al. (2022)	Indonesia; laboratorio	Simulación de amenazas y terrorismo; tres condiciones de WhatsApp Desktop	Adquisición live forensic desde RAM, verificación MD5/SHA-1 y análisis manual	La recuperación se relacionó con el estado de la aplicación y el momento de adquisición, mientras que el original fue conservado y la copia se verificó mediante el hash.
Herman et al. (2022)	Indonesia; laboratorio	Comparación de Magnet Axion y MOBILEdit Forensics en Android	Proceso NIST: preservación, adquisición, examen, análisis y reporte	Las dos herramientas permitieron recuperar artefactos de WhatsApp,

Autor y año	Jurisdicción y contexto	Diseño o corpus	Procedimiento	Aporte principal
				aunque Axiom alcanzó 92,31 % y MOBILEdit 79,49 % en el índice informado.
Uys y Joubert (2022)	Sudáfrica; penal y civil	Revisión de legislación, jurisprudencia y literatura sobre correo, SMS y WhatsApp	Autenticidad, admisibilidad, original o mejor alternativa, originador y cadena de custodia	La impugnación de la autenticidad requirió examinar de manera conjunta la fuente, la identificación del originador, la integridad, el contexto y el conocimiento forense.
Horsman (2023)	Reino Unido; investigación penal	Estudio de 41 registros ficticios de WhatsApp, iMessage y Twitter	Evaluación visual mediante marcas de interfaz y comparación con registros genuinos	Ningún generador reprodujo por completo la interfaz original; sin embargo, varias imágenes mantuvieron una apariencia semejante y el recorte redujo las señales disponibles para detectar la falsificación.
Maria y Maria (2022)	India; comparación con EE. UU. y Reino Unido	Análisis doctrinal y jurisprudencial sobre evidencia electrónica	Original, evidencia secundaria, certificado, testimonio y peritaje	La forma de incorporación determinó los requisitos aplicables, mientras que la evidencia secundaria requirió

Autor y año	Jurisdicción y contexto	Diseño o corpus	Procedimiento	Aporte principal
				una base específica susceptible de examen.
Reitinger et al. (2023)	Estados Unidos; escenario penal	Dos encuestas experimentales, n = 1.200, con captura acusatoria y seis defensas	Negación simple, explicación experta y demostraciones de falsificación	La negación sin respaldo presentó menor efectividad, mientras que mostrar o permitir el uso de una herramienta de falsificación modificó con mayor intensidad la creencia y la decisión.
Sudiana et al. (2024)	Indonesia; laboratorio	Seis escenarios de mensajes temporales en Android no rooteado	NIST SP 800-101r1, copias de respaldo, bases de datos y registro de notificaciones	Se recuperó 83,33 % de los mensajes desaparecidos; la pérdida de una copia de respaldo impidió recuperar el resto.
Gómez Agudelo et al. (2021)	Colombia; proceso de familia, transferencia penal	Investigación sociojurídica de orientación empírica con revisión documental, grupo focal, cinco entrevistas semiestructuradas y observación no participante	Impresión, captura, archivo original, extracción pericial, cadena y hash	La impresión aislada limita el estudio pericial y puede afectar defensa y contradicción cuando se cuestiona la autenticidad.

Fuente: elaboración propia a partir de los estudios incluidos.

Criterios de autenticación

La primera dimensión se relacionó con la atribución, Uys y Joubert (2022) señalaron que el texto visible no identifica por sí solo al remitente, debido a que el número, la propiedad o uso del dispositivo, la cuenta y los demás datos deben vincular al originador con la comunicación, mientras que la corroboración puede efectuarse mediante registros del propio dispositivo, información de ubicación, llamadas, documentos asociados o conducta posterior. En virtud de ello, el nombre visible en la cabecera de una captura constituye un indicio configurable por el usuario y no una prueba autónoma de autoría.

La segunda dimensión correspondió a la procedencia de la reproducción. Cahyanto et al. (2022) recuperaron quince artefactos en la simulación intacta, diez cuando la sesión había cambiado y seis después de eliminar el chat, aunque no recuperaron el texto de la conversación en la última condición; así mismo, compararon los valores MD5 y SHA-1 de la fuente y la copia, manteniendo el original sin examen directo. Herman et al. (2022) evaluaron Magnet Axion y MOBILedit Forensics mediante pruebas de adquisición, interpretación y hashing, las dos herramientas superaron las pruebas realizadas, aunque presentaron limitaciones diferentes, por consiguiente, los resultados deben interpretarse de acuerdo con la herramienta empleada, su configuración y el alcance de la extracción.

En la tercera dimensión se examinó la suficiencia de la inspección visual, Horsman (2023) analizó 41 registros ficticios y ningún servicio reprodujo por completo las marcas de una interfaz genuina, mientras que las imitaciones de WhatsApp alcanzaron promedios de coincidencia de 72,42 % en Android y 59,36 % en iOS, cabe resaltar que el recorte podía eliminar componentes necesarios para reconocer la falsificación. En virtud de ello, el tamaño de fuente, los iconos, el color, las horas y la disposición de los mensajes pueden contribuir a identificar inconsistencias, pero una apariencia correcta no permite confirmar la autenticidad.

La cuarta dimensión comprendió la volatilidad y la completitud. Sudiana et al. (2024) recuperaron 83,33 % de los mensajes temporales mediante bases de datos de respaldo y registros de notificaciones, aunque no pudieron recuperar el resto cuando faltó la copia programada. Este resultado evidenció que la ausencia del mensaje en la interfaz no significa que no existan artefactos, mientras que la existencia de una captura tampoco demuestra que la secuencia esté completa. La autenticación debe documentar el periodo examinado, las funciones activas, los mensajes anteriores y posteriores, los adjuntos y los vacíos que no pudieron reconstruirse.

Tabla 3.*Criterios integrados para autenticar una captura o impresión impugnada*

Dimensión	Pregunta de control	Elementos verificables	Límite
Fuente y procedencia	¿De qué dispositivo, cuenta, archivo o base de datos se obtuvo la captura?	Dispositivo original, archivo exportado, base de datos, copia forense, ruta y fecha de adquisición.	La procedencia resulta insuficiente cuando la captura fue recibida por reenvío y no puede relacionarse con una fuente verificable.

Dimensión	Pregunta de control	Elementos verificables	Límite
Atribución	¿Qué vincula el mensaje con la persona a quien se atribuye?	Número, titularidad o uso del dispositivo, identificadores de cuenta, contactos, llamadas, ubicación, testimonio y conducta corroborante.	El nombre y la fotografía visibles pueden ser configurados por un tercero; por ello, no demuestran por sí solos la atribución.
Integridad	¿La información presentada es la misma que fue adquirida?	Hash de la fuente y de las copias, imagen bit a bit, preservación del original y registro de cada transferencia.	El hash permite comprobar que el archivo no cambió desde su cálculo, pero no demuestra la veracidad del contenido ni permite establecer una autoría anterior.
Complejidad y contexto	¿La conversación está íntegra y conserva su secuencia?	Mensajes anteriores y posteriores, fechas, adjuntos, respuestas, reenvíos, ediciones, eliminaciones y vacíos identificados.	El recorte puede excluir información relevante sin modificar los píxeles que permanecen en la imagen.
Validación técnica	¿El método y la herramienta permiten repetir o revisar el resultado?	Versión de aplicación y sistema, herramienta, parámetros, registros de ejecución, limitaciones y resultado reproducible.	Las herramientas recuperan artefactos diferentes y no superan los mismos controles; por ello, el resultado debe examinarse de acuerdo con su alcance.
Corroboración	¿Existen elementos independientes compatibles con el contenido?	Metadatos, registros de llamadas, archivos multimedia, copias de respaldo, notificaciones, proveedor y otros testimonios.	La corroboración puede reforzar la fiabilidad del contenido, aunque cada fuente requiere una autenticación independiente.

Fuente: elaboración propia a partir de la síntesis de los estudios incluidos.

Incorporación, práctica y garantías de contradicción

La forma utilizada para incorporar la conversación modificó las posibilidades de contradicción. Gómez Agudelo et al. (2021) diferenciaron el archivo original de la impresión o captura y de la extracción forense

acompañada de informe, testimonio experto y cadena de custodia, debido a que la impresión transforma un mensaje integrado por datos y metadatos en un documento estático, por consiguiente, no permite efectuar el mismo examen que la fuente. Uys y Joubert (2022) señalaron que, cuando el original no se presenta, debe justificarse que la alternativa incorporada corresponde a la mejor opción razonablemente disponible, además, debe examinarse la fiabilidad de la generación, el almacenamiento, la comunicación y la identificación del originador.

El análisis jurídico comparado mostró que la impugnación no produce una consecuencia idéntica en todas las jurisdicciones. Maria y Maria (2022) describieron que el régimen indio diferencia el original electrónico de la evidencia secundaria y exige para esta última el cumplimiento de las condiciones y el certificado previsto en la sección 65B, mientras que el testimonio de quien operó o produjo el dispositivo puede sustentar la evidencia original. La revisión también presentó experiencias estadounidenses y británicas en las cuales la autenticación, el testimonio experto, la regla del original y la posibilidad de contrainterrogar forman parte de un examen articulado.

La impugnación tampoco puede reducirse a una afirmación general de que cualquier captura es falsificable. En el escenario penal de Reitinger et al. (2023), dos tercios de quienes recibieron únicamente una negación simple mantuvieron la creencia en la captura acusatoria, mientras que las condiciones que incorporaron evidencia sobre la falsificación hicieron a los participantes entre 5,6 y 10,7 veces más propensos a desplazar su creencia y entre 1,5 y 1,8 veces más propensos a decidir no culpabilidad frente a la condición de referencia. Cabe resaltar que la demostración de una herramienta fue más comprensible que una explicación criptográfica aislada, por consiguiente, la contradicción efectiva requiere una hipótesis técnica examinable y no solamente la posibilidad abstracta de manipulación.

Tabla 4.

Garantías necesarias para la contradicción de la evidencia

Garantía	Contenido operativo	Finalidad procesal
Acceso a la fuente	Entrega o exhibición del dispositivo, archivo original, exportación o copia forense disponible.	Comparar la captura con la conversación e identificar la información que no fue incorporada.
Acceso a datos y documentación	Metadatos, hashes, cadena de custodia, registros de adquisición, versión de la aplicación y parámetros.	Examinar la procedencia, integridad, límites y continuidad del manejo.
Tiempo y medios adecuados	Disponibilidad previa a la audiencia y plazo para analizar volúmenes, formatos y cifrado.	Evitar que la defensa conozca la base técnica cuando ya no dispone de tiempo para preparar una respuesta útil.
Asistencia pericial	Perito propio, examen independiente o asistencia técnica cuando la complejidad lo requiera.	Formular hipótesis alternativas y comprobar si el método aplicado fue adecuado.

Garantía	Contenido operativo	Finalidad procesal
Interrogatorio y contrainterrogatorio	Comparecencia de quien obtuvo, preservó o analizó la información.	Examinar la fuente, la selección, la herramienta utilizada, los posibles errores y sus limitaciones.
Decisión motivada	Separación entre legalidad, autenticidad, admisibilidad y peso probatorio.	Impedir que la apariencia de la captura o la ausencia de una prueba defensiva sustituyan la carga de autenticación.

Fuente: elaboración propia a partir de la síntesis de los estudios incluidos.

Evaluación del riesgo de sesgo

La evaluación se presenta en la Figura 2. El riesgo global se clasificó con algunas preocupaciones en Cahyanto et al. (2022), Herman et al. (2022), Uys y Joubert (2022), Horsman (2023) y Reitinger et al. (2023), mientras que Maria y Maria (2022), Sudiana et al. (2024) y Gómez Agudelo et al. (2021) presentaron riesgo alto; por consiguiente, ningún estudio alcanzó un juicio global bajo. Las principales dificultades correspondieron a la selección limitada de dispositivos, escenarios, servicios o fuentes, la ausencia de replicaciones independientes, la falta de descripción del procedimiento de integración y análisis en los estudios jurídicos, y la subjetividad no contrastada de la inspección visual. Cabe resaltar que Reitinger et al. (2023) informó pilotos, criterios de exclusión, modelos estadísticos, corrección por comparaciones múltiples, concordancia entre codificadores y una segunda encuesta de réplica; sin embargo, la asignación a las condiciones no fue descrita con suficiente detalle y la muestra procedió de una plataforma de participación en línea.

Figura 2. Evaluación del riesgo de sesgo de los estudios incluidos

Estudio	Instrumento	D1	D2	D3	D4	D5	Global
Cahyanto et al. (2022)	MMAT						
Herman et al. (2022)	MMAT						
Uys y Joubert (2022)	JB1						
Horsman (2023)	MMAT						
Maria y Maria (2022)	JB1						
Reitinger et al. (2023)	MMAT						
Sudiana et al. (2024)	MMAT						
Gómez Agudelo et al. (2021)	MMAT						

Dominios:

D1: pregunta o fuente D2: selección del corpus D3: procedimiento o medición
D4: análisis e integración D5: transparencia e interpretación

Juicio:

Bajo
 Algunas preocupaciones
 Alto

MMAT: Mixed Methods Appraisal Tool. JB1: lista para evidencia textual narrativa.

Fuente: elaboración propia mediante MMAT 2018 y la lista JB1 para evidencia textual narrativa.

DISCUSIÓN

Los hallazgos evidenciaron que una captura impugnada no puede autenticarse mediante un único requisito, debido a que la apariencia, el hash, la cadena de custodia, los metadatos y el peritaje responden a dimensiones diferentes. La apariencia permite advertir incoherencias, mientras que el hash establece si el archivo cambió desde un momento determinado, la cadena de custodia identifica a las personas que manejaron la evidencia y los metadatos relacionan el contenido con una fuente; así mismo, el peritaje explica el procedimiento aplicado y sus limitaciones. En virtud de ello, la procedencia, atribución, integridad, completitud y corroboración deben examinarse de manera conjunta, incrementando la verificación cuando la impugnación plantea una posible edición, suplantación, recorte o fabricación.

Esta integración coincide con los trabajos que proponen validar por separado la tecnología, el método y su aplicación al caso, en virtud de que una herramienta aceptada no garantiza que haya sido utilizada correctamente ni que el artefacto interpretado responda a la pregunta jurídica (Stoykova & Franke, 2023). La conclusión forense también debe presentar las alternativas y el alcance de los datos, evitando que una afirmación categórica o la autoridad del experto oculten la incertidumbre existente (Casey, 2020); cabe resaltar que esta exigencia adquiere mayor relevancia cuando la captura de WhatsApp constituye la única fuente presentada, debido a que el juzgador podría relacionar la familiaridad de la interfaz con una autenticidad que todavía no ha sido verificada.

El hash requiere una consideración semejante. Los sistemas de cadena electrónica muestran que el valor criptográfico puede permitir una comprobación independiente de que el archivo no cambió después de su registro, siempre que también se documente el momento, la identidad del responsable y la secuencia de transferencias (Burri et al., 2020). Otras propuestas han utilizado blockchain para mejorar la inmutabilidad, la trazabilidad y la auditoría del manejo de evidencia, aunque su utilidad depende de que la información inicial haya sido adquirida correctamente y de que el sistema conserve una relación demostrable con la fuente (Lone & Mir, 2019; Tsai, 2021). En virtud de ello, calcular el hash de una captura recibida no corrige una atribución incierta ni demuestra que la imagen represente la conversación completa; únicamente fija el archivo que fue sometido al cálculo.

La contradicción efectiva debe examinarse como una condición material del juicio y no como la posibilidad formal de objetar. El derecho a un proceso justo frente a evidencia digital exige reglas que permitan cuestionar su obtención, su fiabilidad y su utilización, en virtud de que la complejidad técnica puede colocar a la defensa en desventaja aunque ambas partes tengan acceso nominal al expediente (Stoykova, 2023). Esta dificultad se amplía cuando la fiscalía dispone del dispositivo, las herramientas y el conocimiento especializado, mientras que la defensa recibe solamente un informe o una reproducción; por ello, el acceso a los datos subyacentes, a la cadena de evidencia, a las validaciones y a una asistencia forense razonable forma parte de una precisión procesal susceptible de corrección (Stoykova, 2024).

La evidencia digital también puede producir un desequilibrio por su volumen, su opacidad y la confianza que genera una salida tecnológica. En procedimientos internacionales, la dependencia de fuentes digitales ha sido relacionada con problemas de igualdad de armas cuando la defensa no puede examinar la procedencia o reproducir el análisis (de Arcos Tejerizo, 2023). De manera concordante, abogados defensores han informado dificultades para interpretar formatos, obtener asesoramiento y mantenerse al día con el cambio tecnológico, situación que incide en la capacidad de identificar una limitación relevante antes

del juicio (Wilson-Kovacs et al., 2023). Estas observaciones respaldan que el tribunal no traslade a la persona acusada la obligación de demostrar una falsificación cuando quien presenta la captura todavía no ha explicado su origen y fiabilidad.

La cooperación para obtener evidencia alojada por proveedores añade otra diferencia entre integridad y legalidad. Una información técnicamente preservada puede haber sido conseguida mediante un procedimiento incompatible con las garantías aplicables, mientras que una obtención autorizada puede resultar incompleta o insuficientemente autenticada. El análisis europeo sobre evidencia electrónica transfronteriza ha resaltado que la fiabilidad exige conservar un régimen adecuado en cada etapa de recolección y procesamiento, sin que ello sustituya las reglas de autorización, necesidad y protección de derechos (Rojszczak, 2022). En este sentido, el juez debe resolver primero si la obtención fue lícita y luego establecer si el material corresponde a lo que afirma representar, evitando que la cadena de custodia se utilice como respuesta automática a todas las objeciones.

Con base en los resultados, el examen de una captura impugnada se organizó en seis decisiones relacionadas entre sí, la primera correspondió a determinar la proposición que se pretende probar, debido a que demostrar la existencia de un intercambio no significa atribuir cada mensaje a una persona, la segunda comprendió la identificación de la fuente y la ruta seguida desde el dispositivo hasta el expediente, la tercera se relacionó con la verificación de la integridad mediante originales, copias forenses, hashes y registros de custodia, mientras que la cuarta examinó la completitud y el contexto, incluyendo los mensajes omitidos, adjuntos, reenvíos y funciones temporales. La quinta decisión comprendió el acceso oportuno de la defensa, la asistencia técnica y el contrainterrogatorio, mientras que la sexta diferenció la legalidad, la admisión y el peso atribuido a la evidencia, indicando las dudas que permanecieron y las corroboraciones utilizadas para resolverlas.

La completitud debe valorarse de manera independiente, debido a que una imagen puede permanecer intacta y presentar una versión parcial de la conversación, la selección de mensajes, el recorte de la cabecera, la ausencia de respuestas anteriores, la omisión de adjuntos y la pérdida de una secuencia temporal pueden cambiar el sentido sin producir una señal de edición en el archivo incorporado. Por consiguiente, cuando la impugnación se encuentra relacionada con el contexto, no resulta suficiente comprobar que la captura permaneció sin cambios después de su recepción, en virtud de que debe ser comparada con la conversación disponible para identificar los fragmentos ausentes y determinar si la parte incorporada representa de manera adecuada aquello que se pretende probar.

El nivel de exigencia debe guardar relación con la controversia, debido a que una captura reconocida por ambas partes y corroborada mediante hechos independientes no presenta el mismo problema que una imagen aislada cuya autoría, secuencia y origen han sido negados. Esta proporcionalidad no significa que la defensa deba demostrar la falsificación, debido a que quien incorpora la evidencia debe presentar primero una base suficiente sobre su procedencia, mientras que la objeción específica permite orientar el examen hacia una cuenta, un dispositivo, una fecha o una alteración concreta. Cabe resaltar que la ausencia de recursos técnicos no puede considerarse como la aceptación de una evidencia que todavía no ha sido examinada.

Aplicación de los criterios al proceso penal ecuatoriano

En el proceso penal ecuatoriano, la incorporación de una captura de WhatsApp debe relacionarse con las garantías constitucionales que regulan la obtención, actuación y contradicción de la prueba, en virtud de que el artículo 76, numeral 4, establece que las pruebas obtenidas o actuadas con violación de la Constitución o la ley carecen de validez y eficacia probatoria, mientras que el numeral 7, literales b), d), h) y j), reconoce el tiempo y los medios adecuados para preparar la defensa, el acceso a los documentos y actuaciones, la presentación y contradicción de las pruebas y la posibilidad de interrogar a testigos y peritos (Constitución de la República del Ecuador, 2008, art. 76).

Estas garantías permiten establecer que la contradicción no se cumple únicamente cuando la defensa puede formular una objeción durante la audiencia, debido a que la autenticidad impugnada exige acceso oportuno a los elementos utilizados para establecer la procedencia, integridad, atribución y completitud de la conversación, así como tiempo suficiente para formular una hipótesis alternativa, solicitar asistencia pericial y contrainterrogar a la persona que realizó la adquisición o el análisis. Por consiguiente, una reproducción que llega al juicio separada del dispositivo, el archivo o el procedimiento mediante el cual fue obtenida puede limitar materialmente la defensa, aunque formalmente se permita cuestionarla.

De igual manera, el artículo 454, numerales 3 y 7, del Código Orgánico Integral Penal reconoce la contradicción y la igualdad de oportunidades para la prueba; el artículo 456 aplica la cadena de custodia a los elementos físicos y al contenido digital con la finalidad de garantizar su autenticidad, identidad y estado original, mientras que el artículo 457 exige valorar la legalidad, autenticidad, sometimiento a cadena de custodia y aceptación científica y técnica de los principios que sustentan los informes periciales. Cabe resaltar que esta última disposición asigna a la parte que presenta los elementos no sometidos a cadena de custodia la demostración de su autenticidad (Código Orgánico Integral Penal, 2014, arts. 454, 456-457).

El tratamiento jurídico del contenido digital no concluye con su preservación, debido a que el artículo 500 dispone que el análisis, la valoración, la recuperación y la presentación deben efectuarse mediante técnicas digitales forenses. De igual manera, el artículo 616.1 establece que el contenido que pretende incorporarse como prueba digital debe exhibirse o reproducirse en su formato original y acreditarse mediante el testimonio pericial correspondiente, explicando la cadena de custodia, la integridad y la autenticidad de acuerdo con dichas técnicas (Código Orgánico Integral Penal, 2014, arts. 500 y 616.1). En virtud de ello, una captura aislada no puede equipararse con la adquisición de la fuente ni con el examen técnico de los datos relacionados con la conversación.

En el proceso penal ecuatoriano, una captura impugnada no adquiere autenticidad por reproducir la interfaz de WhatsApp, mostrar un nombre o número telefónico o encontrarse incorporada materialmente en el expediente, debido a que quien la presenta debe relacionarla con el dispositivo, la cuenta, el archivo, la conversación o el procedimiento de extracción, además de explicar la continuidad entre su obtención y presentación. El hash permite comprobar que el archivo no cambió después de su cálculo, mientras que la cadena de custodia documenta su manejo, cabe resaltar que ninguno de estos elementos permite establecer por sí solo quién produjo los mensajes ni demostrar que la conversación se encuentra completa.

Cuando la impugnación se encuentra relacionada con una posible edición, suplantación, selección parcial o modificación del contexto, la defensa debe contar con acceso al dispositivo o a la copia forense disponible, los metadatos, los valores hash, el registro de custodia, la herramienta utilizada, sus parámetros y las

limitaciones del procedimiento, además, debe tener la posibilidad de interrogar a la persona que obtuvo o analizó la información. Esta posibilidad no significa que la defensa deba demostrar inicialmente la falsificación, debido a que corresponde a la parte que presenta la captura establecer primero su procedencia y autenticidad. Por consiguiente, la hipótesis defensiva orienta la intensidad del examen, pero no sustituye la carga de autenticación.

La consecuencia procesal depende de la deficiencia identificada, en virtud de que la obtención contraria a la Constitución o la ley, la ausencia de una base mínima de autenticidad y las dudas sobre atribución, completitud o contexto no producen el mismo efecto. Cuando la prueba fue obtenida o actuada con vulneración normativa carece de validez y eficacia probatoria, mientras que la captura que no puede relacionarse con una fuente verificable no debería sostener por sí sola la proposición para la cual fue presentada, sin embargo, cuando la fuente ha sido identificada y permanecen limitaciones sobre la atribución, completitud o contexto, estas deben someterse a contradicción y considerarse de manera expresa al motivar el peso probatorio. Por consiguiente, legalidad, autenticidad, admisibilidad y valoración corresponden a decisiones relacionadas, aunque no intercambiables.

Limitaciones

Las limitaciones de la revisión deben considerarse al interpretar la propuesta, en virtud de que cinco estudios presentaron algunas preocupaciones y tres un riesgo alto, principalmente por la selección limitada de dispositivos, escenarios o fuentes y por la ausencia de replicación o de procedimientos analíticos suficientemente detallados. A lo cual se suma que la selección de los registros, la extracción de los datos y la evaluación metodológica fueron realizadas por una investigadora, situación que puede incrementar la posibilidad de errores o de decisiones dependientes del juicio individual. El número de estudios incluidos fue reducido y los diseños no correspondieron a una misma tradición metodológica, mientras que parte de la evidencia procedió de simulaciones técnicas y una investigación jurídica fue desarrollada en procesos de familia, aunque sus mecanismos resultaron transferibles. En el contexto ecuatoriano no se identificaron estudios que examinaran de manera conjunta la impugnación, el análisis pericial y la decisión judicial dentro de causas penales, a lo cual se suma que las aplicaciones, los sistemas operativos y las herramientas cambian con rapidez, por consiguiente, los porcentajes de recuperación o coincidencia visual no deben utilizarse como umbrales generales. La búsqueda consideró publicaciones académicas de tres bases durante el periodo 2021-2026, situación que pudo excluir jurisprudencia y documentos técnicos no indexados, de este modo, los criterios integrados pueden utilizarse como una estructura de análisis, pero no como una regla automática de admisión.

CONCLUSIONES

Los resultados permitieron establecer que la captura de pantalla o la impresión de una conversación de WhatsApp constituye una representación derivada, debido a que su valor no depende únicamente de aquello que puede observarse. Cuando la autenticidad ha sido impugnada, se debe relacionar la imagen con una fuente identificable, comprobar la continuidad entre la adquisición y la presentación, establecer la atribución del mensaje, conservar el contexto y verificar la existencia de artefactos independientes compatibles con la conversación, en virtud de que estos elementos permiten examinar si la reproducción corresponde con el contenido que se pretende incorporar. Cabe resaltar que la inspección visual permite

advertir inconsistencias, aunque no confirma la autenticidad, mientras que el hash y la cadena de custodia demuestran estabilidad y trazabilidad desde un momento determinado, pero no establecen quién produjo el mensaje ni corrigen una conversación incompleta, por consiguiente, la suficiencia no depende de un único medio, sino de la coincidencia entre la fuente, los metadatos, el testimonio, la pericia y otras corroboraciones verificables.

La garantía de contradicción exige que la defensa conozca y pueda examinar el dispositivo, el archivo o la copia forense disponible, los metadatos, los valores hash, la cadena de custodia, la herramienta, los parámetros y las limitaciones del procedimiento, así mismo, requiere tiempo suficiente, asistencia pericial cuando sea necesaria y la posibilidad de interrogar a quien obtuvo o analizó la evidencia. En virtud de ello, la captura impugnada no debe ser aceptada únicamente porque su apariencia resulte familiar ni excluida por la posibilidad de manipulación, debido a que el tribunal debe exigir una base de autenticación proporcional al cuestionamiento, diferenciar la autenticidad de la legalidad y motivar el peso atribuido a la reproducción después de que la contradicción se haya desarrollado en condiciones reales. La principal brecha identificada correspondió a la ausencia de estudios penales ecuatorianos que documenten esta secuencia dentro de casos concretos, por consiguiente, las investigaciones posteriores deberán examinar las decisiones judiciales, las prácticas de fiscalía y defensa, el acceso a peritajes y los criterios utilizados para resolver las impugnaciones de conversaciones digitales.

REFERENCIAS BIBLIOGRÁFICAS

- Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9, S24-S33. <https://doi.org/10.1016/j.diin.2012.05.007>
- Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3), 201-213. <https://doi.org/10.1016/j.diin.2014.04.003>
- Ashouri, A., Bowers, C., & Warden, C. (2014). An overview of the use of digital evidence in international criminal courts. *Digital Evidence and Electronic Signature Law Review*, 11. <https://doi.org/10.14296/deeslr.v11i0.2130>
- Azfar, A., Choo, K.-K. R., & Liu, L. (2016). An Android communication app forensic taxonomy. *Journal of Forensic Sciences*, 61(5), 1337-1350. <https://doi.org/10.1111/1556-4029.13164>
- Burri, X., Casey, E., Bollé, T., & Jaquet-Chiffelle, D.-O. (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation*, 33, 300976. <https://doi.org/10.1016/j.fsidi.2020.300976>
- Cahyanto, T. A., Rizal, M. A., Wardoyo, A. E., Warisaji, T. T., & Daryanto. (2022). Live forensic to identify the digital evidence on the desktop-based WhatsApp. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 6(2), 213-219. <https://doi.org/10.29207/resti.v6i2.3849>
- Casey, E. (2020). Standardization of forming and expressing preliminary evaluative opinions on digital evidence. *Forensic Science International: Digital Investigation*, 32, 200888. <https://doi.org/10.1016/j.fsidi.2019.200888>
- Código Orgánico Integral Penal. (2014). Registro Oficial Suplemento 180 de 10 de febrero de 2014.
- Constitución de la República del Ecuador. (2008). Registro Oficial 449 de 20 de octubre de 2008.

- de Arcos Tejerizo, M. (2023). Digital evidence and fair trial rights at the International Criminal Court. *Leiden Journal of International Law*, 36(3), 749-769. <https://doi.org/10.1017/S0922156523000031>
- Gómez Agudelo, D. S., Acevedo Valencia, J. M., & Aguirre Espinosa, J. E. (2021). Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio. *Revista Chilena de Derecho y Tecnología*, 10(2), 123-148. <https://doi.org/10.5354/0719-2584.2021.58039>
- Granja, F. M., & Rodríguez Rafael, G. D. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, 9(1), 1-18. <https://doi.org/10.1504/IJESDF.2017.081749>
- Herman, Riadi, I., & Rafiq, I. A. (2022). Forensic mobile analysis on social media using National Institute Standard of Technology method. *International Journal of Safety and Security Engineering*, 12(6), 707-713. <https://doi.org/10.18280/ijssse.120606>
- Hong, Q. N., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., Dagenais, P., et al. (2018). The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers. *Education for Information*, 34(4), 285-291. <https://doi.org/10.3233/EFI-180221>
- Horsman, G. (2023). Identifying fake vs. real communication records: A case study. *Forensic Science International: Reports*, 8, 100346. <https://doi.org/10.1016/j.fsir.2023.100346>
- Karpisek, F., Baggili, I., & Breitingner, F. (2015). WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. *Digital Investigation*, 15, 110-118. <https://doi.org/10.1016/j.diin.2015.09.002>
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103-115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44-55. <https://doi.org/10.1016/j.diin.2019.01.002>
- Maria, U., & Maria, A. V. (2022). Mapping the changing contours of electronic evidence in India. In *Handbook of Research on Cyber Law, Data Protection, and Privacy* (pp. 303-312). IGI Global. <https://doi.org/10.4018/978-1-7998-8641-9.ch018>
- McArthur, A., Cooper, A., Edwards, D., Klugarova, J., Yan, H., Barber, B. V., Gregg, E., Weeks, L. E., & Jordan, Z. (2025). Textual evidence systematic reviews series paper 3: Critical appraisal of evidence from narrative, opinion, and policy. *JB1 Evidence Synthesis*, 23(5), 833-839. <https://doi.org/10.11124/JBIES-24-00293>
- Novak, M. (2019). Digital evidence in criminal cases before the U.S. Courts of Appeal: Trends and issues for consideration. *Journal of Digital Forensics, Security and Law*, 14(4). <https://doi.org/10.15394/jdfsl.2019.1609>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>

- Rawashdeh, S. (2017). Evidence obtained from social media sites and their role in criminal proceedings: A study in the English and the American laws. *International Review of Law*, 2017(3), 14. <https://doi.org/10.5339/irl.2017.14>
- Reitingner, N., Malkin, N., Akgul, O., Mazurek, M. L., & Miers, I. (2023). Is cryptographic deniability sufficient? Non-expert perceptions of deniability in secure messaging. *2023 IEEE Symposium on Security and Privacy*, 274-292. <https://doi.org/10.1109/SP46215.2023.10179361>
- Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., et al. (2021). PRISMA-S: An extension to the PRISMA Statement for reporting literature searches in systematic reviews. *Systematic Reviews*, 10, 39. <https://doi.org/10.1186/s13643-020-01542-z>
- Rojszczak, M. (2022). e-Evidence cooperation in criminal matters from an EU perspective. *The Modern Law Review*, 85(4), 997-1028. <https://doi.org/10.1111/1468-2230.12749>
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 105801. <https://doi.org/10.1016/j.clsr.2023.105801>
- Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, 55, 106040. <https://doi.org/10.1016/j.clsr.2024.106040>
- Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, 301554. <https://doi.org/10.1016/j.fsidi.2023.301554>
- Sudiana, D., Nuruddin, C. H., Rizkinia, M., & Husna, D. (2024). Forensic analysis of WhatsApp disappearing message on unrooted Android using mobile device forensics methodology NIST SP 800-101r1. *Evergreen*, 11(1), 516-524.
- Tsai, F.-C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, 192, 2779-2788. <https://doi.org/10.1016/j.procs.2021.09.048>
- Uys, W., & Joubert, K. (2022). Forensic inquiries: Evidencing the reliability and admissibility of digital communication. *OIDA International Journal of Sustainable Development*, 15(5), 37-48.
- Wilson-Kovacs, D., Helm, R., Grown, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *The International Journal of Evidence & Proof*, 27(3), 235-253. <https://doi.org/10.1177/13657127231171620>
- Wijnberg, D., & Le-Khac, N.-A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, 38, 301132. <https://doi.org/10.1016/j.fsidi.2021.301132>

CONFLICTO DE INTERESES

La autora declara no tener conflictos de intereses.