DOI: https://doi.org/10.46296/ig.v9i17.0346

EVIDENCIA DIGITAL DE WHATSAPP EN LA JUSTICIA ECUATORIANA: REVISIÓN SISTEMÁTICA (2020-2025)

DIGITAL EVIDENCE FROM WHATSAPP IN THE ECUADORIAN JUSTICE SYSTEM: A SYSTEMATIC REVIEW (2020-2025)

Bracho-Rodriguez Alina Maria [1]; Toala-Dueñas Ramon [2]

[1] Universidad Técnica de Manabí, Maestría en Ciberseguridad. Portoviejo, Ecuador.
Correo: abracho2193@utm.edu.ec. ORCID ID: https://orcid.org/0000-0002-5176-9579.

[2] Universidad Técnica de Manabí, Maestría en Ciberseguridad. Portoviejo, Ecuador.
Correo: ramon.toala@utm.edu.ec. ORCID ID: https://orcid.org/0000-0001-5397-9054.

Resumen

La presente investigación desarrolla una revisión sistemática de literatura sobre el tratamiento legal y técnico de la evidencia digital de WhatsApp durante el período 2020–2025, conforme al protocolo PRISMA 2020. La búsqueda se practicó en Scopus, IEEE Xplore y Google Scholar, consultado este último con Publish or Perish, mientras que Rayyan, Zotero y Parsifal respaldaron el cribado y la organización documental, lo que permitió retener 47 estudios de un universo inicial de 3.068 registros. Los resultados obtenidos indican que el sistema de justicia de Ecuador no posee criterios definidos para el tratamiento de la prueba digital extraída de Whatsapp, lo cual se relaciona con el cifrado de extremo a extremo, la naturaleza efímera de ciertas comunicaciones y las dificultades asociadas a la autenticación y la integridad del material probatorio. En resumen, la conclusión manifiesta la necesidad de Ecuador de establecer un estándar técnico-jurídico propio, compatible con estándares internacionales y alineado a las exigencias forenses particulares de esta plataforma.

Palabras clave: evidencia digital, WhatsApp, forense móvil, prueba digital, cadena de custodia, cifrado E2EE, COIP, Ecuador, PRISMA 2020.

Abstract

This study develops a systematic literature review on the legal and technical treatment of WhatsApp digital evidence between 2020 and 2025, in accordance with the PRISMA 2020 protocol. The search was conducted in Scopus, IEEE Xplore, and Google Scholar (queried via Publish or Perish), while Rayyan, Zotero, and Parsifal supported the screening and documentary organization, allowing 47 studies to be retained from an initial universe of 3,068 records. The results indicate that Ecuador’s justice system lacks defined criteria for handling digital evidence extracted from WhatsApp, which is related to end-to-end encryption, the ephemeral nature of certain communications, and the challenges associated with authentication and the integrity of evidentiary material. In summary, the conclusion highlights the need for Ecuador to establish its own technical and legal standard, compatible with international standards and aligned with the specific forensic requirements of this platform.

Keywords: digital evidence, WhatsApp, mobile forensics, digital proof, chain of custody, E2EE encryption, COIP, Ecuador, PRISMA 2020.

Información del manuscrito:
Fecha de recepción: 09 de marzo de 2026.
Fecha de aceptación: 20 de mayo de 2026.
Fecha de publicación: 15 de junio de 2026.

1. Introducción

En el ámbito judicial ecuatoriano, los tribunales ya incorporan y ponderan conversaciones de WhatsApp como elementos probatorios en litigios penales, civiles y de familia. La Corte Nacional de Justicia ha examinado, en procesos recientes, intercambios extraídos por vía forense y acompañados de cadena de custodia documentada y peritajes acreditados; en esa misma línea, la doctrina nacional más actualizada reconoce la presencia creciente de esta plataforma como soporte de prueba en sede judicial. El asunto medular no es la aptitud de WhatsApp para constituir evidencia, sino las condiciones bajo las cuales su obtención, preservación, autenticación y valoración cumplen con los requisitos de licitud, integridad, contradicción y seguridad jurídica (Torres Loján, 2024; Llugsha Chicaiza et al., 2025; Morante Mendoza et al., 2025).

A lo anterior se suman particularidades técnicas propias de WhatsApp, entre ellas el cifrado extremo a extremo sustentado en el protocolo Signal, los mensajes efímeros y de visualización única, la arquitectura multidispositivo, las versiones Web, Desktop y UWP, las aplicaciones no oficiales modificadas y las bases de datos cifradas del tipo msgstore.db.crypt14. El examen de artefactos locales, metadatos, respaldos, registros de notificación, almacenamiento persistente del navegador y estructuras de bases de datos cifradas pasa a ser el eje del análisis forense, desplazando la atención que antes recaía sobre la interceptación del contenido en tránsito (Wijnberg & Le-Khac, 2021; Heath et al., 2023; Kim et al., 2025; Prabowo et al., 2025).

Los artículos 456, 471.1, 476 y 477 del COIP, aunados al artículo 202 del COGEP, constituyen el soporte normativo del régimen general de la evidencia digital en el ordenamiento ecuatoriano, en la medida en que reconocen fuerza probatoria a los documentos electrónicos y a los mensajes de datos. Sin embargo, dicha base legal no se ha materializado en procedimientos técnico-jurídicos homogéneos que regulen la identificación, recolección, preservación, sellado, traslado, peritaje y valoración judicial de

evidencia procedente de aplicaciones como WhatsApp, circunstancia que perpetúa problemas de admisibilidad, fiabilidad, trazabilidad y heterogeneidad de criterios entre los operadores judiciales (De la Torre Muñoz et al., 2024; Avemañay Lema et al., 2025; Llugsha Chicaiza et al., 2025).

El presente estudio se articula en torno a la interrogante de: ¿en qué medida los criterios técnicos y jurídicos internacionales sobre el tratamiento de la evidencia digital de WhatsApp (2020–2025) convergen o divergen respecto de la práctica forense y del marco normativo ecuatoriano, y qué vacíos de sistematización persisten para impedir la consolidación de un estándar procesal específico?

La hipótesis sugiere que, aunque Ecuador cuenta con jurisprudencia relevante y práctica pericial documentada sobre evidencia digital de WhatsApp, la ausencia de un protocolo normativo específico mantiene una brecha entre la práctica judicial heterogénea y los estándares técnicos internacionales, lo que compromete la predictibilidad de la valoración probatoria y la seguridad jurídica.

El estudio tiene por objetivo general determinar la convergencia o divergencia entre los estándares forenses y legales internacionales y la práctica normativa y judicial ecuatoriana sobre evidencia digital de WhatsApp, e identificar las brechas de sistematización que impiden consolidar un estándar procesal específico, propósito del que se derivan tres objetivos específicos consistentes en caracterizar la producción científica y normativa 2020–2025, clasificando los estudios incluidos según su contribución a las fases de obtención, preservación y valoración de la evidencia digital de WhatsApp, sistematizar los desafíos técnicos (E2EE, volatilidad, integridad, mensajes efímeros) y jurídicos (cadena de custodia, privacidad, licitud, admisibilidad) asociados al uso de WhatsApp como prueba, y contrastar los marcos técnicos y jurídicos internacionales con la práctica forense y normativa ecuatoriana, identificando las brechas de sistematización y los vacíos que impiden la consolidación de un estándar específico para la

evidencia digital de WhatsApp en Ecuador.

2. Metodología

La investigación adopta el protocolo PRISMA 2020, registrado en OSF. Con miras a garantizar una cobertura equilibrada, la indagación bibliográfica se estructuró en cinco cadenas repartidas entre Scopus (B1), IEEE Xplore (B2) y Google Scholar mediante Publish or Perish, segmentadas en tres dimensiones: técnica en inglés (B3e-Tec), jurídica bilingüe (B3e-Jur) y doctrinal ecuatoriana en español (B3e-Ec). La segmentación por dimensiones neutralizó el sesgo del algoritmo de Google Scholar hacia la literatura anglófona y facilitó la recuperación de producción técnico-forense reciente sobre Android, WhatsApp en sus versiones Web, Desktop y UWP, mensajes efímeros y bases de datos cifradas. Una búsqueda manual complementaria, basada en referencias cruzadas y fuentes especializadas, aportó once documentos adicionales.

Tabla 1. *Cadenas de búsqueda y registros identificados*

Cadena	Base	Términos exactos	n
B1	Scopus	TITLE-ABS-KEY("WhatsApp" AND "digital forensics") AND PUBYEAR > 2019 AND PUBYEAR < 2026	63
B2	IEEE Xplore	("WhatsApp" OR "instant messaging") AND ("digital forensics" OR "mobile forensics" OR "forensic analysis" OR …) AND ("digital evidence" OR "admissibility" OR "chain of custody" OR …)	13
B3e-Tec	GS vía PoP — técnico	WhatsApp ("forensic analysis" OR "digital forensics" OR "forense" OR "mobile forensics" OR "digital evidence" OR …)	995
B3e-Jur	GS vía PoP — jurídico	("WhatsApp" OR "mensajería instantánea" OR "prueba digital" OR …) ("admissibility" OR "cadena de custodia" OR "valoración probatoria" OR …)	999
B3e-Ec	GS vía PoP — Ecuador	("WhatsApp" OR "evidencia digital" OR "peritaje informático" OR "informática forense" OR …) ("Ecuador" OR "COIP" OR "COGEP")	987
Manual	Búsqueda manual	Referencias cruzadas y consulta directa de fuentes especializadas	11
TOTAL	**—**	**Registros identificados**	**3.068**

Fuente: elaboración propia.

Tabla 2. *Criterios de elegibilidad aplicados*

Código	Tipo / Fase	Descripción
CI1	Inclusión	Artículos científicos, jurisprudencia, normativa y manuales forenses oficiales
CI2	Inclusión	Publicaciones emitidas entre enero de 2020 y diciembre de 2025
CI3	Inclusión	Investigaciones sobre WhatsApp o mensajería segura con foco forense o jurídico
CI4	Inclusión	Documentos publicados en español o inglés
CE1	Exclusión P2	Literatura gris, tesis no indexadas, blogs, foros, notas de prensa
CE2	Exclusión P1	Estudios sobre redes sociales sin foco en mensajería instantánea o WhatsApp
CE3	Exclusión P1	Investigaciones ajenas al derecho o la ciberseguridad
CE4	Exclusión P2	Texto completo inaccesible mediante base de datos original o vías de acceso abierto
CE5	Exclusión P1/P2	Sin pertinencia con OE1, OE2 u OE3; hallazgos no transferibles al marco forense-normativo ecuatoriano
CE6	Exclusión P1	Documentos cuyo texto completo está en idioma distinto al español o al inglés

Fuente: elaboración propia.

El proceso de cribado se desarrolló en dos pasadas: P1 (Rayyan, título y resumen, con aplicación de CI1-CI4, CE2, CE3, CE5 y CE6) y P2 (Parsifal, texto completo, con aplicación de CE1, CE4 y CE5). La extracción de datos se realizó mediante una matriz estructurada de 28 campos, que incluyó autoría, año, país, fuente, tipo de estudio, objetivo específico asociado, herramienta forense, marco metodológico, artefactos recuperados, limitaciones técnicas, aportes jurídicos, aplicabilidad a Ecuador y nivel de calidad; la evaluación de calidad empleó una checklist de 8 preguntas con umbral mínimo de 4/8 puntos.

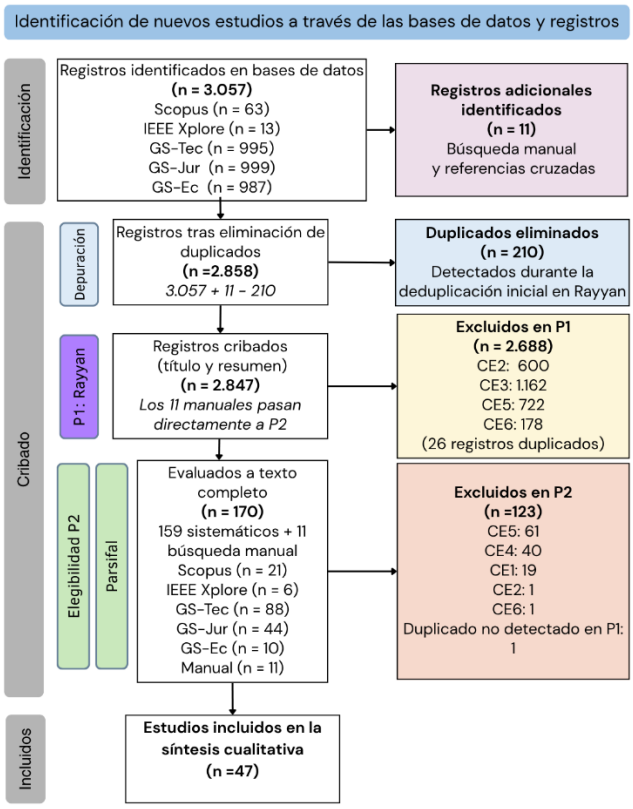
3. Resultados y discusión

Los resultados se presentan en secuencia con los objetivos específicos: la caracterización del corpus y la clasificación por fases responden al OE1; la sistematización de desafíos técnicos y jurídicos, al OE2; y el contraste entre estándares internacionales y práctica ecuatoriana, al OE3. La discusión integradora cierra el apartado articulando los tres planos.

Flujo PRISMA y caracterización del corpus

De los 3.068 registros identificados, tras eliminar 210 duplicados quedaron 2.858 registros para el cribado P1, cifra que incluye 11 documentos procedentes de la búsqueda manual. Rayyan eliminó un total de 2.688 registros, de los cuales 600 correspondían al criterio CE2 por no centrarse en mensajería de WhatsApp, 1.162 al criterio CE3 por pertenecer a disciplinas ajenas al derecho o la ciberseguridad, 722 al CE5 por no ser transferibles al contexto de Ecuador y 178 al CE6 por no cumplir con el requisito idiomático, además de 26 registros excluidos por doble criterio. Posteriormente, los 170 estudios restantes fueron sometidos a revisión en texto completo mediante Parsifal, proceso en el que se descartaron 123 trabajos adicionales: 61 por CE5, 40 por CE4, 19 por CE1, uno por CE2, uno por CE6 y uno por duplicación no detectada en la fase P1. En consecuencia, la muestra final quedó conformada por 47 estudios, tal como se recoge en la Figura 1.

Figura 1. *Diagrama PRISMA 2020 del proceso de selección*

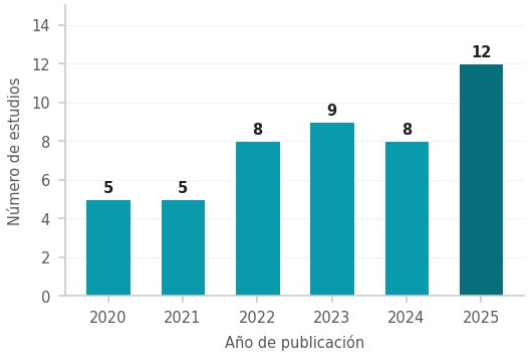


Fuente: elaboración propia, adaptado de Page et al. (2021).

El corpus final de 47 estudios se distribuye como sigue: 21 desde Google Scholar técnico (44,7 %), 11 desde Scopus (23,4 %), 11 desde Google Scholar jurídico (23,4 %), 3 desde búsqueda manual (6,4 %) y 1 desde Google Scholar Ecuador (2,1 %). Dado que los registros recuperados de IEEE Xplore respondían principalmente a enfoques de ingeniería técnica sin correspondencia temática con la gestión probatoria de WhatsApp en el marco normativo ecuatoriano, ninguno fue incorporado al corpus final. En cuanto a la distribución cronológica de la literatura seleccionada, esta se presenta en la Figura 2, en tanto que su clasificación por finalidad específica se recoge en la Figura 3.

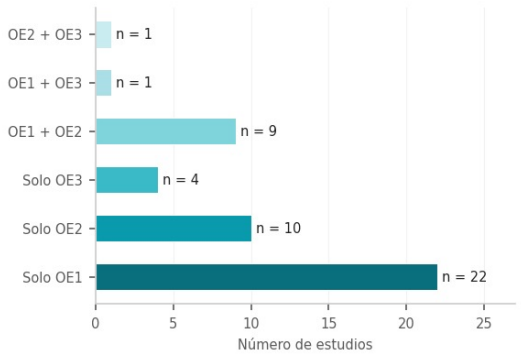
Los trabajos incluidos para el primer objetivo específico fueron agrupados conforme a la fase del proceso probatorio y a la naturaleza de su aportación científica. En la literatura técnico-forense se centra en la extracción de artefactos digitales, recuperación de mensajes efímeros y el análisis de repositorios SQLite en plataformas web y de escritorio, en cambio, los estudios jurídicos privilegian la preservación de la evidencia documental y la admisibilidad de la prueba. A su vez, el examen de la producción científica y normativa correspondiente al periodo 2020–2025 revela un avance desigual, dado que los progresos técnicos en materia forense han evolucionado con mayor rapidez que el desarrollo doctrinal y regulatorio, configurando un panorama en el que la validación pericial coexiste con una discusión jurídica todavía pendiente respecto a la autenticidad y el valor probatorio de los registros digitales.

Figura 2. *Distribución del corpus por año de publicación*



Fuente: elaboración propia.

Figura 3. *Distribución del corpus por objetivo específico*

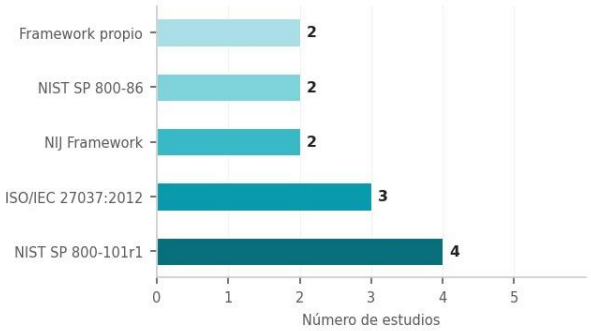


Fuente: elaboración propia.

Hallazgos OE1: dimensión técnico-forense

La síntesis del OE1 identifica un conjunto de herramientas y enfoques con respaldo empírico en la literatura. En el plano comercial destacan Cellebrite UFED, MSAB XRY, Oxygen Forensic Detective, Magnet AXIOM, MOBILedit y Belkasoft, empleados para adquirir o analizar artefactos como mensajes, contactos, archivos multimedia, llamadas, bases de datos y registros del sistema (Heath et al., 2023; Nahdli et al., 2024; Sharma et al., 2025; Zamroni & Riadi, 2020). En el conjunto de herramientas abiertas o de apoyo, WhatsApp Key/DB Extractor, WhatsApp Viewer, DB Browser for SQLite, Autopsy, FTK Imager y utilidades como Binwalk aparecen ligadas a tareas de descifrado o examen de repositorios locales, con predominancia en entornos Android no rooteado (Fayyad-Kazan et al., 2022; Rotaru & Tatu, 2021; Prabowo et al., 2025; Sulisdyantoro & Marzuki, 2023). En materia de marcos metodológicos, NIST SP 800-101r1, NIST SP 800-86, NIJ e ISO/IEC 27037:2012 son los referentes de uso más extendido (Figura 4).

Figura 4. *Marcos metodológicos forenses más utilizados*



Fuente: elaboración propia.

Respecto del cifrado E2EE, los estudios coinciden en que impide la lectura directa de mensajes en tránsito y limita la cooperación del proveedor al suministro de información de cuenta o metadatos, no del historial completo de mensajes (Abd Elmonsef Sarhan et al., 2023; Wijnberg & Le-Khac, 2021; Onik et al., 2025). En la vertiente técnica, los estudios se concentran en la extracción de llaves de cifrado y el análisis de almacenamiento persistente en sistemas Windows, ámbito que abarca también las notificaciones y las bases de datos SQLite cifradas. El análisis de los ficheros msgstore.db.crypt14 demanda métodos de adquisición directa o técnicas de descifrado vinculadas a la clave del dispositivo, lo que los convierte en un objeto de estudio particularmente exigente dentro de la disciplina forense. Diversos estudios especializados recogen métodos orientados a la recuperación de este tipo de evidencia, entre los cuales destacan el APK Downgrade y el empleo de utilidades de extracción de bases de datos en variados escenarios forenses, con el propósito de garantizar la integridad y recuperabilidad de la información (Rotaru & Tatu, 2021; Fayyad-Kazan et al., 2022; Sulisdyantoro & Marzuki, 2023; Prabowo et al., 2025).

En relación con los mensajes efímeros, se ha constatado experimentalmente que la recuperación de datos es viable incluso en dispositivos Android sin permisos de superusuario: Sudiana et al. (2024) restauraron el 83,33 % de las comunicaciones desaparecidas empleando registros de notificación y ficheros de respaldo, mientras que Heath et al. (2023) demostraron que la eficacia en la obtención de evidencia está condicionada tanto por la herramienta forense seleccionada como por la plataforma objeto de estudio. Los trabajos incluidos en el primer objetivo específico giran en torno a la obtención, preservación y valoración de evidencia digital de WhatsApp, cuya agrupación obedece a las particularidades técnicas de cada actuación pericial, comprendiendo desde el acceso a artefactos locales, claves criptográficas y respaldos en plataformas web y de escritorio, hasta el resguardo de la integridad por medio de funciones hash,

registro técnico y cadena de custodia. Finalmente, la fase de valoración se orienta a garantizar que los resultados obtenidos puedan ser sometidos a un control de veracidad y a un ejercicio efectivo de contradicción dentro del proceso judicial.

Hallazgos OE2: dimensión jurídica

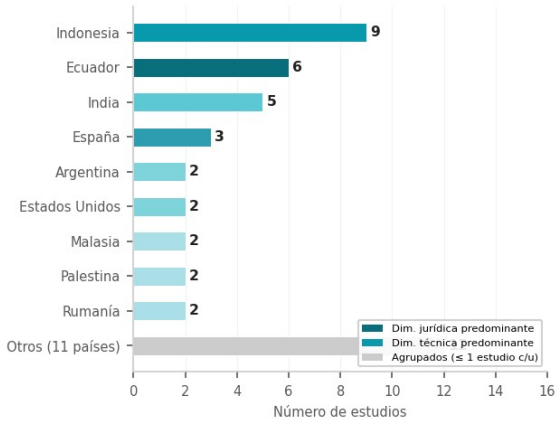
La literatura comparada coincide en reconocer las conversaciones de WhatsApp como documentos electrónicos con potencial valor probatorio, aunque muestra diferencias notables en cuanto al estándar de rigor exigido para su incorporación al proceso. En jurisdicciones como España, Colombia, Argentina, México, Perú e Indonesia, la exigencia de contradicción procesal, dictamen pericial informático, preservación de metadatos, cadena de custodia y mecanismos de verificación técnica como el hash o la extracción forense aparece de forma recurrente (Martínez Guerrero, 2022; Gómez Agudelo et al., 2021; Robledo & Robledo, 2022/2023; Ávila Silva et al., 2023; Lovera & Farias, 2024; Deviriana et al., 2025; Sánchez Pérez, 2025). En Ecuador, Torres Loján (2024) coincide en que las capturas por sí solas pueden resultar insuficientes para acreditar autoría, pertenencia del número telefónico o integridad del contenido.

De la literatura revisada se desprende una conclusión clara: la captura de pantalla simple no puede equipararse a una extracción forense de WhatsApp, su valor debe considerarse indiciario o complementario cuando se discuten autenticidad, integridad, autoría o contexto, pues los datos digitales pueden ser modificados, editados o recreados y requieren mecanismos científicos de preservación, fiabilidad y cadena de custodia (Sánchez Pérez, 2025). La incorporación al proceso judicial de evidencia electrónica de WhatsApp exige garantizar los principios de integridad, autenticidad, veracidad y legalidad, por lo que, ante contenidos controvertidos, el peritaje informático aporta mayor solidez probatoria que una captura de pantalla (Lovera & Farias, 2024). En presencia de evidencia volátil, como sesiones activas de WhatsApp Web, mensajes no persistentes o información almacenada en memoria, dicha exigencia adquiere particular relevancia, razón por la

cual la literatura técnica recomienda aplicar técnicas de live forensics y procedimientos de adquisición verificable en lugar de impresiones o grabaciones de pantalla (Soares, 2022).

El segundo objetivo específico estructura los obstáculos detectados en dos dimensiones, una técnica que engloba el cifrado de extremo a extremo, los mensajes efímeros, las arquitecturas multidispositivo, la volatilidad e integridad de los datos y la dependencia operativa del terminal, y otra jurídica concerniente a la licitud probatoria, la privacidad, la cadena de custodia, la autenticación, el principio de contradicción y la admisibilidad de la prueba. La convergencia entre uno y otro conjunto pone al descubierto que la eficacia probatoria de los mensajes de WhatsApp no descansa en la sola recuperación de datos: demanda que estos sean obtenidos, conservados y fundamentados en plena consonancia con las garantías procesales vigentes. En la vertiente jurídica del corpus sobresalen Ecuador, España, Colombia, México y Perú, mientras que Indonesia e India lideran la producción técnica, lo que refleja una marcada polarización geográfica entre ambas dimensiones (Figura 5).

Figura 5. *Distribución geográfica del corpus*



Fuente: elaboración propia.

Hallazgos OE3: Ecuador y derecho comparado

El corpus incluyó ocho estudios directamente vinculados a Ecuador, el COIP, el COGEP o la práctica judicial ecuatoriana, cuyos hallazgos apuntan a cinco vacíos centrales: (1) inexistencia de protocolos técnicos específicos para la obtención,

preservación y tratamiento de evidencia digital; (2) debilidades en la cadena de custodia digital, el sellado, el registro y la trazabilidad; (3) déficit de infraestructura forense y de peritos certificados; (4) ausencia de mecanismos operativos de cooperación internacional que materialicen el acceso ágil a evidencia alojada fuera del país; y (5) heterogeneidad de criterios judiciales en materia de autenticidad, integridad y valoración probatoria. Llugsha Chicaiza et al. (2025) estiman que cerca del 60 % de las investigaciones penales con evidencia digital presentarían problemas de admisibilidad por deficiencias en la cadena de custodia y la autenticación técnica, dato que los autores vinculan con la elevada impunidad reportada en el país, lo que lo sitúa como un indicador del impacto de la fragmentación más que como una medición censal de expedientes; por su parte, De la Torre Muñoz et al. (2024), Avemañay Lema et al. (2025), Morante Mendoza et al. (2025) y Torres Loján (2024) concuerdan en la necesidad de protocolos nacionales armonizados con los estándares ISO/IEC 27037, 27041, 27042 y 27043.

La fragmentación normativa detectada no debe leerse únicamente como una contradicción entre resoluciones judiciales o cortes provinciales, sino como una desarticulación entre el marco legal general, la práctica pericial y los criterios de valoración judicial. Aunque el COIP reconoce formalmente la prueba digital y regula la cadena de custodia, la literatura ecuatoriana advierte que su puesta en práctica sigue afrontando vacíos legales, restricciones operativas y carencia de mecanismos específicos para el tratamiento de evidencias electrónicas, circunstancias que pueden comprometer la trazabilidad y la credibilidad de los elementos probatorios (Morante Mendoza et al., 2025). El COGEP y la Ley de Comercio Electrónico confieren aptitud probatoria a los documentos electrónicos y mensajes de datos; sin embargo, ninguno de esos cuerpos normativos contempla una regulación propia para la prueba documental obtenida por medio de WhatsApp (Torres Loján, 2024).

Con el propósito de salvar la brecha técnica entre laboratorios forenses y peritos informáticos, De la Torre

Muñoz et al. (2024) proponen un marco metodológico sustentado en las normas ISO 27037, ISO 27042 y las guías RFC, que normaliza procedimientos críticos como la observación, el registro, la individualización, el sellado y el traslado de la evidencia digital. Ese diagnóstico coincide con el de Avemañay Lema et al. (2025), quienes señalan que la inexistencia de protocolos técnicos, las debilidades en la cadena de custodia, la infraestructura forense deficiente y la falta de uniformidad en los criterios de autenticidad e integridad determinan la brecha que en el ámbito iberoamericano separa el reconocimiento normativo de su aplicación práctica, confirmando la misma carencia identificada en el contexto ecuatoriano. Lo que Ecuador necesita no es más prueba digital, sino una sistematización de carácter normativo, técnico e institucional específicamente orientada al tratamiento de la evidencia de WhatsApp.

Tabla 3. *Niveles de fragmentación en la evidencia digital de WhatsApp en Ecuador*

Nivel de fragmentación	Dónde radica	Consecuencia para la evidencia de WhatsApp	Respaldo
Normativa	El COIP, el COGEP y la Ley de Comercio Electrónico validan los mensajes de datos con carácter general, pero omiten directrices precisas para gestionar y valorar WhatsApp.	Inexistencia de pautas rigurosas para validar autenticidad, integridad y admisibilidad de comunicaciones de WhatsApp.	Morante Mendoza et al. (2025); Torres Loján (2024).
Técnica-institucional	Falta de estándares obligatorios unificados entre peritos para extracción de bases cifradas, metadatos, hashes y duplicados forenses.	Disparidad en los procesos de obtención, preservación, documentación técnica y cadena de custodia.	De la Torre Muñoz et al. (2024); Avemañay Lema et al. (2025).
Esfera jurisdiccional	La apreciación de capturas de pantalla, registros exportados e informes periciales recae en el juicio particular de cada operador judicial, sin parámetros homogéneos que orienten dicha valoración.	La inexistencia de pautas comunes compromete la licitud, la autoría, la trazabilidad de la evidencia y su integridad en el plano probatorio.	Torres Loján (2024); Avemañay Lema et al. (2025).
Desarrollo doctrinal	Ecuador cuenta con literatura académica propia sobre el tema, pero esta permanece fragmentada y con débil conexión respecto a los estándares técnicos de referencia internacional.	Falta de una doctrina consolidada acerca de WhatsApp como fuente de evidencia digital cifrada.	De la Torre Muñoz et al. (2024); Morante Mendoza et al. (2025).

Fuente: elaboración propia.

La fragmentación constituye el eje central del presente artículo, ya que no se limita a la existencia de un vacío legal ni a discrepancias jurisprudenciales aisladas, sino que refleja una brecha estructural entre el reconocimiento normativo general, la práctica forense, las capacidades institucionales disponibles y la uniformidad en los criterios de valoración judicial. A partir de esta premisa, el tercer objetivo específico se desarrolla mediante la comparación entre los marcos internacionales incorporados en el corpus, particularmente las guías NIST y NIJ junto con las normas ISO 27037, 27041, 27042 y 27043, las buenas prácticas comparadas y la realidad del sistema jurídico ecuatoriano. Del análisis comparado se advierte que Ecuador cuenta con un reconocimiento normativo general respecto de la prueba digital; sin embargo, todavía no dispone de un estándar específico aplicable a la evidencia proveniente de WhatsApp que articule de forma sistemática aspectos vinculados con el cifrado, la extracción forense, la preservación de la evidencia, la cadena de custodia, la pericia informática y la valoración judicial.

Tabla 4. *Caracterización de los estudios incluidos en el corpus*

Autor (año)	OE	Herramienta principal	Hallazgo principal
Abd Elmonsef Sarhan et al. (2023)	1+2	Análisis tráfico cifrado	Perfiles de uso, metadatos y límites del E2EE en la recuperación de evidencia
Adijisman & Riadi (2021)	OE1	MOBILedit, WA Viewer, DB Browser	Condiciones técnicas del dispositivo determinan la factibilidad de extracción
Aniza & Riadi (2021)	OE1	MOBILedit Express, FTK Imager	Marco NIST en caso de estafa: mensajes, multimedia e identidad recuperados
Avemañay Lema et al. (2025)	OE3	N/A — análisis jurídico-comparado	Vacíos en capacidad técnica, guías de actuación y valoración probatoria en Ecuador
Ávila Silva et al. (2023)	OE2	N/A — análisis jurídico	Validez de WhatsApp como prueba en el sistema penal acusatorio mexicano
Banegas-Crespo & Andrade-Pesantez (2024)	1+3	Herramientas móviles; ISO/IEC 27037	Guía técnica ISO 27037 para delitos de ciberextorsión en Ecuador (Android)
Bogos et al. (2023)	OE2	N/A — análisis comparativo	Comparación de cifrado en Signal, WhatsApp y Telegram; contexto E2EE
Cahyanto et al. (2022)	OE1	FTK Imager, HashMyFiles, live forensics	Live forensics en WhatsApp Desktop: evidencia efímera en RAM y sesiones activas
De la Torre Muñoz et al. (2024)	OE3	N/A — estándares ISO/RFC	Guía metodológica ISO/RFC para primeros respondedores y peritos en Ecuador
Deo et al. (2023)	OE1	WA Key/DB Extractor, Avilla Forensics	Framework open-source para artefactos y bases de datos cifradas de WhatsApp
Deviriana et al. (2025)	OE2	N/A — análisis jurídico	Problemas de autenticación, alteración y ausencia normativa en Indonesia

Autor (año)	OE	Herramienta principal	Hallazgo principal
Egho-Promise et al. (2020)	OE1	Herramientas extracción Android	Referente pionero: extracción de datos WhatsApp desde almacenamiento interno
Fathiyana et al. (2022)	OE1	WA Viewer, herramientas Android	Artefactos WhatsApp vs. Telegram en Android sin root; reconstrucción de contactos
Fayyad-Kazan et al. (2022)	OE1	Python, SQLite DB, extractor de llave	Bases SQLite cifradas en Android sin root: mensajes, grupos y llamadas
Gómez Agudelo et al. (2021)	OE2	N/A — análisis jurídico	Hash, autenticidad y garantías procesales; riesgo de falsificación de capturas
Heath et al. (2023)	1+2	Cellebrite, MSAB XRY, Magnet AXIOM	Mensajes efímeros en WhatsApp, Snapchat y Telegram: retos antiforenses
Idris & Ab Rahman (2022)	OE1	MOBILedit, FTK Imager, Autopsy	Caché, logs y multimedia en WhatsApp móvil vs. web; líneas temporales de usuario
Kaushik & Katara (2022)	OE1	Adquisición lógica/física	Clasificación de herramientas y procedimientos para análisis de conversaciones
Kim et al. (2025)	OE1	Análisis Web/UWP, descifrado local	Recuperación y descifrado de WhatsApp en Windows Web y UWP
Llugsha Chicaiza et al. (2025)	OE3	N/A — análisis normativo y jurisprudencial	Barreras de admisibilidad y carencias del sistema ecuatoriano de evidencia digital
Lovera & Farias (2024)	OE2	N/A — análisis jurídico-procesal	Admisibilidad, impugnación y pericia de WhatsApp y Telegram en proceso civil
Manzoor et al. (2025)	1+2	Extracción datos móviles	Obstáculos técnicos, jurídicos y procedimentales en extracción de datos WhatsApp
Martínez Guerrero (2022)	OE2	N/A — análisis procesal penal	Cuestiona cotejos informales de WhatsApp; exige garantías del debido proceso
Martínez Guerrero (2025)	OE2	N/A — análisis procesal penal	Admisibilidad de WhatsApp como prueba; límites del cotejo sin respaldo técnico
Morante Mendoza et al. (2025)	OE3	N/A — análisis COIP/ISO/IEC	Cadena de custodia, COIP y estándares ISO/IEC en Ecuador
Nahdli et al. (2024)	OE1	MOBILedit, Belkasoft, Magnet AXIOM	Contraste de herramientas forenses para artefactos WhatsApp (framework NIJ)
Onik et al. (2025)	1+2	N/A — revisión sistemática	Artefactos, herramientas, cifrado y brechas en aplicaciones de mensajería (SLR)
Paligu & Varol (2020)	OE1	FTK Imager, Browser History Examiner	Rastros de WhatsApp Web en IndexedDB: cronología y actividad del usuario
Pandey et al. (2025)	OE1	Análisis Windows/UWP	Protocolo de recuperación de multimedia eliminada en WhatsApp Windows/UWP
Pirzada et al. (2023)	1+2	N/A — revisión herramientas/visualización	Forense y visualización de mensajería: sistematización y claridad expositiva
Prabowo et al. (2025)	OE1	WA Key DB Extractor, Binwalk, DB Browser	Claves, metadatos y análisis de msgstore.db.crypt14 con y sin root
Robledo & Robledo (2022/2023)	OE2	N/A — análisis procesal y constitucional	WhatsApp como correspondencia protegida y medio probatorio atípico
Rotaru & Tatu (2021)	OE1	WA Key DB Extractor, WA Viewer	Extractor de claves, degradación APK y archivos wa.db/msgstore.db; limitaciones
Sánchez Gálvez (2020)	OE2	N/A — análisis jurídico	Valor probatorio de WhatsApp en distintas ramas del derecho guatemalteco
Sánchez Pérez (2025)	OE2	N/A — análisis procesal penal	Derecho a confrontar capturas de WhatsApp; admisibilidad procesal comparada
Shadeed et al. (2022)	OE1	WA Key/DB Extractor, SQLite Browser	Extracción de artefactos WhatsApp en Android sin root: msgstore.db y wa.db
Sharma et al. (2025)	OE1	MSAB XRY, Oxygen Forensic Detective	Evaluación comparativa MSAB XRY vs. Oxygen en 30 dispositivos Android

Autor (año)	OE	Herramienta principal	Hallazgo principal
Shidek et al. (2020)	OE1	Python, visualizador web, Timeline	Visualizador cronológico: participantes, secuencia e intervenciones de chat
Soares (2022)	1+2	ZAPiXWEB, live forensics	Adquisición en vivo de WhatsApp Web; pantallazo insuficiente para preservación
Soni (2024)	1+2	N/A — revisión técnica /herramientas	Fuentes de evidencia, cifrado, volatilidad y necesidad de cooperación internacional
Sudiana et al. (2024)	1+2	MOBILedit, Autopsy, backup Android	83,33% de mensajes efímeros recuperados en Android sin root (NIST SP 800-101r1)
Sulisdyantoro & Marzuki (2023)	OE1	Cellebrite, MOBILedit, APK Downgrade	APK Downgrade para descifrar crypt14 e incrementar artefactos recuperados
Torres Loján (2024)	2+3	N/A — análisis jurídico ecuatoriano	WhatsApp en litigios financieros: autenticidad, integridad y protocolos en Ecuador
Utomo et al. (2023)	OE1	Autopsy, FTK Imager, NIST	Análisis de WhatsApp Browser con NIST y Autopsy: conversaciones y multimedia
Wijnberg & Le-Khac (2021)	1+2	OSINT, WA Web analysis, descifrado	E2EE limita interceptación; alternativas: fuentes web, OSINT y metadatos
Zakarneh (2024)	OE1	Mobile forensics iOS/Android	Caso real iOS/Android: extracción de conversaciones, llamadas y recomposición temporal
Zamroni & Riadi (2020)	OE1	WA Key/DB Extractor, Oxygen, Magnet AXIOM	Validación de WA Key/DB Extractor, Oxygen y Magnet AXIOM en adquisición de artefactos

Fuente: elaboración propia. Nota: En los estudios de carácter jurídico, doctrinal o normativo, la columna Herramienta indica "N/A", dado que su contribución no deriva de experimentación forense sino del análisis legal o jurisprudencial.

Discusión integradora

El corpus permite articular tres ejes analíticos. En el plano internacional, existe un patrón extendido de cautela frente al uso de capturas de pantalla aisladas como prueba plena, pues su fuerza probatoria depende de la posibilidad de verificar autenticidad, autoría, integridad, contexto y cadena de custodia (Gómez Agudelo et al., 2021; Martínez Guerrero, 2022; Sánchez Pérez, 2025). En el plano técnico, la literatura documenta avances relevantes en recuperación de artefactos locales, bases cifradas, registros de notificación, almacenamiento web, live forensics y entornos Windows y UWP; con todo, estos avances no equivalen a una ruptura general del cifrado E2EE, sino a estrategias de adquisición sobre datos remanentes o accesibles en dispositivos y sesiones autorizadas (Soares, 2022; Kim et al., 2025; Prabowo et al., 2025). En el plano ecuatoriano, el contexto evidencia una brecha estructural entre el reconocimiento general de la prueba digital y la ausencia de procedimientos específicos para el tratamiento probatorio de evidencia proveniente de WhatsApp.

Aunque buena parte de la producción técnico-forense sobre WhatsApp proviene de investigaciones desarrolladas fuera de Ecuador, sus resultados pueden ser aprovechados en el ámbito nacional siempre que se integren en un informe pericial ajustado al COIP, al COGEP y a la Ley de Comercio Electrónico, ya que la literatura especializada describe herramientas como WhatsApp-Key-Database Extractor, Binwalk, Mobile Edit, WhatsApp Viewer y DB Browser for SQLite para examinar bases cifradas como msgstore.db.crypt14, metadatos y claves de cifrado (Prabowo et al., 2025). No obstante, dicha incorporación competente exige una interpretación cuidadosa, puesto que diversos estudios desarrollados en Ecuador evidencian la persistencia de vacíos técnicos, la ausencia de protocolos nacionales estandarizados y deficiencias tanto en la cadena de custodia como en la práctica pericial forense (Morante Mendoza et al., 2025). Por ello, la procedencia internacional de la herramienta adquiere una relevancia secundaria frente a la reproducibilidad metodológica y al respeto del derecho de contradicción procesal, de manera que la valoración jurídica debe sustentarse en la licitud de la obtención, la integridad de los registros digitales, la preservación de los metadatos y el respeto de la cadena de custodia.

La desconexión existente entre la praxis judicial y el marco normativo vigente, agravada por la ausencia de protocolos técnicos obligatorios que articulen ambos planos, describe con mayor precisión la realidad del contexto ecuatoriano que la idea de un vacío legal absoluto, lo cual se corresponde con la hipótesis previamente validada. Aunque tanto la jurisprudencia como la práctica pericial evidencian que los mensajes de WhatsApp ya son admitidos como medio probatorio, la literatura nacional señala que dicha incorporación se realiza bajo estándares heterogéneos, condicionada por limitaciones de infraestructura, deficiencias en la capacitación y criterios de valoración que carecen de coherencia y articulación entre sí. La desconexión identificada se manifiesta en tres dimensiones diferenciadas, en el ámbito técnico se observa una falta de correspondencia entre herramientas, métodos de

extracción y mecanismos de preservación de la evidencia, en el plano jurídico se evidencia la ausencia de un procedimiento normativo específico aplicable a la mensajería cifrada, y en el nivel conceptual se aprecia la dispersión existente en la literatura ecuatoriana junto con su limitada articulación con los estándares internacionales (De la Torre Muñoz et al., 2024; Avemañay Lema et al., 2025; Llugsha Chicaiza et al., 2025).

En este sentido, el alcance del presente trabajo se encuentra delimitado por tres condicionantes principales. En primer lugar, la cobertura relativa a iOS, la plataforma universal de Windows y las arquitecturas multidispositivo más recientes resulta insuficiente, debido al predominio de estudios técnicos centrados en el entorno Android. En segundo lugar, la literatura jurídica ecuatoriana se caracteriza por aproximaciones de tipo descriptivo o doctrinal, las cuales presentan una limitada verificación empírica a nivel local en relación con protocolos forenses. En tercer lugar, se observa la rápida obsolescencia de herramientas y metodologías como consecuencia de las actualizaciones de WhatsApp, con especial incidencia en aspectos como el cifrado, el almacenamiento local, los mensajes efímeros, la sincronización multidispositivo y los servicios en versiones Web y Desktop (Heath et al., 2023; Kim et al., 2025; Pandey et al., 2025; Prabowo et al., 2025).

4. Conclusiones

La revisión sistemática responde a la pregunta de investigación al confirmar una divergencia significativa entre los estándares técnico-jurídicos internacionales y la práctica ecuatoriana. En lo concerniente al OE1, la literatura evidencia una convergencia técnica en torno al uso de marcos como NIST, NIJ e ISO/IEC 27037, así como de herramientas comerciales y abiertas orientadas a la recuperación de artefactos locales, bases cifradas, respaldos, registros de notificación y datos derivados de WhatsApp en sus entornos Web y Desktop. En el marco del OE2, la literatura revisada coincide de manera unánime en que la autenticidad y el contexto constituyen elementos indivisibles de la cadena de custodia a la hora de determinar la admisibilidad

probatoria, de modo que una captura de pantalla básica debe ser analizada con criterios estrictos de cautela y, en caso de cuestionarse su integridad, únicamente podrá tener eficacia jurídica si cuenta con el respaldo técnico de un perito especializado. El examen comparado correspondiente al tercer objetivo específico deja en evidencia que la heterogeneidad valorativa y la falta de pautas técnicas concretas constituyen impedimentos relevantes, sumándose a ello la escasa cualificación del personal, el rezago en infraestructura pericial y la falta de operativización de los mecanismos de cooperación internacional como elementos que afianzan el desajuste estructural propio del entorno ecuatoriano.

La seguridad jurídica en el tratamiento de la evidencia digital se vería reforzada con la consolidación, por parte de Ecuador, de una guía nacional vinculante que articule componentes técnicos y normativos conforme a referentes internacionales, asegure la cadena de custodia desde el origen y dote de coherencia a las fases de obtención, conservación y valoración del material probatorio, premisa que se impone toda vez que el cifrado y la transformación de la plataforma plantean condicionantes técnicos cuya respuesta institucional coordinada debe subsanar las carencias periciales vigentes, dado que los avances en la extracción de datos de WhatsApp no han tenido correlato proporcional en la fijación de pautas de licitud aplicables.

A partir del corpus analizado se identifican cinco líneas prioritarias para el contexto ecuatoriano. En primer lugar, se plantea la adopción de protocolos estandarizados basados en las normas ISO/IEC 27037, 27041, 27042 y 27043, incorporando criterios específicos relativos a metadatos, funciones hash, copias forenses, respaldos, registros de notificación, entornos Web y Desktop, así como bases de datos cifradas (De la Torre Muñoz et al., 2024; Morante Mendoza et al., 2025; Avemañay Lema et al., 2025). La formación técnica de peritos y operadores judiciales se erige en una segunda exigencia inexcusable (Llugsha Chicaiza et al., 2025; Torres Loján, 2024), a la cual se añade la habilitación de laboratorios forenses certificados con personal acreditado, articulados mediante un

Instituto Nacional de Pericia Digital u organismo técnico análogo (Morante Mendoza et al., 2025; Avemañay Lema et al., 2025), debiendo además todo análisis pericial sobre WhatsApp ceñirse a protocolos verificables que incorporen funciones hash, cadena de custodia documentada y resguardo de metadatos (Gómez Agudelo et al., 2021; Sánchez Pérez, 2025; Lovera & Farias, 2024; Torres Loján, 2024). Finalmente, se recomienda implementar un sistema de cadena de custodia digital trazable de extremo a extremo, con sellado de tiempo, registro de hash y bitácora de accesos verificable, que garantice la integridad y autenticidad de la evidencia de WhatsApp desde su obtención hasta su valoración judicial y fortalezca los mecanismos de cooperación internacional en investigaciones que involucren infraestructura o datos ubicados fuera del país, como cuentas, servidores o servicios en la nube (De la Torre Muñoz et al., 2024; Morante Mendoza et al., 2025; Avemañay Lema et al., 2025). A este esfuerzo se suma la conveniencia de aprovechar plenamente el marco de cooperación internacional del que Ecuador ya forma parte como Estado adherido al Convenio de Budapest sobre Ciberdelincuencia, traduciendo sus disposiciones en mecanismos operativos internos, puntos de contacto permanentes, procedimientos de preservación expedita y solicitud de datos a proveedores extranjeros, que permitan su aplicación efectiva en la investigación penal.

La investigación futura debe orientarse al diseño de herramientas de visualización y análisis automatizado de conversaciones (Shidek et al., 2020; Pirzada et al., 2023), a la profundización en live forensics sobre WhatsApp Web y Desktop (Soares, 2022; Cahyanto et al., 2022; Kim et al., 2025) y a la comprobación empírica de los protocolos internacionales en el sistema judicial ecuatoriano.

Declaración de conflicto de intereses

Los autores declaran que no existe ningún conflicto de interés.

Declaración sobre el uso de inteligencia artificial

Los autores declaran un uso mínimo de herramientas de inteligencia artificial en la elaboración de este

manuscrito, limitado a ajustes estilísticos en la redacción de secciones específicas y al apoyo en la generación de gráficos de visualización de datos. Toda la investigación, el análisis, la interpretación de resultados y las conclusiones son responsabilidad exclusiva de los autores.

Declaración de autoría

Ambos autores participaron en la concepción y diseño del estudio, en el análisis e interpretación de los datos, en la redacción del manuscrito y en la revisión crítica del contenido intelectual. La adquisición de datos y la búsqueda bibliográfica fueron realizadas por Alina-Maria Bracho-Rodriguez. Ramon-A Toala-Dueñas brindó la supervisión general del estudio.

Bibliografía

Abd Elmonsef Sarhan, S., Youness, H. A., & Bahaa-Eldin, A. M. (2023). A framework for digital forensics of encrypted real-time network traffic, instant messaging, and VoIP application case study. Ain Shams Engineering Journal, 14, Article 102069. https://doi.org/10.1016/j.asej.2022.102069

Adijisman, R., & Riadi, I. (2021). Mobile forensic on WhatsApp services using National Institute of Standards and Technology method. International Journal of Computer Applications, 183(29), 41–48. https://doi.org/10.5120/ijca2021921680

Aniza, S. N., & Riadi, I. (2021). Mobile forensic for cyber fraud case on WhatsApp services using National Institute of Standard Technology method. International Journal of Computer Applications, 183(41), 44–50. https://doi.org/10.5120/ijca2021921811

Avemañay Lema, S. A., Avemañay Lema, A. J., & Duarte Correa, M. A. (2025). La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica. Ciencia Latina Revista Científica Multidisciplinar, 9(6), 17879–17900. https://doi.org/10.37811/cl_rcm.v9i6.21212

Ávila Silva, J. M., García Rodríguez, O., & Aguilera Durán, J. (2023). Facebook y WhatsApp como pruebas digitales en el Sistema Penal Acusatorio en México. Advocatus, 20(41), 57–75.

https://dialnet.unirioja.es/servlet/articulo?codigo=9611165

Banegas-Crespo, D. A., & Andrade-Pesantez, D. J. (2024). Análisis forense en dispositivos móviles Android para casos de ciberextorsión, revisión sistemática de literatura. MQRInvestigar, 8(3), 4076–4097. https://doi.org/10.56048/MQR20225.8.3.2024.4076-4097

Bogos, C.-E., Mocanu, R., & Simion, E. (2023). A security analysis comparison between Signal, WhatsApp and Telegram. Cryptology ePrint Archive, Paper 2023/071. https://eprint.iacr.org/2023/071

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

De la Torre Muñoz, F. M., Puertas Realpe, A. X., & Burbano Peña, C. E. (2024). Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador. INNOVACIÓN & SABER, (9), 43–57. https://innovacionysaber.isupol.edu.ec/index.php/innovacion/article/view/280

Deo, T., Kaur, M., & Kaplesh, P. (2023). A novel framework for WhatsApp forensics using open-source tools. Digital Forensics (4N6) Journal, 1(1), 1–17. https://www.researchgate.net/publication/373076630_A_NOVEL_FRAMEWORK_FOR_WHATSAPP_FORENSICS_USING_OPEN-SOURCE_TOOLS

Deviriana, B. I., Nurdianti, D., Chandra, F. T., Nagib, M., & Danella, X. (2025). Analysis of WhatsApp chat usage as court evidence. Devotion: Journal of Research and Community Service, 6(6), 574–583. https://doi.org/10.59188/devotion.v6i6.25492

Egho-Promise, I., Ola, B., Arhin, A., & Asuming, R. (2020). A forensic analysis of WhatsApp on Android smart phone. International Research Journal of Computer Science, 7(8), 209–219. https://doi.org/10.26562/irjcs.2020.v0708.001

Fathiyana, R. Z., Yudiansyah, Cahyadi, N., & Hidayat, D. J. (2023). A comparative study and analysis of forensic artifacts of WhatsApp and Telegram on Android devices. Journal of Informatics and

Communication Technology, 4(2), 109–118. https://doi.org/10.52661/j_ict.v4i2.143

Fayyad-Kazan, H., Kassem-Moussa, S., Hejase, H. J., & Hejase, A. J. (2022). Forensic analysis of WhatsApp SQLite databases on the unrooted Android phones. HighTech and Innovation Journal, 3(2), 175–194. https://doi.org/10.28991/HIJ-2022-03-02-06

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

Heath, H., MacDermott, A., & Akinbi, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? Forensic Science International: Digital Investigation, 46, Article 301585. https://doi.org/10.1016/j.fsidi.2023.301585

Mohd Idris, A. S., & Ab Rahman, N. H. (2022). A Comparative Analysis of Potential Digital Evidence in WhatsApp Web-Based and Mobile-Based Application. Applied Information Technology And Computer Science, 3(2), 84-100. https://publisher.uthm.edu.my/periodicals/index.php/aitcs/article/view/7492

Kaushik, K., & Katara, Y. (2022). Forensic analysis of WhatsApp chat data. In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1–6). IEEE. https://www.researchgate.net/publication/366149178_Forensic_Analysis_of_WhatsApp_chat_data

Kim, G., Hur, U., Kang, S., & Kim, J. (2025). Analyzing the Web and UWP versions of WhatsApp for digital forensics. Forensic Science International: Digital Investigation, 52, Article 301861. https://doi.org/10.1016/j.fsidi.2024.301861

Llugsha Chicaiza, O. A., Arcos Pineda, M. F., Freire Gaibor, E. F., & Castillo López, L. M. (2025). La prueba digital en el proceso penal ecuatoriano: Análisis normativo, probatorio y jurisprudencial. Reincisol, 4(8), Article 1251. https://doi.org/10.59282/reincisol.V4(8)1251

Lovera, F., & Farias, L. A. (2024). Prueba electrónica en el proceso civil: WhatsApp y Telegram. En XXV Jornada sobre Experiencias en Investigación (pp. 92–98). Facultad de Derecho, Universidad Nacional de Córdoba. https://revistas.unc.edu.ar/index.php/rjei/article/view/48555

Manzoor, I., Ghani, R., & Hamid, K. (2025). Challenges of data extraction from Facebook & WhatsApp applications. Journal of Computing & Biomedical Informatics, 9(2). https://www.jcbi.org/index.php/Main/article/view/1050

Martínez Guerrero, A. (2022). Incorporación de los WhatsApp y otras aplicaciones semejantes de mensajería electrónica al proceso penal en la fase de instrucción. Revista Acta Judicial, 10, 20–36. https://dialnet.unirioja.es/servlet/articulo?codigo=9204564

Martínez Guerrero, A. (2025). A vueltas con el WhatsApp y semejantes como fuente de prueba en la fase instructora del proceso penal. Revista Claves Jurídicas, 1(enero-junio), 2–21. https://doi.org/10.14679/9987

Morante Mendoza, L. E., Safadi Mendoza, J. A., & Gómez Rivera, G. P. (2025). Delitos informáticos y prueba digital en el COIP: Validez, cadena de custodia y pericia forense en el Ecuador. Tesla Revista Científica, 5(2), Article e542. https://doi.org/10.55204/trc.v5i2.e542

Nahdli, M. F. M., Riadi, I., & Biddinika, M. K. (2024). Forensic analysis of the WhatsApp application using the National Institute of Justice framework. International Journal of Advances in Data and Information Systems, 5(2), 113–122. https://doi.org/10.59395/ijadis.v5i2.1328

Onik, A. R., Brown, J., Walker, C., & Baggili, I. (2025). A systematic literature review of secure instant messaging applications from a digital forensics perspective. ACM Computing Surveys, 57(9), Article 239. https://doi.org/10.1145/3727641

Paligu, F., & Varol, C. (2020). Browser forensic investigations of WhatsApp Web utilizing IndexedDB persistent storage. Future Internet, 12(11), Article 184. https://doi.org/10.3390/fi12110184

Pandey, S., Rahman, R. U., Phulre, A. K., Samara, G., Lamkuche, H. S., & Sbaih, A. (2025). Forensic framework for deleted media of WhatsApp

on Windows. In A. M. A. Musleh Al-Sartawi et al. (Eds.), Business resilience and business innovation for sustainability (Studies in Systems, Decision and Control, Vol. 587, pp. 2059–2076). Springer. https://doi.org/10.1007/978-3-031-87584-7_149

Pirzada, S., Ab Rahman, N. H., Cahyani, N. D. W., & Othman, M. F. (2023). A survey of forensic analysis and information visualization approach for instant messaging applications. International Journal of Advanced Computer Science and Applications, 14(2), 237–246. https://doi.org/10.14569/IJACSA.2023.0140229

Prabowo, W. A., Mohsen, F., & Selamat, S. R. (2025). WhatsApp mobile applications in the lens of digital forensics: Deciphering the Msgstore.db.crypt14 file. Journal of Cyber Security and Mobility, 14(4), 823–848. https://doi.org/10.13052/jcsm2245-1439.1443

Robledo, M., & Robledo, F. (2022). La prueba de WhatsApp: Cuestiones procesales y constitucionales. Revista de Derecho Procesal y de Derechos Humanos, 1(1), 187–201. https://revistas.unc.edu.ar/index.php/procesal/article/view/40815

Rotaru, G., & Tatu, G. (2021). Mobile forensic tools: An insight into WhatsApp Key DB Extractor. Romanian Cyber Security Journal, 3(2), 67–76. https://rocys.ici.ro/documents/20/2021_fall_article_7.pdf

Sánchez Gálvez, F. E. (2020). Conversaciones de la aplicación WhatsApp y ejemplos de su valor probatorio como evidencia digital en la legislación guatemalteca. Revista Científica Diálogo Forense, 2(2), 29–39. https://dialogoforense.inacif.gob.gt/public/journals/3/articles/26/605e14a398684.pdf

Sánchez Pérez, C. P. (2025). El derecho a confrontar una captura de pantalla de WhatsApp en el proceso penal. Revista Quaestio Iuris, 15, 250–267. https://doi.org/10.70467/rqi.n15.13

Shadeed, M., Arram, L. A., & Owda, M. (2022). Forensic analysis of “WhatsApp” artifacts in Android without root. Advances in Science, Technology and Engineering Systems Journal, 7(2), 127–132. https://doi.org/10.25046/aj070212

Sharma, A., Yadav, B., & Sharma, B. (2025). Efficiency and reliability of forensic tools in recovering Android WhatsApp data: A comparative study. International Journal of Applied Mathematics, 38(7s), 1044–1053. https://ijamjournal.org/ijam/publication/index.php/ijam/article/view/533

Shidek, H., Cahyani, N. D. W., & Wardana, A. A. (2020). WhatsApp Chat Visualizer: A visualization of WhatsApp Messenger's artifact using the timeline method. International Journal on ICT, 6(1), 1–9. https://doi.org/10.21108/IJOICT.2020.61.489

Soares, A. M. M. (2022). WhatsApp Web Client Live Forensics Technique. In Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022) (pp. 629–636). SCITEPRESS. https://doi.org/10.5220/0011006400003120

Soni, N. (2024). Forensic analysis of WhatsApp: A review of techniques, challenges, and future directions. Journal of Forensic Science and Research, 8, 19–24. https://doi.org/10.29328/journal.jfsr.1001059

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. https://doi.org/10.5109/7172316

Sulisdyantoro, D., & Marzuki, M. I. (2023). Identification of WhatsApp digital evidence on Android smartphones using the Android Backup Application Package Kit (APK) Downgrade method. Journal of Integrated and Advanced Engineering, 3(1), 7–22. https://doi.org/10.51662/jiae.v3i1.70

Torres Loján, C. G. (2024). WhatsApp como herramienta de prueba en litigios por obligaciones financieras: Una mirada al sistema judicial ecuatoriano. Revista Lex, 7(25), 496–511. https://doi.org/10.33996/revistalex.v7i25.196

Utomo, D. S. I., Prayudi, Y., & Ramadhani, E. (2023). Forensic web analysis on the latest version of WhatsApp browser. Journal of Computer Networks, Architecture and High Performance Computing, 5(1), 359–367. https://doi.org/10.47709/cnahpc.v5i1.2286

Wijnberg, D., & Le-Khac, N.-A. (2021). Identifying

interception possibilities for WhatsApp communication. Forensic Science International: Digital Investigation, 38, Article 301132. https://doi.org/10.1016/j.fsidi.2021.301132

Zakarneh, S. K. A. (2024). Mobile forensic investigation on iOS & Android smartphones: Case study investigation on WhatsApp. International Journal of Applied Sciences and Smart Technologies, 6(1), 63–98. https://doi.org/10.24071/ijasst.v6i1.6770

Zamroni, G. M., & Riadi, I. (2020). Mobile forensic tools validation and evaluation for instant messaging. International Journal on Advanced Science, Engineering and Information Technology, 10(5), 1860–1866. https://doi.org/10.18517/ijaseit.10.5.7499