

ANÁLISIS JURÍDICO DEL USO DE LA EVIDENCIA DIGITAL EN LOS PROCESOS PENALES Y SU IMPACTO EN LA GARANTÍA DEL DEBIDO PROCESO

LEGAL ANALYSIS OF THE USE OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS AND ITS IMPACT ON THE GUARANTEE OF DUE PROCESS

María Fernanda Echeverría¹, Juan Carlos Baquero Salazar², Orlando Lenin Carrión³,
Melany Lisseth Escobar Garzon⁴

{maferecheverria@hotmail.com¹, juan.baquero.tse@gmail.com², mgs.orlando_carrión@hotmail.com³,
melany.lgc.23@gmail.com⁴}

Fecha de recepción: 08/07/2026 / Fecha de aceptación: 20/08/2026 / Fecha de publicación: 25/08/2026

RESUMEN: El uso de la evidencia digital en los procesos penales constituye uno de los fenómenos jurídicos más relevantes derivados de la transformación tecnológica de las últimas dos décadas, en la medida en que los sistemas de justicia penal de América Latina, y particularmente de Ecuador, enfrentan el reto de incorporar mensajes de datos, metadatos, imágenes, videos, registros de geolocalización y demás elementos electrónicos como medios de prueba válidos, sin comprometer las garantías del debido proceso. Este trabajo examinó, mediante una revisión sistemática de la literatura especializada siguiendo los parámetros PRISMA, el abordaje procesal de la evidencia digital en las causas penales y cómo esta repercute en las garantías del debido proceso. Se empleó una metodología documental de carácter cualitativo y con un alcance descriptivo-analítico; para lograrlo, se llevó a cabo una búsqueda estructurada en bases de datos indexadas aplicando criterios definidos de inclusión y exclusión, lo que permitió seleccionar un grupo final de artículos académicos publicados entre 2021 y 2026. Los hallazgos revelan que, aunque la normativa ecuatoriana y de la región admite el valor probatorio de los componentes informáticos, aún existen vacíos legales y operativos al resguardar la cadena de custodia, sumado a la ausencia de protocolos forenses uniformes, la limitada formación de los servidores judiciales y la falta de criterio único al momento de evaluar su autenticidad e integridad. Estas falencias perjudican de forma directa el derecho a la defensa, la contradicción de las pruebas y la imparcialidad en las resoluciones de los jueces. En consecuencia, asegurar una verdadera protección judicial frente a las pruebas tecnológicas exige adecuar las leyes locales a los parámetros internacionales, formalizar guías para las pericias y capacitar de forma permanente a los profesionales del sistema de justicia. Únicamente de esta manera se

¹Investigador Independiente, <https://orcid.org/0000-0002-7266-2906>

²BS Legal Tech, <https://orcid.org/0009-0004-1762-2778>

³Consultoría Jurídica Criminalística "Carrión", <https://orcid.org/0009-0005-1335-905X>

⁴Dirección Provincial, Consejo de la Judicatura de Tungurahua, <https://orcid.org/0009-0001-1124-1585>

podrá consolidar un juzgamiento penal transparente, riguroso y en apego estricto a los derechos constitucionales en el entorno digital.

Palabras clave: *prueba electrónica, cadena de custodia, informática forense, garantías judiciales, ciberdelincuencia*

ABSTRACT: The use of digital evidence in criminal proceedings is one of the most significant legal developments resulting from the technological transformation of the past two decades, as criminal justice systems in Latin America—and particularly in Ecuador—face the challenge of incorporating data messages, metadata, images, videos, geolocation records, and other electronic elements as valid forms of evidence without compromising due process guarantees. This study examined, through a systematic review of the specialized literature following the PRISMA guidelines, the procedural approach to digital evidence in criminal cases and how it impacts due process guarantees. A qualitative, descriptive-analytical documentary methodology was employed; to achieve this, a structured search was conducted in indexed databases using defined inclusion and exclusion criteria, which allowed for the selection of a final set of academic articles published between 2021 and 2026. The findings reveal that, although Ecuadorian and regional regulations recognize the evidentiary value of digital evidence, there are still legal and operational gaps in safeguarding the chain of custody, compounded by the absence of uniform forensic protocols, limited training for judicial officials, and the lack of a single standard for evaluating the authenticity and integrity of such evidence. These shortcomings directly undermine the right to a defense, the right to challenge evidence, and the impartiality of judicial rulings. Consequently, ensuring genuine judicial protection against digital evidence requires aligning local laws with international standards, formalizing guidelines for forensic analysis, and providing ongoing training to professionals in the justice system. Only in this way can a transparent and rigorous criminal justice process be established, one that strictly adheres to constitutional rights in the digital environment.

Keywords: *electronic evidence, chain of custody, computer forensics, judicial safeguards, cybercrime*

INTRODUCCIÓN

La sociedad contemporánea atraviesa un proceso de transformación digital que ha modificado de manera sustancial la forma en que se cometen, se investigan y se judicializan los hechos delictivos. El uso masivo de dispositivos móviles, redes sociales, sistemas de mensajería, plataformas de almacenamiento en la nube y dispositivos del internet de las cosas ha generado un volumen creciente de información susceptible de constituirse en fuente de prueba dentro de los procesos penales (1). Este fenómeno ha dado lugar a la categoría jurídica de evidencia digital, entendida como todo dato o información almacenada o transmitida en formato binario que puede ser utilizada como elemento de convicción dentro de un proceso judicial (15). A diferencia de la prueba

tradicional, la evidencia digital se caracteriza por su volatilidad, su fácil alterabilidad y la necesidad de conocimientos técnicos especializados para su identificación, recolección, preservación y análisis, tal como lo evidencian estudios recientes sobre el análisis forense de memoria volátil aplicado a delitos comunes con componente tecnológico en el contexto ecuatoriano (3), lo que exige el desarrollo de protocolos forenses rigurosos que garanticen su autenticidad e integridad a lo largo de toda la cadena de custodia (4).

A escala internacional, organismos como el Consejo de Europa impulsaron desde el año 2001 el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, como el primer instrumento vinculante orientado a armonizar la persecución penal de los delitos informáticos y a establecer criterios comunes para la obtención de prueba electrónica entre Estados (17). De manera paralela, la Organización Internacional de Normalización desarrolló la familia de normas ISO/IEC 27037 e ISO/IEC 27042, que fijan directrices técnicas para la identificación, recolección, adquisición, preservación, análisis e interpretación de la evidencia digital, convirtiéndose en referentes de buenas prácticas forenses adoptados por laboratorios policiales y peritos informáticos de distintos países (15,16).

En América Latina, el crecimiento exponencial de los delitos informáticos ha superado, en muchos casos, la capacidad de respuesta normativa e institucional de los sistemas de justicia penal. Según el diagnóstico regional elaborado por la Organización de los Estados Americanos, los países de la región enfrentan brechas significativas en materia de infraestructura forense, capacitación de operadores de justicia y cooperación internacional para la obtención de evidencia digital transfronteriza, lo cual repercute directamente en la eficacia de la persecución penal y en la protección de los derechos de las personas procesadas (2). Estudios comparados desarrollados en países como España, Colombia, Chile y Perú evidencian igualmente tensiones entre la necesidad de incorporar tecnología a la investigación penal y el respeto a garantías como la intimidad, la inviolabilidad de las comunicaciones y el derecho de defensa (5).

En el caso particular de Ecuador, el Código Orgánico Integral Penal reconoce expresamente a los mensajes de datos, registros informáticos, correos electrónicos y demás documentos digitales como medios de prueba válidos dentro del proceso penal, y regula, aunque de manera general, la cadena de custodia y la actuación de peritos acreditados (8). Sin perjuicio de este reconocimiento normativo, diversas investigaciones desarrolladas en el país han identificado deficiencias relevantes en su aplicación práctica: ausencia de protocolos técnicos unificados, insuficiencia de infraestructura forense especializada, escasez de peritos informáticos acreditados y disparidad de criterios judiciales para valorar la autenticidad e integridad de la prueba digital (5,6,7). Estas deficiencias adquieren especial relevancia constitucional, en la medida en que el artículo 76 de la Constitución de la República del Ecuador consagra el debido proceso como conjunto de garantías básicas aplicables a todo procedimiento en el que se determinen derechos y obligaciones, entre ellas la presunción de inocencia, el derecho a la defensa, la contradicción de la prueba y la motivación de las resoluciones judiciales (9).

El debido proceso, además de su consagración constitucional interna, encuentra fundamento en el artículo 8 de la Convención Americana sobre Derechos Humanos, que reconoce el derecho de toda persona a ser oída con las debidas garantías por un juez o tribunal competente, independiente e imparcial (10). La Corte Interamericana de Derechos Humanos ha desarrollado una jurisprudencia consolidada sobre los componentes del debido proceso penal, entre ellos el derecho de defensa, el acceso a la prueba de cargo y la posibilidad efectiva de controvertirla, estándares que resultan plenamente aplicables al tratamiento de la evidencia digital (11). Cuando la cadena de custodia de un elemento digital se rompe, cuando no existen protocolos verificables de recolección o cuando el perito informático carece de acreditación técnica, se abre la posibilidad de que la prueba sea cuestionada por manipulación, afectando garantías como la contradicción y la igualdad de armas procesales.

Desde una perspectiva criminológica, el crecimiento de los delitos que dejan rastro digital fraude informático, suplantación de identidad, extorsión mediante redes sociales, pornografía infantil en línea y violencia digital de género, entre otros ha convertido a la evidencia digital en el elemento probatorio central de un número creciente de causas penales, incluso en delitos tradicionalmente investigados mediante prueba física, como el homicidio o el robo, en los que los registros de geolocalización, las cámaras de videovigilancia y los metadatos de dispositivos móviles se han incorporado como piezas clave de la investigación (1,2). Está marcada relevancia de la prueba informática intensifica el impacto legal ante cualquier falla en su manejo pericial: una modificación en la cadena de custodia o una obtención al margen de la ley no solo invalida un dato aislado, sino que llega a anular el juicio entero. Esto abre la puerta tanto a que queden impunes diversos delitos como a que se sancione injustamente a personas inocentes a partir de información alterada o defectuosa (3,4).

Frente a este panorama, resulta necesario sistematizar el conocimiento científico disponible sobre el tratamiento jurídico de la evidencia digital en los procesos penales y su relación con las garantías del debido proceso, identificando los principales vacíos normativos, técnicos y jurisprudenciales documentados en la literatura especializada de los últimos años. En este sentido, el objetivo general del presente estudio fue analizar, mediante una revisión sistemática de la literatura científica, el tratamiento jurídico de la evidencia digital en los procesos penales y su impacto en la garantía del debido proceso, con énfasis en el contexto ecuatoriano y latinoamericano.

El problema de investigación abordado en este estudio se sitúa en la intersección entre el derecho procesal penal, el derecho constitucional y la informática forense, tres campos disciplinares que, según la literatura revisada, no siempre dialogan de manera articulada en la práctica judicial. Mientras el legislador ha avanzado en el reconocimiento formal de la evidencia digital como medio de prueba, el desarrollo de capacidades técnicas periciales y de protocolos institucionales de actuación no ha seguido el mismo ritmo, generando una asimetría que traslada a los jueces la carga de resolver, caso por caso y sin criterios uniformes, cuestiones eminentemente técnicas relativas a la autenticidad, integridad y trazabilidad de la prueba electrónica (6,7).

A pesar del reconocimiento normativo de la evidencia digital como medio de prueba válido en el proceso penal ecuatoriano y en la mayoría de los ordenamientos latinoamericanos, subsiste una brecha entre dicho reconocimiento formal y las condiciones técnicas e institucionales necesarias para garantizar su autenticidad, integridad y confiabilidad probatoria (5,6). Esta brecha se traduce en prácticas heterogéneas de recolección y preservación de la evidencia, ausencia de protocolos nacionales estandarizados, insuficiente acreditación de peritos informáticos forenses y criterios judiciales dispares para admitir o excluir prueba digital, lo cual genera incertidumbre jurídica tanto para la Fiscalía como para la defensa técnica (12,13). El problema adquiere especial gravedad cuando se advierte que la vulneración de la cadena de custodia digital no solo compromete la eficacia de la persecución penal, sino que puede derivar en la afectación de derechos fundamentales del procesado, al admitirse como prueba de cargo elementos cuya trazabilidad no puede ser plenamente verificada (14). En consecuencia, se plantea la siguiente pregunta de investigación: ¿cuál es el tratamiento jurídico que la literatura científica ha documentado respecto del uso de la evidencia digital en los procesos penales de Ecuador y América Latina, y de qué manera dicho tratamiento incide en la garantía del debido proceso?

Esta investigación analizó, mediante una revisión sistemática de la literatura académica aplicando el enfoque PRISMA, la regulación legal de las pruebas digitales dentro del sistema penal y su impacto en las garantías del debido proceso. El estudio examinó con especial énfasis el panorama de Ecuador y América Latina, compilando la producción científica difundida entre 2021 y 2026.

MATERIALES Y MÉTODOS

Este estudio emplea un diseño documental, elaborado a partir de una perspectiva cualitativa y con un nivel descriptivo-analítico. Su desarrollo se llevó a cabo mediante un examen sistemático de literatura especializada, alineado a los lineamientos de la declaración PRISMA 2020. Este esquema metodológico asegura un proceso claro y riguroso en las etapas de localización, selección, evaluación de la calidad probatoria e incorporación de los textos que constituyen la muestra final de análisis, disminuyendo de forma significativa el sesgo propio de las revisiones teóricas habituales.

La recolección de información se llevó a cabo entre junio y agosto de 2026 en bases de datos especializadas como Scopus, Dialnet, Redalyc, SciELO, Latindex y Google Académico, reforzada con el acceso a bibliotecas digitales universitarias de la región y repositorios jurídicos orientados a tecnología y derecho procesal. Las fórmulas de búsqueda combinaron descriptores como «evidencia digital», «prueba digital», «proceso penal», «debido proceso», «cadena de custodia» y «ciberdelito» mediante operadores booleanos AND y OR, añadiendo además sus equivalentes en inglés («digital evidence», «criminal proceedings», «due process») para extender la cobertura bibliográfica.

El proceso de selección dio prioridad a artículos indexados con evaluación por pares, tesis de posgrado, informes institucionales y capítulos de libros difundidos entre 2021 y

2026, redactados en español o inglés, con acceso a texto completo y centrados en el uso de la prueba informática en la justicia penal. Se descartaron publicaciones no arbitradas, registros duplicados, contenidos no científicos y trabajos técnicos carentes de análisis normativo-procesal.

El rastreo inicial identificó 138 registros. Tras eliminar 22 duplicados, se analizaron 116 mediante título y resumen, descartando 61 por no ajustarse al objeto de estudio. De los 55 trabajos revisados a texto completo, se depuraron 24 por incumplir los criterios de rigor (12 puramente informáticos, 7 sin arbitraje formal y 5 redundantes), consolidando una muestra final de 31 publicaciones académicas procesadas mediante matrices de análisis sintético.

Tabla 1. Fases del proceso de selección según el método PRISMA.

Fase	N.º de registros	Observación
Identificación	138	Búsqueda en bases indexadas y repositorios
Duplicados eliminados	22	Gestor bibliográfico y revisión manual
Cribado (título/resumen)	116	61 excluidos por falta de pertinencia temática
Elegibilidad (texto completo)	55	24 excluidos por criterios de calidad/pertinencia
Incluidos en la síntesis	31	Muestra final analizada

Los 31 documentos seleccionados se catalogaron en una plantilla bibliográfica que registró autoría, año de publicación, país, tipo de estudio, metodología y hallazgos principales. Sobre esta base, se efectuó un análisis de contenido cualitativo destinado a identificar patrones recurrentes, estructurados en cuatro ejes temáticos: (a) marco normativo de la prueba digital; (b) garantías procesales y exigencias técnicas; (c) valoración probatoria del material informático; y (d) tutela del debido proceso. Dado el enfoque cualitativo-documental del trabajo, no se utilizaron modelos estadísticos inferenciales, restringiendo el tratamiento de datos al cálculo descriptivo básico (frecuencias y porcentajes) para caracterizar el cuerpo de literatura examinado.

RESULTADOS

Los resultados de la presente revisión sistemática se organizan siguiendo los cuatro ejes temáticos derivados del análisis de contenido de la muestra documental, precedidos de una caracterización general de los estudios incluidos. Esta organización permite ofrecer una lectura integral del estado del arte sobre la evidencia digital en el proceso penal, desde su reconocimiento normativo hasta su incidencia concreta en las garantías del debido proceso, pasando por los aspectos técnico-forenses y de valoración judicial que constituyen el núcleo del debate identificado en la literatura especializada.

De un total de 31 indagaciones analizadas en la presente investigación, el 58 % (n=18) deriva de publicaciones distribuidas en revistas científicas ecuatorianas indexadas en Latindex, Dialnet y diversos repertorios regionales. Asimismo, un 23 % (n=7) encuentra

su origen en estudios comparados procedentes de otras naciones iberoamericanas, mientras que el 19 % (n=6) que resta se compone de marcos regulatorios, dictámenes técnicos e jurisprudencia interamericana. En lo que concierne a la fecha de emisión, el 74 % de los insumos bibliográficos se sitúa entre 2023 y 2026, lo cual refleja una atención académica cada vez mayor frente a la convergencia entre la prueba digital y las garantías del debido proceso.

Tabla 2. Distribución de la muestra documental según eje temático.

Eje temático	n	%	Fuente principal
Marco normativo de la evidencia digital	9	29 %	COIP, COGEP, LOPD
Cadena de custodia y estándares técnicos	11	35 %	ISO/IEC 27037, ISO/IEC 27042
Valoración judicial de la prueba digital	6	20 %	Jurisprudencia y doctrina procesal
Garantías del debido proceso	5	16 %	Constitución, CADH, Corte IDH

Marco normativo de la evidencia digital

El análisis documental evidencia que el Código Orgánico Integral Penal reconoce expresamente a los documentos electrónicos, mensajes de datos y registros informáticos como medios de prueba, remitiendo de manera complementaria a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos para efectos de su valoración probatoria (8). No obstante, los estudios coinciden en señalar que dicha regulación resulta insuficiente frente a la complejidad técnica de la evidencia digital contemporánea, al no establecer protocolos específicos y unificados de recolección para dispositivos móviles, sistemas en la nube o servidores institucionales, dejando dicha estandarización librada a propuestas técnicas puntuales antes que a una política pública consolidada (1,6). En el ámbito comparado, los ordenamientos de España, Colombia, Chile y Perú presentan un desarrollo normativo desigual: mientras España cuenta con regulación específica sobre diligencias de investigación tecnológica, Ecuador y otros países de la región carecen todavía de un marco legal autónomo para la prueba electrónica, apoyándose en disposiciones generales del código procesal penal (5,20).

Cadena de custodia y estándares técnicos

El eje temático con mayor frecuencia documental fue el relativo a la cadena de custodia digital, presente en el 35 % de la muestra. Los estudios revisados identifican de manera reiterada la ausencia de protocolos técnicos unificados a nivel nacional en Ecuador para la identificación, recolección, embalaje, transporte y almacenamiento de dispositivos electrónicos, lo que incrementa el riesgo de contaminación o alteración de la evidencia antes de su análisis pericial (12,22). Se documenta igualmente la escasa adopción formal de estándares internacionales como la norma ISO/IEC 27037, que establece los principios de auditabilidad, repetibilidad, reproducibilidad y justificabilidad como condiciones mínimas para garantizar la fiabilidad de la evidencia digital (15,16). Casos judiciales analizados en la literatura ilustran cómo la falta de coincidencia entre los

valores hash registrados al momento de la incautación y los verificados en la fase pericial ha derivado en la declaratoria de nulidad o exclusión de la prueba por ruptura de cadena de custodia (14).

Asimismo, se identifica en la región una carencia significativa de peritos informáticos forenses acreditados y de laboratorios especializados dotados de herramientas de duplicación forense bit a bit, lo que obliga en muchos casos a recurrir a peritos externos o a organismos de cooperación internacional, generando dilaciones procesales y encareciendo el acceso a la justicia (6,24). La Organización de los Estados Americanos ha señalado que esta limitación de capacidades técnicas constituye uno de los principales obstáculos para la persecución efectiva de la ciberdelincuencia en la región (2).

Valoración judicial de la prueba digital

En cuanto a la valoración judicial, los estudios revisados evidencian criterios dispares entre operadores de justicia respecto de la admisibilidad de capturas de pantalla, conversaciones de mensajería instantánea y publicaciones en redes sociales como prueba de cargo, en ausencia de peritajes técnicos que certifiquen su autenticidad (13,25). Se documenta una tendencia jurisprudencial creciente a exigir la verificación técnica de metadatos y la trazabilidad completa de la cadena de custodia como condición de admisibilidad, aunque dicha exigencia no se aplica de manera uniforme en todas las judicaturas del país (28,29). Por otra parte, algunos estudios advierten sobre el riesgo de una valoración judicial excesivamente formalista, que podría descartar evidencia digital sustancialmente relevante por defectos procedimentales menores, en desmedro de la búsqueda de la verdad material (21,23).

Garantías del debido proceso

Los documentos que abordan directamente la relación entre evidencia digital y debido proceso destacan tres tensiones principales. En primer lugar, la posible afectación del derecho a la intimidad y a la inviolabilidad de las comunicaciones durante la obtención de evidencia digital sin las debidas autorizaciones judiciales, así como el riesgo de que dicha prueba sea utilizada de manera selectiva o a conveniencia por las partes procesales (30). En segundo lugar, las limitaciones al derecho de defensa cuando la parte procesada no cuenta con acceso oportuno ni con capacidad técnica para controvertir la prueba digital de cargo, lo que compromete el principio de igualdad de armas (11,31). En tercer lugar, la exigencia de motivación judicial reforzada cuando la condena se sustenta de manera preponderante en evidencia digital, en virtud de los estándares fijados por la Corte Interamericana de Derechos Humanos en materia de garantías judiciales (10,11). Estos hallazgos convergen en señalar que la validez técnica de la evidencia digital constituye una condición necesaria, aunque no suficiente, para garantizar el respeto integral del debido proceso, el cual exige además condiciones de contradicción, igualdad procesal y motivación judicial suficiente.

Jurisprudencia comparada y casos ilustrativos

El análisis documental identificó varios casos ilustrativos citados de manera reiterada en la literatura revisada, que permiten observar la aplicación práctica de los principios antes descritos. En un caso analizado dentro de la muestra, la absolución de los procesados se fundamentó, entre otros elementos, en la constatación de que los valores hash del material informático incautado no coincidían con los registrados en el acta policial al momento de la intervención, lo que llevó al tribunal a declarar la evidencia contaminada, inválida y no fiable, por ausencia de certeza sobre su preservación y autenticidad (14). Este tipo de precedentes refuerza la importancia práctica y no meramente teórica de los estándares técnicos de preservación de la evidencia digital, en la medida en que su inobservancia puede determinar directamente el sentido del fallo. En el ámbito ecuatoriano, la Corte Nacional de Justicia ha tenido oportunidad de pronunciarse sobre la valoración de prueba electrónica en procesos por delitos informáticos, reiterando que la sola existencia del dato digital no basta para acreditar su autenticidad si no se documenta el proceso técnico de su obtención (22).

En el plano comparado, los estudios revisados sobre Colombia documentan un desarrollo jurisprudencial orientado a exigir la intervención de peritos acreditados y la aplicación de protocolos forenses estandarizados como condición de admisibilidad de la evidencia digital en los procesos judiciales, en línea con los principios de la norma ISO/IEC 27037 (15,23). En Chile, el Ministerio Público ha desarrollado lineamientos institucionales específicos sobre integridad y autenticidad de la evidencia tecnológica, orientados a unificar los criterios de actuación de los fiscales a nivel nacional, un desarrollo institucional que, según los documentos analizados, todavía se encuentra en una etapa incipiente en el caso ecuatoriano (5). Estos hallazgos comparados sugieren que el fortalecimiento institucional antes que exclusivamente normativo constituye un factor determinante para la efectiva garantía del debido proceso frente a la evidencia digital.

DISCUSIÓN

Los resultados obtenidos confirman, en términos generales, los hallazgos reportados por Avemañay Lema et al. (5), quienes identificaron una brecha entre el reconocimiento normativo de la prueba digital en Ecuador y su aplicación práctica, marcada por la ausencia de protocolos técnicos y limitaciones en la cadena de custodia. Esta coincidencia sugiere que dicha brecha no constituye un hallazgo aislado, sino una tendencia sostenida en la literatura ecuatoriana reciente, también documentada por Navas-Abad y Vázquez-Martínez (6) y por Morante Mendoza et al. (12), quienes atribuyen el problema a la ausencia de una regulación específica sobre prueba electrónica, en contraste con la Ley Modelo de Prueba Electrónica impulsada para la región latinoamericana por organismos de cooperación internacional.

En relación con la cadena de custodia, los hallazgos de este estudio refuerzan lo señalado por Ordoñez Ordoñez et al. (14), quienes documentaron casos concretos de impunidad derivados de la ruptura de la cadena de custodia por parte de organismos de

seguridad, así como lo expuesto por Quichimbo Román et al. (13) respecto de la insuficiente regulación de la prueba digital en el Código Orgánico General de Procesos. Estos resultados son consistentes con la literatura internacional: Casey (3) y Kerr (4) sostienen desde hace más de una década que la volatilidad de la evidencia digital exige protocolos forenses más rigurosos que los aplicables a la prueba física tradicional, mientras que los estándares ISO/IEC 27037 e ISO/IEC 27042 constituyen, a nivel comparado, la referencia técnica más aceptada para su recolección y análisis (15,16), coincidencia que respalda la recomendación, sostenida por múltiples estudios de la muestra, de adoptar formalmente dichos estándares en los protocolos periciales ecuatorianos.

No obstante, los resultados de este estudio matizan parcialmente las conclusiones de López (20) y de López Morales (21), quienes, en el contexto latinoamericano comparado, sostienen que la validez jurídica de la prueba digital se ha consolidado con mayor claridad en aquellos países que han desarrollado jurisprudencia específica sobre su admisibilidad. A diferencia de dicho escenario, la evidencia recopilada en el presente estudio indica que Ecuador continúa apoyándose en disposiciones procesales generales, sin un desarrollo normativo autónomo equivalente, lo que podría explicar la mayor disparidad de criterios judiciales identificada en la valoración de la prueba digital ecuatoriana frente a la observada en los sistemas comparados (28).

Respecto de las garantías del debido proceso, los hallazgos coinciden con la jurisprudencia de la Corte Interamericana de Derechos Humanos en el caso Suárez Rosero vs. Ecuador, en cuanto reafirman que el derecho de defensa exige el acceso oportuno y efectivo a los elementos de prueba que sustentan la acusación (11). Esta convergencia refuerza la tesis, sostenida también por Mendoza (25) y por San Martín Andrade et al. (26), de que la validez técnica de la evidencia digital resulta insuficiente si no se garantizan condiciones procesales de contradicción e igualdad de armas. Sin embargo, a diferencia de posturas más deterministas que atribuyen la vulneración del debido proceso exclusivamente a factores tecnológicos, los resultados de este estudio sugieren que las principales causas identificadas en la literatura son de naturaleza institucional y organizacional falta de protocolos, insuficiente capacitación, escasez de peritos acreditados antes que estrictamente tecnológicas, lo que reorienta las recomendaciones de política pública hacia el fortalecimiento institucional más que hacia la sola actualización normativa.

Un aspecto adicional que merece discusión es la efectividad práctica de los instrumentos de cooperación internacional en materia de evidencia digital transfronteriza. Si bien el Convenio de Budapest constituye el marco de referencia más citado en la literatura para la obtención de prueba electrónica alojada en servidores ubicados fuera de la jurisdicción nacional (17), Ecuador no forma parte de dicho instrumento como Estado suscriptor pleno, lo que, de acuerdo con los estudios revisados, dificulta los procesos de asistencia judicial mutua y de conservación expedita de datos informáticos ante proveedores de servicios internacionales de mensajería y redes sociales (2,7). Esta limitación coincide con lo señalado por la Organización de los Estados Americanos en su diagnóstico regional, que identifica a la cooperación internacional como uno de los

componentes más rezagados de la respuesta estatal frente a la ciberdelincuencia en América Latina (2), y sugiere que las reformas normativas internas, por sí solas, resultan insuficientes si no se acompañan de una política exterior activa en materia de cooperación judicial digital.

Finalmente, conviene señalar como limitación del presente estudio el carácter eminentemente documental de la revisión, que no incorporó un componente empírico primario mediante entrevistas o encuestas a operadores de justicia, a diferencia de estudios mixtos como el de Avemañay Lema et al. (5). Se recomienda que futuras investigaciones complementen la presente revisión sistemática con estudios de campo que permitan contrastar los hallazgos documentales con la práctica judicial cotidiana en las distintas judicaturas del país.

CONCLUSIONES

La revisión sistemática de la literatura evidencia que, si bien el ordenamiento jurídico ecuatoriano y la mayoría de los sistemas penales latinoamericanos reconocen normativamente la validez de la evidencia digital como medio de prueba, dicho reconocimiento formal no se encuentra acompañado de un desarrollo técnico-procedimental suficiente, lo que genera una brecha estructural entre la norma y su aplicación práctica en el proceso penal.

El fortalecimiento de la cadena de custodia digital, mediante la adopción de estándares técnicos internacionalmente reconocidos como la norma ISO/IEC 27037 y la acreditación formal de peritos informáticos forenses, constituye una condición indispensable para garantizar la autenticidad e integridad de la evidencia digital y, con ello, para prevenir su exclusión o nulidad por defectos procedimentales.

El impacto de la evidencia digital en la garantía del debido proceso no depende exclusivamente de factores tecnológicos, sino principalmente de condiciones institucionales relacionadas con la capacitación especializada de jueces, fiscales, defensores y peritos, así como con la existencia de protocolos claros que aseguren el derecho de defensa, la contradicción y la motivación judicial reforzada en aquellos procesos penales sustentados de manera preponderante en prueba electrónica, respondiendo así al objetivo general planteado en el presente estudio.

REFERENCIAS BIBLIOGRÁFICAS

1. De la Torre Muñoz FM, Puertas Realpe AX, Burbano Peña CE. Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador. ISUPOL Rev Investig Segur Ciudadana Orden Público. 2024;(9):43-57.
2. Organización de los Estados Americanos. Ciberdelito en América Latina y el Caribe: diagnóstico regional 2022. Washington DC: Secretaría de Seguridad Multidimensional, OEA; 2022.

3. Vaca H. El análisis forense de memoria RAM como evidencia digital en delitos comunes: simulación de peculado en Ecuador. *Rev Dig Cienc Forense*. 2026;5(1).
4. Kerr OS. *Computer Crime Law*. 5th ed. St. Paul: West Academic Publishing; 2022.
5. Avemañay Lema SA, Avemañay Lema AJ, Duarte Correa MA. La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica. *Cienc Lat Rev Cient Multidiscip*. 2025;9(5):17880-900. doi:10.37811/cl_rcm.v9i6.21212
6. Navas-Abad CE, Vázquez-Martínez DS. La importancia de la prueba digital en los procedimientos penales en Ecuador. *Polo Conoc*. 2025;10(1):1742-75. doi:10.23857/pc.v10i1.8778
7. Herrera Zapata SM. El papel de la prueba digital en los procedimientos penales en Ecuador: marco legal, desafíos y necesidad de modernización [tesis de maestría]. Quito: Universidad Andina Simón Bolívar; 2025.
8. Asamblea Nacional del Ecuador. Código Orgánico Integral Penal. Registro Oficial Suplemento 180, 10 de febrero de 2014 (actualización 2023).
9. Constitución de la República del Ecuador. Registro Oficial 449, 20 de octubre de 2008.
10. Convención Americana sobre Derechos Humanos. Art. 8, Garantías Judiciales. San José: Organización de los Estados Americanos; 1969.
11. Corte Interamericana de Derechos Humanos. Caso Suárez Rosero Vs. Ecuador. Sentencia de fondo, 12 de noviembre de 1997.
12. Morante Mendoza LE, Safadi Mendoza JA, Gómez Rivera GP. Delitos informáticos y prueba digital en el COIP: validez, cadena de custodia y pericia forense en el Ecuador. *Tesla Rev Cient*. 2025;5(2):e542. doi:10.55204/trc.v5i2.e542
13. Quichimbo Román MA, Mereci Balcázar LS, Ramón Merchán ME. La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos. *Domin Cienc*. 2024;10(3):1126-42. doi:10.23857/dc.v10i3.3972
14. Ordoñez Ordoñez LA, Vásquez Olaya AY, Campoverde Nivicela LJ. La impunidad por violentarse la cadena de custodia por parte de la Policía Nacional. *Cienc Lat Rev Cient Multidiscip*. 2024;8(2):1742-75. doi:10.37811/cl_rcm.v8i2.11208
15. International Organization for Standardization. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO; 2012.
16. International Organization for Standardization. ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO; 2015.
17. Consejo de Europa. Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Budapest: Consejo de Europa; 2001.
18. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Rev Esp Cardiol*. 2021;74(9):790-9.
19. González Reyes M. Naturaleza y valoración de la evidencia digital. Salamanca: Universidad de Salamanca; 2021.
20. López JA. Evidencia digital y su admisibilidad en los procesos penales latinoamericanos. *Rev Iberoam Derecho Penal Proces*. 2023;10(2):55-74.

21. López Morales ZA. Validez jurídica de la prueba digital en Guatemala. *Rev Cienc Multidiscip CUNORI*. 2023;7(2).
22. Porras MA. La cadena de custodia digital en el proceso penal ecuatoriano. *Rev Ecuat Cienc Juríd*. 2023;12(3):87-105.
23. Yepes J, Cárdenas S, Gómez D. La evidencia digital en los procesos judiciales colombianos: un análisis forense comparado. *Rev Derecho Proces Comp*. 2022;8(1):33-49.
24. Espinoza EE. Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos en Ecuador. *Rev Cient*. 2024;8(2):101-15.
25. Mendoza M. Interpretación y desafíos de la evidencia digital en la investigación criminal. *Código Cient Rev Investig*. 2024;5(3):480-98. doi:10.55813/gaea/ccri/v5/nE3/328
26. San Martín Andrade MA, Bravo Moreno SR, Garza Lomas CD. Desafíos de la evidencia digital en la protección de datos personales: la cadena de custodia. *Rev Lechuzas*. 2026;2(4):1-14.
27. Espinales J. Análisis del derecho procesal y los entornos jurídicos. *Rev Cient Arbit Investig Comun Mark Empresa REICOMUNICAR*. 2023;6(12):89-97.
28. Riofrío García IA, Ruiz K, Lema P. La prueba electrónica en los procesos penales en Ecuador en concordancia con celeridad y economía procesal. *Serie Cient UCI*. 2025;18(2):49-62.
29. Imaicela Revilla JA, Alvarado Ajila LA. La incorporación de la prueba digital en el derecho procesal ecuatoriano. *Rev Lex*. 2024;7(27):1338-50. doi:10.33996/revistalex.v7i27.247
30. Valdés R. La excepcional limitación al derecho fundamental a la intimidad: una reflexión sobre la prueba ilícita y su uso a conveniencia. *Rev Derecho Debates Pers*. 2023.
31. Jiménez Guartán FA. La prueba digital y su valoración en el proceso penal ecuatoriano frente a las garantías constitucionales. *Polo Conoc*. 2026;11(1):1-18.