Tesla Revista Científica, ISSN: 2796-9320
Vol. 5 Núm. 2 (2025), e542

Área: Derecho
Artículo de Investigación Original

Delitos Informáticos y prueba digital en el COIP: validez, cadena de custodia y pericia forense en el Ecuador

Luis Eduardo Morante Mendoza[1][0009-0006-8633-0378], Jorge Andrés Safadi Mendoza [2][0009-0008-4951-3698]
Gonzalo Patricio Gómez Rivera [1][0000-0002-9216-6168]

[1] Municipio de Quevedo, Quevedo, Los Rios, Ecuador.
[2] Investigador Independiente, Portoviejo, Manabí, Ecuador.
[3] Investigador Independiente, Riobamba, Chimborazo, Ecuador.

emorante19@outlook.com tatosafadi@hotmail.com gpatriciogomez225@gmail.com

CITA EN APA:

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). https://doi.org/10.55204/trc.v5i2.e542

Recibido: 2025-08-02
Aceptado: 2025-09-24
Publicado: 2025-10-19

TESLA
Revista Científica
ISSN: 2796-9320

Resumen:
El presente artículo realiza una revisión bibliográfica sobre la validez de la prueba digital, la cadena de custodia y la pericia forense informática en el contexto penal ecuatoriano, con base en el Código Orgánico Integral Penal (COIP) y los estándares internacionales ISO/IEC y del Convenio de Budapest sobre la Ciberdelincuencia. Se adopta un enfoque cualitativo, descriptivo y analítico, sustentado en la revisión de fuentes doctrinarias, normativas y jurisprudenciales publicadas entre 2018 y 2025. Los resultados evidencian avances normativos en el reconocimiento de la evidencia digital, aunque persisten vacíos técnicos y procedimentales en su aplicación judicial. Se identifican deficiencias en la cadena de custodia, ausencia de protocolos nacionales y carencia de peritos forenses acreditados, lo cual compromete la autenticidad y fiabilidad de la prueba electrónica. Asimismo, se observa que Ecuador aún no ha incorporado plenamente los estándares internacionales sobre gestión probatoria digital ni se ha adherido al Convenio de Budapest, lo que limita la cooperación transfronteriza en casos de ciberdelitos. Finalmente, se proponen lineamientos para fortalecer el sistema penal ecuatoriano mediante la adopción de normas ISO, la creación de un instituto de pericia digital y la capacitación especializada de los operadores judiciales.
Palabras clave: Prueba digital; Cadena de custodia; Delitos informáticos; Pericia forense.

Abstract:
This article presents a bibliographic review on the validity of digital evidence, chain of custody, and computer forensic expertise within the Ecuadorian criminal justice context, based on the Comprehensive Organic Criminal Code (COIP) and international standards such as ISO/IEC and the Budapest Convention on Cybercrime. The study adopts a qualitative, descriptive, and analytical approach supported by a review of doctrinal, normative, and jurisprudential sources published between 2018 and 2025. The findings reveal legal progress in the recognition of digital evidence, although significant technical and procedural gaps persist in judicial practice. Deficiencies in the digital chain of custody, lack of national protocols, and the absence of certified forensic experts compromise the authenticity and reliability of electronic evidence. Additionally, Ecuador has not yet incorporated international standards on digital evidence management nor adhered to the Budapest Convention, limiting transnational cooperation in cybercrime investigations. The study proposes strategic measures to strengthen Ecuador's criminal justice system through the adoption of ISO standards, the creation of a national digital forensics institute, and the continuous training of judicial operators in technological and forensic competencies.
Keywords:
Digital evidence; Chain of custody; Cybercrime; Forensic expertise.

1. INTRODUCCIÓN

En la última década, el vertiginoso avance de las tecnologías de la información y comunicación (TIC) ha transformado profundamente la dinámica delictiva y, en consecuencia, los mecanismos de persecución penal. En Ecuador, este fenómeno se ha reflejado en un incremento sostenido de los delitos informáticos, tales como la suplantación de identidad, el fraude electrónico, el acceso ilícito a sistemas informáticos y la difusión no consentida de información digital. Según Sarmiento y Maldonado (2024), entre enero y agosto de 2020 se registraron más de 5.000 denuncias por delitos informáticos, representando un desafío sin precedentes para las instituciones judiciales encargadas de garantizar la seguridad jurídica en el entorno digital.

Ante esta realidad, la prueba digital (entendida como toda información generada, transmitida o almacenada mediante dispositivos electrónicos) ha adquirido un papel determinante en la investigación y juzgamiento de conductas delictivas. No obstante, su admisibilidad y validez en el proceso penal ecuatoriano continúan siendo objeto de debate, debido a la ausencia de protocolos técnicos y normativos estandarizados que aseguren la autenticidad, integridad y fiabilidad de dicha evidencia (Navas-Abad & Vázquez-Martínez, 2025).

El Código Orgánico Integral Penal (COIP) reconoce formalmente la validez de la prueba digital (arts. 456, 499 y 500); sin embargo, su aplicación práctica enfrenta vacíos legales y limitaciones operativas. La cadena de custodia, por ejemplo, carece de mecanismos específicos para evidencias electrónicas, lo que puede comprometer la trazabilidad y credibilidad de los elementos probatorios. Asimismo, la pericia forense informática, elemento clave en la verificación de autenticidad, aún no cuenta con una certificación nacional estandarizada que garantice uniformidad técnica en las investigaciones judiciales (Porras, 2023; Banegas & Andrade, 2022).

En el contexto internacional, organismos como el Consejo de Europa a través del Convenio de Budapest sobre Ciberdelincuencia (2001) y su Segundo Protocolo Adicional (2023) han establecido estándares avanzados para la cooperación entre Estados y la gestión forense de evidencia digital. De igual forma, las normas ISO/IEC 27037:2012, 27041:2015, 27042:2015 y 27043:2015 proporcionan directrices específicas para la identificación, recolección, análisis e interpretación de pruebas digitales, asegurando su confiabilidad y reproducibilidad en el proceso judicial (International Organization for Standardization, 2015a, 2015b, 2015c).

Frente a este panorama, el presente artículo tiene como propósito analizar la validez de la prueba digital en los procesos penales ecuatorianos, con especial énfasis en la regulación del COIP sobre la cadena de custodia y la pericia forense, a la luz de los estándares internacionales vigentes. A través de una revisión bibliográfica de fuentes legislativas, doctrinarias y jurisprudenciales, se busca identificar los

principales vacíos normativos, compararlos con modelos de países como España y Colombia, y proponer lineamientos que fortalezcan la gestión de evidencia digital en el sistema judicial del Ecuador.

1.1 Contextualización del problema

La expansión de la tecnología digital ha modificado la estructura de las relaciones sociales, económicas y jurídicas, introduciendo nuevos escenarios delictivos que desafían las formas tradicionales de investigación penal. Los delitos informáticos, definidos como aquellas conductas ilícitas que emplean sistemas o redes electrónicas para cometer infracciones, han crecido exponencialmente en América Latina y particularmente en Ecuador, donde la suplantación de identidad, el fraude electrónico y el acceso no autorizado a sistemas informáticos encabezan las denuncias ante la Fiscalía General del Estado (Sarmiento & Maldonado, 2024).

La evidencia digital se ha convertido en un elemento esencial para la persecución penal de estos delitos. Según Navas-Abad y Vázquez-Martínez (2025), la prueba digital constituye "todo rastro o información electrónica generada, transmitida o almacenada mediante dispositivos tecnológicos que sirve para demostrar hechos relevantes dentro del proceso penal". No obstante, su adecuada utilización depende de que se garantice la autenticidad, integridad y fiabilidad de los datos, lo que solo es posible mediante una correcta cadena de custodia y la intervención de peritos forenses especializados.

En el contexto ecuatoriano, el Código Orgánico Integral Penal (COIP) reconoce la validez de la prueba digital (arts. 456, 499 y 500), pero carece de un procedimiento uniforme para su obtención, conservación y análisis, lo que genera incertidumbre jurídica respecto a su valor probatorio (Asamblea Nacional del Ecuador, 2023). Estudios recientes advierten que la inexistencia de protocolos estandarizados facilita la impugnación de estas pruebas en juicio y limita su eficacia en casos de ciberdelitos (Porras, 2023; Banegas & Andrade, 2022).

En consecuencia, la comprensión de los fundamentos teóricos, técnicos y normativos de la prueba digital dentro del proceso penal ecuatoriano es clave para evaluar su validez probatoria. Este análisis permite no solo identificar las deficiencias del sistema judicial frente a los delitos informáticos, sino también proponer medidas que armonicen la práctica forense nacional con las exigencias internacionales de transparencia y trazabilidad de la evidencia.

2. MARCO TEÓRICO:

2.1 Delitos informáticos en el contexto ecuatoriano

El auge de las tecnologías digitales ha propiciado el surgimiento de nuevos tipos de criminalidad que vulneran derechos fundamentales y afectan tanto al sector público como al privado. En Ecuador, los delitos informáticos se han incrementado significativamente, convirtiéndose en una de las principales preocupaciones de las autoridades judiciales y policiales. De acuerdo con la Fiscalía General del Estado,

entre los años 2020 y 2023 se reportaron más de 15.000 denuncias relacionadas con ciberdelitos, siendo los más comunes la suplantación de identidad (43%), la falsificación de documentos electrónicos (29%) y la apropiación fraudulenta por medios digitales (20%) (Sarmiento & Maldonado, 2024).

El Código Orgánico Integral Penal (COIP), reformado en 2023, incorpora en su Título IV, Capítulo V, un conjunto de tipos penales destinados a sancionar las conductas ilícitas cometidas a través de medios informáticos. Entre ellos destacan el artículo 230 (acceso no consentido a sistemas informáticos), el artículo 231 (interceptación ilícita de datos) y el artículo 232 (falsificación y fraude electrónico). Estas disposiciones buscan proteger la integridad de la información y la privacidad de los usuarios frente al uso indebido de las tecnologías (Asamblea Nacional del Ecuador, 2023).

No obstante, diversos estudios han señalado que la tipificación penal de estos delitos aún presenta vacíos que dificultan la persecución efectiva de los infractores. Navas-Abad y Vázquez-Martínez (2025) sostienen que la falta de especialización técnica en las investigaciones y la ausencia de protocolos estandarizados para la gestión de evidencia digital obstaculizan la correcta aplicación del COIP en los casos de ciberdelincuencia. A ello se suma la insuficiente capacitación de fiscales y jueces en materia de análisis forense informático, lo cual genera inconsistencias en la valoración probatoria (Porras, 2023; Banegas & Andrade, 2022).

Por otro lado, la Organización de Estados Americanos (OEA), a través de su *Informe sobre Ciberseguridad en América Latina y el Caribe* (2022), advierte que Ecuador se encuentra entre los países de la región con mayores desafíos en materia de infraestructura digital y legislación penal especializada. Esto se debe, principalmente, a la falta de adhesión al Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), instrumento internacional que establece estándares comunes para la cooperación jurídica y la preservación de evidencia digital.

La rápida evolución tecnológica también ha modificado la naturaleza de los crímenes. Actualmente, los delitos informáticos no solo abarcan ataques a sistemas o redes, sino también delitos tradicionales con medios tecnológicos, como la corrupción, el lavado de activos, el acoso digital o la trata de personas en línea. Esta convergencia entre criminalidad tradicional y tecnológica exige un marco penal más dinámico y pericias especializadas capaces de garantizar la autenticidad de la evidencia en entornos digitales (López, 2023).

En consecuencia, el análisis de los delitos informáticos en Ecuador debe comprenderse no solo desde su configuración normativa, sino también desde la capacidad del sistema judicial para responder con eficiencia técnica y jurídica ante estas nuevas formas de criminalidad. La adecuada gestión de la prueba digital y la implementación de protocolos forenses compatibles con los estándares internacionales constituyen pilares esenciales para consolidar un modelo de justicia penal acorde con la era digital.

Tabla 1. Principales delitos informáticos tipificados en el COIP (2023)

Tipo penal (COIP)	Descripción legal	Sanción	Relevancia en la práctica judicial
Art. 230. Acceso no consentido a sistemas informáticos	Introducirse, sin autorización, en un sistema informático o telemático ajeno.	Pena privativa de libertad de uno a tres años.	Delito base más frecuente en denuncias por intrusión y hackeo.
Art. 231. Interceptación ilícita de datos	Interceptar transmisiones electrónicas o de datos sin consentimiento.	Uno a tres años de prisión.	Asociado a espionaje informático y filtración de correos.
Art. 232. Falsificación y fraude electrónico	Alterar datos, programas o sistemas con ánimo de lucro o perjuicio.	Tres a cinco años de prisión.	Relevante en fraudes bancarios y manipulación de documentos digitales.
Art. 233. Daño a sistemas informáticos	Dañar, alterar o destruir información digital o infraestructura tecnológica.	Uno a tres años de prisión.	Frecuente en sabotajes a empresas o entidades públicas.
Art. 234. Uso no autorizado de datos personales	Usar, divulgar o comercializar datos personales sin autorización.	Uno a tres años de prisión.	Vinculado a vulneraciones de privacidad y robo de identidad.

Fuente: Asamblea Nacional del Ecuador (2023).

En la Tabla 1 se puede identificar la clasificación de los principales delitos informáticos reconocidos por el Código Orgánico Integral Penal (COIP, 2023), los cuales reflejan la adaptación del ordenamiento jurídico ecuatoriano a las nuevas formas de criminalidad digital. Como se observa, la tipificación penal abarca conductas que van desde el acceso no autorizado a sistemas informáticos hasta el uso indebido de datos personales.

No obstante, la práctica judicial evidencia que, a pesar de la existencia de este marco legal, la persecución y sanción efectiva de estos delitos aún enfrenta limitaciones técnicas y probatorias. La ausencia de un protocolo uniforme para la obtención y manejo de evidencia digital, sumada a la escasa capacitación de los operadores de justicia, genera inconsistencias en la aplicación de estas normas (Navas-Abad & Vázquez-Martínez, 2025; Porras, 2023). Por ello, resulta indispensable fortalecer la gestión de la prueba digital y la capacitación forense especializada, garantizando la autenticidad y trazabilidad de los datos electrónicos presentados en juicio.

2.2 Concepto y validez jurídica de la prueba digital en el COIP

La prueba digital se ha consolidado como un elemento central en los procesos penales contemporáneos, especialmente ante el crecimiento de los delitos informáticos y la progresiva digitalización de la vida social. De acuerdo con Navas-Abad y Vázquez-Martínez (2025), la prueba

digital comprende “todo dato o información generada, transmitida, recibida o almacenada en formato electrónico, susceptible de ser utilizado para acreditar hechos relevantes dentro de un proceso judicial”. Esta definición abarca desde correos electrónicos y mensajes instantáneos hasta registros de navegación, bases de datos, videos y documentos electrónicos.

En Ecuador, el Código Orgánico Integral Penal (COIP) reconoce la validez de la prueba digital en su artículo 499, al establecer que todo contenido digital será admisible como prueba documental siempre que se ajuste a los procedimientos legales de autenticación y cadena de custodia (Asamblea Nacional del Ecuador, 2023). El artículo 500 precisa que se entiende por contenido digital toda representación informática que refleje hechos, datos o ideas de la realidad, susceptibles de ser procesados o transmitidos mediante tecnologías informáticas. De esta manera, la legislación ecuatoriana legitima la utilización de medios electrónicos en el ámbito probatorio, equiparándolos a la prueba documental tradicional.

Sin embargo, la validez de la prueba digital depende estrictamente del cumplimiento de tres principios fundamentales: autenticidad, integridad y fiabilidad. La autenticidad se refiere a la capacidad de demostrar que la evidencia proviene efectivamente de la fuente indicada y no ha sido manipulada. La integridad implica que los datos se mantienen completos y sin alteraciones desde su recolección hasta su presentación en juicio. Finalmente, la fiabilidad exige que la evidencia pueda ser verificada o reproducida por peritos independientes, garantizando el principio de contradicción procesal (López, 2023).

En la práctica judicial ecuatoriana, estos criterios se relacionan directamente con la cadena de custodia y con la pericia forense informática, ya que ambas aseguran la trazabilidad y legitimidad de la prueba. No obstante, la ausencia de protocolos técnicos detallados y de peritos debidamente certificados genera un riesgo latente de nulidad procesal. Porras (2023) advierte que la falta de una normativa específica sobre la gestión de evidencia digital permite que las defensas cuestionen la validez de la prueba por presuntas alteraciones o fallos en el procedimiento de preservación.

La doctrina internacional coincide en que la evidencia digital solo puede considerarse válida si se obtiene y analiza conforme a estándares técnicos universalmente aceptados. En este sentido, la ISO/IEC 27037:2012 establece las pautas para la identificación, recolección y preservación de evidencia digital, mientras que las normas ISO/IEC 27041:2015 y ISO/IEC 27042:2015 proporcionan directrices sobre la validación y análisis de la información obtenida (International Organization for Standardization, 2015a, 2015b, 2015c). Estas guías técnicas aseguran que los procedimientos sean reproducibles, verificables y compatibles con los principios del debido proceso.

Tabla 2. Requisitos de validez de la prueba digital según doctrina y normativa

Criterio	Definición	Fundamento normativo/doctrinario	Referencia
Autenticidad	Capacidad de demostrar que la prueba proviene de su fuente original y no ha sido alterada.	Art. 499 COIP; ISO/IEC 27037:2012.	López (2023); ISO (2015a).
Integridad	Garantía de que los datos no han sufrido modificaciones desde su obtención.	Art. 456 COIP; ISO/IEC 27043:2015.	Porras (2023); Navas-Abad & Vázquez-Martínez (2025).
Fiabilidad	Posibilidad de verificar y reproducir la prueba mediante procedimientos técnicos verificables.	ISO/IEC 27041:2015 y 27042:2015.	Banegas & Andrade (2022).
Pertinencia	Relación directa de la evidencia con el objeto del proceso penal.	Arts. 454 y 455 COIP.	Asamblea Nacional del Ecuador (2023).

En la Tabla 2 se analizan los criterios fundamentales que determinan la validez jurídica de la prueba digital en el proceso penal ecuatoriano. Estos principios autenticidad, integridad, fiabilidad y pertinencia constituyen los pilares sobre los cuales se sustenta la admisibilidad de toda evidencia electrónica.

Su correcta aplicación permite que los tribunales valoren la prueba digital con la misma solidez que las pruebas físicas o documentales tradicionales. Sin embargo, la falta de protocolos nacionales estandarizados y de herramientas forenses certificadas continúa siendo un desafío relevante. Tal como señalan Banegas y Andrade (2022), la verificación técnica debe complementarse con la observancia de los derechos procesales de las partes, asegurando que cada etapa de la recolección, análisis y presentación de la evidencia sea transparente, reproducible y conforme a estándares internacionales.

Asimismo, la jurisprudencia comparada ha reforzado el reconocimiento de la prueba digital como un medio legítimo y confiable. En el ámbito europeo, la Ley de Enjuiciamiento Criminal de España (art. 588 bis) reconoce expresamente la validez de las pruebas electrónicas obtenidas mediante interceptaciones legales, siempre que se respete el principio de proporcionalidad y los derechos fundamentales de las personas involucradas (Magro, 2020). De manera similar, en Colombia, el Código General del Proceso y la Ley 527 de 1999 legitiman los mensajes de datos y documentos electrónicos como medios probatorios equivalentes a los escritos tradicionales (Yepes, Cárdenas & Gómez, 2022).

En el caso ecuatoriano, la legislación aún presenta vacíos normativos respecto a la admisibilidad técnica y jurídica de las evidencias digitales, especialmente en relación con los delitos informáticos. Banegas y Andrade (2022) sostienen que la falta de armonización entre la práctica forense y las disposiciones del COIP limita la eficacia de las investigaciones. Por tanto, resulta imperativo que el sistema judicial ecuatoriano desarrolle protocolos específicos de actuación digital, en concordancia con los estándares ISO y con los principios del Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), para fortalecer la validez de la prueba digital dentro del proceso penal.

2.3 Cadena de custodia de la evidencia digital

La cadena de custodia constituye uno de los pilares fundamentales para garantizar la validez jurídica y la autenticidad probatoria de la evidencia digital dentro del proceso penal. Su finalidad es asegurar que los elementos de prueba recolectados mantengan su estado original desde el momento de la obtención hasta su presentación ante la autoridad judicial, evitando alteraciones, manipulaciones o pérdidas de información (López, 2023). En el contexto ecuatoriano, este principio adquiere especial relevancia frente al auge de los delitos informáticos, en los cuales los datos electrónicos se convierten en los principales indicios del hecho punible.

El Código Orgánico Integral Penal (COIP) regula la cadena de custodia en su artículo 456, definiéndola como el procedimiento que garantiza la identidad e integridad de los elementos materiales y evidencias —incluidas las digitales— durante todas las fases de la investigación penal (Asamblea Nacional del Ecuador, 2023). Este proceso comprende la recolección, preservación, transporte, almacenamiento, análisis y presentación de los indicios, bajo la supervisión del fiscal y con intervención de peritos especializados. Sin embargo, aunque el COIP contempla la evidencia digital dentro de este marco general, no establece un protocolo específico adaptado a las particularidades técnicas de los datos electrónicos, lo que genera vacíos prácticos en su aplicación (Navas-Abad & Vázquez-Martínez, 2025).

En términos técnicos, la cadena de custodia digital requiere procedimientos diferenciados respecto a la evidencia física, ya que los datos pueden ser modificados sin dejar rastros visibles. Por ello, es esencial utilizar herramientas forenses certificadas que permitan clonar la información original mediante copias bit a bit (bitstream images), garantizando la inmutabilidad y trazabilidad de los archivos (Banegas & Andrade, 2022). Asimismo, todo acceso o manipulación debe quedar registrado en un acta digital con metadatos verificables, donde consten la hora, fecha, persona responsable y motivo de cada intervención.

En la práctica judicial ecuatoriana, la falta de lineamientos técnicos estandarizados ha permitido que la cadena de custodia sea vulnerada en múltiples ocasiones, afectando la admisibilidad de la prueba. Porras (2023) advierte que, en algunos casos, las autoridades judiciales han admitido evidencias electrónicas sin documentación completa de su recorrido probatorio, lo cual abre la posibilidad de

impugnaciones por parte de la defensa. Este problema evidencia la necesidad de contar con protocolos uniformes y con capacitación especializada para fiscales, policías y peritos forenses.

A nivel internacional, las normas ISO/IEC 27037:2012 y ISO/IEC 27043:2015 establecen procedimientos precisos para la gestión de la cadena de custodia digital. La primera norma detalla las fases de identificación, recolección, adquisición y preservación de la evidencia, mientras que la segunda amplía el proceso al ciclo completo de investigación forense, promoviendo la documentación exhaustiva y la reproducibilidad de los resultados (International Organization for Standardization, 2015a, 2015c). Estas directrices técnicas aseguran que cualquier evidencia digital pueda ser auditada o replicada por terceros, fortaleciendo su credibilidad en los tribunales.

La validez de la cadena de custodia también se relaciona con el principio de debido proceso y el derecho de defensa. Magro (2020) señala que, en el derecho comparado europeo, la alteración o pérdida de trazabilidad en la evidencia digital puede implicar su exclusión del juicio oral, por considerarse violatoria de las garantías procesales. En este sentido, la cadena de custodia no solo cumple una función técnica, sino también constitucional, al proteger el equilibrio entre la búsqueda de la verdad procesal y los derechos fundamentales del acusado.

En el proceso de manejo de evidencia digital, cada fase cumple una función específica orientada a preservar la integridad y autenticidad de la información obtenida. Las etapas fundamentales son:

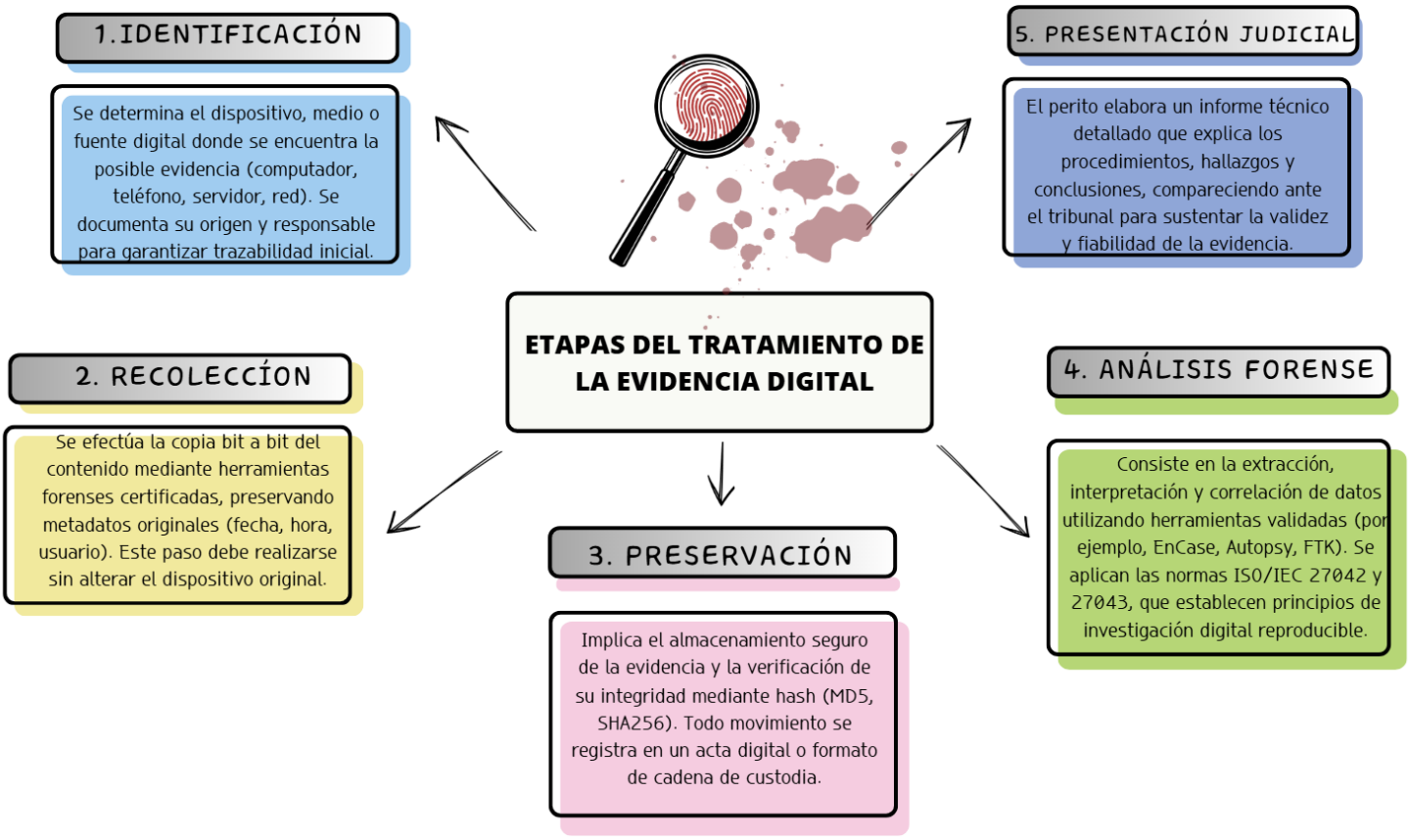

Figura 1. Etapas del tratamiento de la evidencia digital
Fuente: Elaboración propia con base en ISO/IEC 27037 y 27043 (2025).

Estas fases garantizan la integridad procesal de la evidencia digital y su admisibilidad judicial. Su correcta aplicación no solo preserva la trazabilidad técnica del material recolectado, sino que también fortalece la transparencia y credibilidad del sistema penal frente a los desafíos tecnológicos actuales.

En Ecuador, la implementación de una cadena de custodia digital estandarizada requiere armonizar la normativa penal con los estándares internacionales de investigación forense. Para ello, resulta indispensable desarrollar protocolos operativos nacionales basados en la ISO/IEC 27037 y el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), que garanticen la trazabilidad, integridad y autenticidad de las evidencias digitales en todos los niveles de la investigación penal. De igual modo, la creación de un registro nacional de peritos en informática forense con certificación técnica reconocida fortalecería la transparencia y legitimidad de los procesos judiciales vinculados a delitos informáticos.

En definitiva, la cadena de custodia de la evidencia digital no es solo un requisito formal, sino un mecanismo de garantía judicial que asegura la veracidad de la información, preserva los derechos de las partes y consolida la confianza en la justicia penal ecuatoriana ante los desafíos de la era digital.

2.4 Pericia forense informática en el proceso penal ecuatoriano

La pericia forense informática constituye un elemento determinante en la verificación de la autenticidad, integridad y trazabilidad de la evidencia digital dentro del proceso penal. Su función principal es examinar, recuperar y analizar información contenida en dispositivos electrónicos o sistemas informáticos con el fin de establecer hechos relevantes para la investigación judicial (Banegas & Andrade, 2022). En los casos de delitos informáticos, el informe pericial adquiere especial relevancia, pues constituye el medio idóneo para validar la prueba digital conforme a criterios científicos y técnicos reconocidos.

En el sistema penal ecuatoriano, la intervención del perito informático se encuentra regulada en el artículo 503 del Código Orgánico Integral Penal (COIP), que dispone que los peritos deben ser designados por la autoridad competente y actuar bajo los principios de objetividad, imparcialidad y competencia técnica (Asamblea Nacional del Ecuador, 2023). No obstante, el COIP no detalla procedimientos específicos para la pericia digital, lo que deja un margen discrecional en la metodología aplicada por los expertos y puede afectar la validez procesal de los resultados.

De acuerdo con Navas-Abad y Vázquez-Martínez (2025), la falta de estandarización en los métodos de análisis digital es una de las principales debilidades del sistema judicial ecuatoriano. Los autores señalan que en muchos casos los informes periciales carecen de documentación detallada sobre las herramientas utilizadas, los procedimientos de extracción o los algoritmos de validación de datos, lo

que dificulta la reproducibilidad del análisis y puede generar controversia sobre la autenticidad de los resultados.

En este contexto, la adopción de estándares internacionales resulta fundamental para asegurar la validez técnica y jurídica de la pericia forense. La norma ISO/IEC 27042:2015 establece directrices para el análisis e interpretación de evidencia digital, enfatizando la importancia de documentar cada fase del proceso de investigación, desde la identificación de la evidencia hasta su presentación en juicio (International Organization for Standardization, 2015b). Asimismo, la ISO/IEC 27043:2015 define un marco metodológico completo para la investigación digital forense, que incluye procedimientos de planificación, ejecución y control de calidad de los resultados (International Organization for Standardization, 2015c).

A nivel práctico, la pericia informática forense debe cumplir con tres etapas básicas:

- Adquisición de la evidencia, que consiste en obtener una copia exacta de los datos originales mediante técnicas de clonación o imágenes bit a bit, preservando los metadatos originales;
- Análisis técnico, que implica el uso de herramientas especializadas (por ejemplo, EnCase, Autopsy o FTK) para examinar registros, archivos eliminados y trazas digitales; y
- Elaboración del informe pericial, donde se describen los hallazgos, las herramientas utilizadas, la metodología empleada y las conclusiones técnicas, en lenguaje comprensible para el juez y las partes (López, 2023).

La formación y certificación de los peritos forenses es otro aspecto crítico. En Ecuador, no existe un registro nacional unificado de peritos informáticos con acreditación técnica, lo que genera disparidad en la calidad de los informes periciales y en la valoración judicial de la prueba digital. Porras (2023) sostiene que la falta de especialización y la limitada capacitación de los operadores judiciales (jueces, fiscales y peritos) constituye una barrera estructural para la correcta aplicación de la prueba digital en el proceso penal.

En países como España y Colombia, se han implementado modelos de certificación profesional y protocolos judiciales de actuación pericial que garantizan la fiabilidad de las investigaciones. Por ejemplo, en el sistema español, los peritos deben acreditar competencia técnica y cumplir con los estándares ISO e ILAC (International Laboratory Accreditation Cooperation), garantizando la validez de las pruebas en juicio (Magro, 2020). De manera similar, el Código General del Proceso colombiano y la Ley 527 de 1999 establecen la obligatoriedad de que los peritos utilicen procedimientos verificables y herramientas reconocidas por la comunidad científica (Yepes, Cárdenas & Gómez, 2022).

En este sentido, se propone que Ecuador avance hacia la creación de un Instituto Nacional de Pericia Digital y Forense, encargado de acreditar, formar y supervisar a los peritos informáticos en el

ámbito penal. Este organismo debería basarse en los principios del Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001) y las normas ISO/IEC 27000, garantizando la homologación técnica y la transparencia procesal.

La consolidación de una pericia informática forense tecnológicamente actualizada y jurídicamente sólida representa un paso esencial para fortalecer la lucha contra los delitos informáticos en Ecuador. Solo a través de una adecuada articulación entre derecho y tecnología, el sistema judicial podrá asegurar que las pruebas digitales sean válidas, reproducibles y respetuosas del debido proceso.

3. METODOLOGÍA O MATERIALES Y METODOS

3.1. Enfoque de la investigación

Esta investigación adopta un enfoque cualitativo de tipo descriptivo y analítico, orientado a examinar la regulación, aplicación y validez de la prueba digital en los procesos penales ecuatorianos, conforme al Código Orgánico Integral Penal (COIP) y los estándares internacionales sobre evidencia digital.

El diseño de la revisión bibliográfica se fundamenta en la recopilación y análisis de fuentes legislativas, doctrinarias y jurisprudenciales que abordan la relación entre los delitos informáticos, la cadena de custodia y la pericia forense informática.

Según Hernández-Sampieri, Fernández-Collado y Baptista (2022), el enfoque cualitativo permite explorar fenómenos complejos en su contexto jurídico y social, interpretando significados y relaciones entre categorías normativas y técnicas. De igual modo, la revisión descriptiva y analítica posibilita identificar tendencias, vacíos normativos y convergencias doctrinarias (Ochoa & Yunkor, 2021).

3.2. Unidades de análisis

Las unidades de análisis estuvieron conformadas por documentos jurídicos, doctrinarios y técnicos relacionados con el tratamiento de la prueba digital y los delitos informáticos.

Se analizaron fuentes primarias —como el Código Orgánico Integral Penal (COIP), la Constitución de la República del Ecuador (2008) y el Convenio de Budapest sobre la Ciberdelincuencia (2001)— y fuentes secundarias, entre ellas artículos científicos, informes forenses y tesis publicadas entre 2018 y 2025 en bases de datos académicas como Scielo, Redalyc, Dialnet y Scopus.

El criterio de selección consideró la relevancia temática, la actualidad de las publicaciones y la pertinencia jurídica y técnica para el contexto ecuatoriano.

3.3. Técnicas de recolección

Para la obtención de la información se aplicó una revisión bibliográfica documental exhaustiva, estructurada en cuatro fases:

1. Identificación de fuentes en bases de datos científicas, bibliotecas universitarias y organismos internacionales como la OEA, el Consejo de Europa. Asimismo, se consultaron documentos legislativos fundamentales como el Código Orgánico Integral Penal (COIP) y el Código Orgánico General de Procesos (COGEP), con el propósito de contextualizar la normativa ecuatoriana.
2. Selección de materiales relevantes, priorizando publicaciones con enfoque en derecho penal, ciberseguridad y criminalística forense.
3. Evaluación de calidad y pertinencia mediante criterios de actualidad (últimos 7 años), respaldo institucional y revisión por pares.
4. Sistematización temática mediante fichas de análisis que integraron información sobre los ejes: delitos informáticos, validez probatoria, cadena de custodia y pericia digital.

Asimismo, se efectuó un metaanálisis cualitativo que permitió sintetizar hallazgos recurrentes sobre la eficacia de los procedimientos forenses digitales en Ecuador y en modelos comparados como España y Colombia.

3.4. Procesamiento y análisis de la información

El análisis se desarrolló bajo un método descriptivo-analítico, que permitió desglosar la información normativa y doctrinaria en categorías conceptuales específicas: marco legal ecuatoriano, validez probatoria, cadena de custodia digital y pericia forense informática. Siguiendo a Herszenbaun (2022), el análisis cualitativo busca descomponer los componentes del fenómeno jurídico para establecer relaciones entre teoría, norma y práctica judicial.

Esta metodología garantizó un abordaje sistemático y riguroso, permitiendo extraer conclusiones basadas en evidencia documental verificable y actualizada.

Tabla 3. Esquema metodológico de la investigación

Componente	Descripción
Enfoque de la investigación	Investigación cualitativa, descriptiva y analítica, orientada a examinar la validez jurídica y técnica de la prueba digital en el contexto penal ecuatoriano.
Unidades de análisis	Documentos legales (COIP, Constitución, Convenio de Budapest), artículos científicos, tesis y estándares internacionales (ISO/IEC 27000). Selección de publicaciones entre 2018 y 2025.
Técnicas de recolección	Revisión bibliográfica y documental en bases de datos (Scielo, Dialnet, Redalyc, Scopus). Inclusión de literatura jurídica, doctrinaria y técnica sobre delitos informáticos, cadena de custodia y pericia digital.
Procesamiento y análisis	Análisis descriptivo-analítico y metaanálisis cualitativo. Aplicación del método 5W + 1H para la organización de categorías y comparación entre normativa ecuatoriana e internacional.

Fuente: Elaboración propia a partir de Hernández-Sampieri et al. (2022) y Herszenbaun (2022).

4. RESULTADOS Y DISCUSIÓN

El análisis documental permitió identificar un conjunto de hallazgos relevantes sobre el estado actual del tratamiento jurídico y técnico de la prueba digital en Ecuador, así como las principales debilidades estructurales del sistema penal frente a los delitos informáticos. Los resultados se organizaron en torno a cuatro ejes: marco normativo, validez de la prueba digital, cadena de custodia y pericia forense informática, comparados con los estándares internacionales ISO y el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001).

4.1. Marco normativo y tipificación penal

El COIP (Asamblea Nacional del Ecuador, 2023) contempla un grupo de disposiciones específicas para los delitos informáticos (arts. 230 al 234), lo que demuestra un reconocimiento legislativo del fenómeno digital. Sin embargo, la revisión de fuentes doctrinarias (Navas-Abad & Vázquez-Martínez, 2025; Porras, 2023) evidencia que estas normas carecen de procedimientos claros sobre la gestión probatoria digital, particularmente en la identificación, recolección y análisis de la evidencia. En la Tabla 1 se observó que, si bien los tipos penales cubren una variedad de conductas como el acceso ilícito, la interceptación y la falsificación electrónica, la legislación ecuatoriana aún no desarrolla mecanismos de cooperación internacional ni protocolos judiciales específicos para el manejo de evidencia digital transfronteriza, a diferencia de lo previsto en el Convenio de Budapest.

4.2. Validez jurídica de la prueba digital

En relación con la validez de la prueba digital, el estudio reveló que el COIP equipara los medios electrónicos a los documentales, reconociendo su legitimidad procesal en los artículos 499 y 500. No obstante, la admisibilidad efectiva de esta evidencia depende de la autenticidad, integridad y fiabilidad de los datos, principios que se resumen en la Tabla 2.

Los análisis doctrinarios de López (2023) y Banegas & Andrade (2022) coinciden en que la ausencia de protocolos forenses uniformes y la falta de peritos certificados generan vacíos procesales que permiten a las partes cuestionar la credibilidad de la prueba digital. Además, en comparación con otros países de la región como Colombia o España, Ecuador aún no cuenta con una guía judicial que regule los estándares mínimos de admisión y valoración técnica de la evidencia digital (Magro, 2020; Yepes, Cárdenas & Gómez, 2022).

En síntesis, la normativa ecuatoriana reconoce la validez formal de la prueba digital, pero no establece criterios técnicos obligatorios que garanticen su autenticidad bajo parámetros internacionales.

4.3. Cadena de custodia digital

La revisión de estudios forenses (Banegas & Andrade, 2022; Porras, 2023) demostró que la cadena de custodia digital continúa siendo uno de los eslabones más débiles en el proceso penal

ecuatoriano. Aunque el artículo 456 del COIP regula la cadena de custodia general, no existe un protocolo específico para evidencias electrónicas. Esto provoca inconsistencias en la preservación de la prueba, vulneración de la trazabilidad y, en algunos casos, la exclusión de la evidencia en juicio. A nivel internacional, las normas ISO/IEC 27037:2012 y ISO/IEC 27043:2015 establecen que toda evidencia digital debe conservarse mediante copias bit a bit y documentarse con metadatos verificables (fecha, hora, usuario, dispositivo, herramienta utilizada). Ninguno de estos elementos es aún de cumplimiento obligatorio en Ecuador, lo que evidencia una brecha técnica significativa frente a los estándares internacionales.

Los resultados sugieren que la adopción de un protocolo nacional de cadena de custodia digital, basado en las ISO/IEC 27000, permitiría garantizar la autenticidad y trazabilidad de los datos desde su obtención hasta su presentación judicial.

4.4. Pericia forense informática

El análisis de fuentes técnicas y jurídicas reveló que la figura del perito informático forense carece de regulación unificada en Ecuador. Si bien el artículo 503 del COIP menciona la designación de peritos, no se exige certificación técnica en estándares internacionales ni acreditación ante un organismo nacional. Según Navas-Abad y Vázquez-Martínez (2025), muchos informes periciales carecen de registro metodológico, lo cual compromete su reproducibilidad y validez judicial. Esto contrasta con la práctica de países como España y Colombia, donde los peritos deben cumplir con acreditaciones ISO/IEC y guías judiciales oficiales (Magro, 2020; Yepes et al., 2022).

Los resultados de la revisión sugieren la necesidad urgente de crear un Instituto Nacional de Pericia Digital y Forense, que regule la acreditación, formación y evaluación continua de los peritos informáticos, en coordinación con el Consejo de la Judicatura y la Fiscalía General del Estado.

5. DISCUSIÓN

Los resultados obtenidos a partir de la revisión bibliográfica permiten evidenciar que el marco jurídico ecuatoriano en materia de prueba digital ha avanzado en su reconocimiento normativo, pero continúa enfrentando deficiencias estructurales en cuanto a su regulación técnica, aplicación forense y validación procesal. Si bien el Código Orgánico Integral Penal (COIP) reconoce expresamente la admisibilidad de la evidencia electrónica (arts. 456, 499 y 500), su efectividad depende del cumplimiento de requisitos técnicos que no se encuentran debidamente estandarizados en el país (Asamblea Nacional del Ecuador, 2023).

De acuerdo con Navas-Abad y Vázquez-Martínez (2025), la principal problemática radica en la fragmentación entre el marco normativo y las prácticas judiciales, pues no existen protocolos nacionales que regulen la obtención, conservación y análisis de evidencia digital. Este vacío normativo genera

incertidumbre sobre la autenticidad de la prueba, lo que puede derivar en su exclusión del proceso penal. Dicho hallazgo coincide con lo planteado por Porras (2023), quien advierte que muchos casos de delitos informáticos son archivados por deficiencias técnicas en la recolección o preservación de los datos digitales.

En este contexto, la cadena de custodia emerge como un punto crítico dentro del proceso judicial ecuatoriano. A pesar de su reconocimiento en el artículo 456 del COIP, la normativa actual no diferencia entre evidencia física y digital, ignorando las particularidades técnicas que exigen los datos electrónicos. En contraste, las normas internacionales ISO/IEC 27037:2012 y ISO/IEC 27043:2015 establecen procedimientos rigurosos de identificación, adquisición y preservación que garantizan la integridad y trazabilidad de la evidencia (International Organization for Standardization, 2015a, 2015c). La comparación evidencia que el sistema ecuatoriano carece de un marco metodológico homologado con los estándares internacionales, lo que limita su confiabilidad en instancias judiciales.

La pericia forense informática, por su parte, se configura como una herramienta esencial para la verificación técnica de la evidencia digital. Sin embargo, la revisión muestra que Ecuador carece de un sistema de acreditación o certificación de peritos, situación que repercute directamente en la calidad y reproducibilidad de los informes forenses. Banegas y Andrade (2022) destacan que la falta de uniformidad metodológica y de control de calidad en las pericias informáticas debilita el valor probatorio de los dictámenes técnicos. En contraposición, países como España y Colombia han avanzado en la institucionalización de la figura del perito digital mediante la adopción de estándares ISO y la creación de cuerpos técnicos especializados (Magro, 2020; Yepes, Cárdenas & Gómez, 2022).

Además, el estudio revela que Ecuador aún no se ha adherido al Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), instrumento que proporciona el marco jurídico más completo para la cooperación internacional en la persecución de delitos digitales y el intercambio de evidencia electrónica. Esta falta de adhesión representa un obstáculo significativo para la gestión transnacional de pruebas digitales, especialmente considerando que gran parte de los ciberdelitos trasciende las fronteras nacionales (Organización de Estados Americanos, 2022).

Por otro lado, el análisis doctrinario sugiere que la formación de los operadores judiciales —fiscales, jueces y peritos— sigue siendo limitada en materia de tecnologías de la información. Tal como afirman López (2023) y Porras (2023), la comprensión insuficiente de los procesos técnicos y la falta de recursos tecnológicos en los laboratorios forenses generan interpretaciones restrictivas sobre la admisibilidad de la prueba digital. Este déficit formativo acentúa la dependencia de criterios subjetivos, reduciendo la objetividad y transparencia en la valoración probatoria.

Finalmente, el estudio pone de manifiesto que la eficacia de la prueba digital no depende únicamente de la existencia de normas legales, sino de su correcta articulación con la práctica forense y

tecnológica. Para garantizar la seguridad jurídica y la confianza en el sistema penal ecuatoriano, resulta urgente integrar las normas ISO/IEC 27000, desarrollar un protocolo nacional de cadena de custodia digital y establecer un registro oficial de peritos informáticos forenses bajo estándares internacionales. Estas medidas fortalecerían la validez de la prueba electrónica, permitirían su interoperabilidad con otros sistemas judiciales y consolidarían un modelo de justicia penal acorde con la era digital.

6. CONCLUSIONES

El presente estudio permitió realizar un análisis integral sobre la validez jurídica de la prueba digital, la cadena de custodia y la pericia forense informática en el contexto penal ecuatoriano. Los hallazgos obtenidos demuestran que, si bien el Código Orgánico Integral Penal (COIP) ha incorporado el reconocimiento formal de la evidencia digital, su aplicación práctica enfrenta limitaciones significativas derivadas de la falta de estandarización técnica y de capacitación especializada entre los operadores judiciales.

En primer lugar, la validez jurídica de la prueba digital en Ecuador se encuentra supeditada al cumplimiento de los principios de autenticidad, integridad y fiabilidad. No obstante, la ausencia de una normativa secundaria o protocolos técnicos de actuación provoca ambigüedades en su admisión y valoración judicial. A diferencia de otros países latinoamericanos que han armonizado su legislación con los estándares internacionales, Ecuador mantiene un marco legal incompleto, lo que dificulta la gestión eficiente de la evidencia electrónica (Porras, 2023; Navas-Abad & Vázquez-Martínez, 2025).

En segundo lugar, la cadena de custodia digital constituye uno de los eslabones más débiles del proceso penal ecuatoriano. El artículo 456 del COIP regula de forma general este procedimiento, pero no distingue entre evidencia física y digital, omitiendo aspectos esenciales como la preservación de metadatos, la creación de copias bit a bit o la documentación digital certificada. Este vacío técnico compromete la trazabilidad y confiabilidad de la evidencia digital presentada en juicio (Banegas & Andrade, 2022).

En tercer lugar, la pericia forense informática carece de regulación unificada y de mecanismos de acreditación técnica. La inexistencia de un registro nacional de peritos especializados y la falta de certificaciones en estándares internacionales limitan la reproducibilidad y objetividad de los dictámenes técnicos, debilitando la fuerza probatoria de la evidencia (López, 2023; Magro, 2020).

Finalmente, la no adhesión de Ecuador al Convenio de Budapest sobre la Ciberdelincuencia (2001) constituye un obstáculo para la cooperación internacional y el intercambio de pruebas electrónicas en investigaciones transfronterizas. La falta de integración a este instrumento limita la capacidad del Estado para responder a los desafíos globales de la criminalidad digital y reduce la eficacia del sistema penal frente a los ciberdelitos (Consejo de Europa, 2001; Organización de Estados Americanos, 2022).

En síntesis, el Ecuador cuenta con una base normativa relevante, pero aún insuficiente. Es necesario evolucionar hacia un modelo integral de justicia penal digital, en el que el derecho, la tecnología y la ciencia forense se articulen de forma coherente y efectiva.

Recomendaciones

1. **Capacitación continua para operadores de justicia:** Implementar programas permanentes de capacitación sobre ciberdelincuencia, evidencia digital y análisis forense, dirigidos a Jueces, Fiscales y Defensores Públicos, asegurando una interpretación uniforme y técnicamente fundamentada de las normas penales.
2. **Adhesión del Ecuador al Convenio de Budapest sobre la Ciberdelincuencia:** Promover la ratificación del Convenio de Budapest (Consejo de Europa, 2001) y su Segundo Protocolo Adicional (2023), con el fin de fortalecer la cooperación judicial internacional y mejorar los mecanismos de obtención y transferencia de evidencia digital transfronteriza.
3. **Modernización tecnológica del sistema judicial:** Invertir en infraestructura digital, laboratorios forenses y herramientas de software certificadas (como FTK, EnCase o Autopsy), que permitan realizar pericias de alto nivel técnico con estándares de calidad verificables.
4. **Creación de una base de datos nacional de ciberdelitos y evidencia digital:** Diseñar un sistema interinstitucional que registre y sistematice casos de delitos informáticos, tipos de evidencia digital, resultados periciales y sentencias, generando indicadores útiles para la política criminal y la prevención tecnológica.

Estas acciones permitirían fortalecer la confianza en la prueba digital, garantizar la seguridad jurídica y consolidar un sistema de justicia penal transparente, técnico y adaptado a los desafíos de la era digital. La adopción de estándares internacionales y la profesionalización de los actores del sistema judicial son pasos indispensables para que Ecuador logre una gestión forense moderna, eficiente y conforme a los derechos fundamentales.

FINANCIACIÓN

No tuvo financiamiento

CONFLICTO DE INTERESES

No hubo conflicto de intereses con la investigación.

CONTRIBUCIÓN DE AUTORÍA

En concordancia con la taxonomía establecida internacionalmente para la asignación de créditos a autores de artículos científicos (https://credit.niso.org/). Los autores declaran sus contribuciones en la siguiente matriz:

Participar activamente en:	*Autor 1.*	*Autor 2*	*Autor 3*
Conceptualización	X	X	X
Análisis formal	X		X
Adquisición de fondos		X	
Investigación	X		
Metodología	X	X	X
Administración del proyecto		X	X
Recursos	X		
Redacción –borrador original	X	X	X
Redacción –revisión y edición		X	
La discusión de los resultados	**X**	**X**	**X**
Revisión y aprobación de la versión final del trabajo.	**X**	**X**	**X**

REFERENCIAS BIBLIOGRÁFICAS

Araujo, F. (2010). *La prueba y su incorporación al proceso en el juicio penal*. Universidad de Cuenca. http://dspace.ucuenca.edu.ec/bitstream/123456789/2933/1/td4311.pdf

Asamblea Nacional del Ecuador. (2015). *Código Orgánico General de Procesos*. Registro Oficial Suplemento 506, 22 de mayo de 2015. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Orgánico-General-de-Procesos.pdf

Asamblea Nacional del Ecuador. (2023). *Código Orgánico Integral Penal (COIP)*. Registro Oficial Suplemento 180, 10 de febrero de 2014 (actualización 2023). https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

Banegas, D., & Andrade, D. (2022). *Análisis forense en dispositivos móviles Android para casos de ciberextorsión: revisión sistemática de literatura*. *MQR Investigar*, 8(3), 4076–4097. https://doi.org/10.56048/mqr20225.8.3.2024.4076-4097

Bielli, G. (2019). *Prueba electrónica: incorporación, admisión y valoración de capturas de pantalla en el proceso de familia*. Pensamiento Civil.

Borges, R. (2018). *La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea*. *Iuris Tantum*, (25), 536–549. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100018

Bujosa, L., & Toro, M. B. (2021). *La prueba digital producto de la vigilancia secreta: implicaciones procesales en el derecho penal*. *Revista de Derecho Procesal Penal*, (7), 112–129.

Consejo de Europa. (2001). *Convenio de Budapest sobre la Ciberdelincuencia*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista, P. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill.

Herszenbaun, G. (2022). *Método analítico aplicado a las ciencias sociales y jurídicas*. Editorial Tirant lo Blanch.

International Organization for Standardization (ISO). (2015a). *ISO/IEC 27037: Guidelines for identification, collection and/or acquisition of digital evidence*. ISO.

International Organization for Standardization (ISO). (2015b). *ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence*. ISO.

International Organization for Standardization (ISO). (2015c). *ISO/IEC 27043: Incident investigation principles and processes*. ISO.

López, J. A. (2023). *Evidencia digital y su admisibilidad en los procesos penales latinoamericanos*. *Revista Iberoamericana de Derecho Penal y Procesal*, 10(2), 55–74.

Magro, V. M. (2020). *La prueba digital en el proceso penal español: avances y desafíos tecnológicos*. *Revista Española de Derecho Procesal*, (1), 45–67.

Navas-Abad, C. E., & Vázquez-Martínez, D. S. (2025). *La importancia de la prueba digital en los procedimientos penales en Ecuador*. *Polo del Conocimiento*, 10(1), 1742–1775. https://doi.org/10.23857/pc.v10i1.8778

Organización de Estados Americanos. (2022). *Ciberdelito en América Latina y el Caribe: diagnóstico regional 2022*. Secretaría de Seguridad Multidimensional, OEA.

Porras, M. A. (2023). *La cadena de custodia digital en el proceso penal ecuatoriano*. *Revista Ecuatoriana de Ciencias Jurídicas*, 12(3), 87–105.

Yepes, J., Cárdenas, S., & Gómez, D. (2022). *La evidencia digital en los procesos judiciales colombianos: un análisis forense comparado*. *Revista Colombiana de Derecho Procesal*, 29(2), 145–169.