REINCISOL
ISSN 2953 - 6421

La Prueba Digital en el Proceso Penal Ecuatoriano: Análisis Normativo, Probatorio y Jurisprudencial

Digital Evidence In The Ecuadorian Criminal Process: A Normative, Evidentiary And Jurisprudential Analysis

Para citar este trabajo:
Llugsha, O., Arcos, M., Freire, E., y Castillo, L., (2025). La Prueba Digital en el Proceso Penal Ecuatoriano: Análisis Normativo, Probatorio y Jurisprudencial. *Reincisol*, 4(8), pp. 1251. https://doi.org/10.59282/reincisol.V4(8)1251

Autores:

Olivia Alexandra Llugsha Chicaiza
Universidad Bolivariana del Ecuador
Ciudad: Quito, País: Ecuador
Correo Institucional: oallugshac@ube.edu.ec
Orcid https://orcid.org/0009-0007-3539-9719

Milton Fernando Arcos Pineda
Universidad Bolivariana del Ecuador
Ciudad: Quito, País: Ecuador
Correo Institucional: mfarcosp@ube.edu.ec
Orcid https://orcid.org/ 0009-0006-0169-531X

Edward Fabricio Freire Gaibor
Universidad Bolivariana del Ecuador
Ciudad: Durán, País: Ecuador
Correo Institucional: effreireg@ube.edu.ec
Orcid https://orcid.org/009-0009-2913-8445

Luz Marina Castillo López
Universidad Bolivariana del Ecuador
Ciudad: Quito, País: Ecuador
Correo Institucional: lmcastillol@ube.edu.ec
Orcid https://orcid.org/0009-0008-0588-4251

RECIBIDO: 15 noviembre 2025 **ACEPTADO**: 26 diciembre 2025 **PUBLICADO:** 31 diciembre 2025

RESUMEN

La era digital ha transformado radicalmente la naturaleza de la evidencia en los sistemas de justicia penal, con la prueba digital presente en aproximadamente el 90% de los casos criminales contemporáneos. Sin embargo, Ecuador enfrenta una paradoja crítica: a pesar del reconocimiento normativo de la prueba digital en el Código Orgánico Integral Penal y el Código Orgánico General de Procesos, su eficacia probatoria permanece significativamente comprometida por deficiencias sistémicas. Esta investigación analizo integralmente las causas y efectos de esta ineficacia mediante un estudio mixto que combina análisis normativo, jurisprudencial y doctrinal. La metodología incluyó el examen de 18 normas fundamentales, 32 sentencias emblemáticas y 35 obras especializadas, además de entrevistas con 18 operadores de justicia. Los resultados revelan tres áreas críticas de deficiencia: insuficiencia normativa caracterizada por la ausencia de protocolos técnicos específicos y criterios homogéneos de valoración; deficiencias procedimentales manifestadas en protocolos inadecuados de cadena de custodia digital y escasa capacitación especializada; y restricciones jurisprudenciales evidenciadas en criterios interpretativos dispares entre instancias judiciales. El análisis jurisprudencial demostró que el 60% de investigaciones que involucran evidencia digital enfrentan problemas de admisibilidad. Esta situación genera impactos severos en la administración de justicia, incluyendo inadmisibilidad probatoria, prolongación procesal e inequidad, contribuyendo a tasas de impunidad del 90% en 2023. Se propone un modelo integral de reforma que abarca modificaciones normativas específicas, protocolos técnico-jurídicos estandarizados conforme a estándares internacionales ISO 27037, programas de capacitación especializada y fortalecimiento de infraestructura tecnológica para optimizar la eficacia probatoria digital.

Palabras clave: prueba digital, proceso penal ecuatoriano, eficacia probatoria, cadena de custodia digital, admisibilidad, reforma procesal

.

ABSTRACT

The digital era has radically transformed the nature of evidence in criminal justice systems, with digital evidence present in approximately 90% of contemporary criminal cases. However, Ecuador faces a critical paradox: despite the normative recognition of digital evidence in the Comprehensive Criminal Code and the General Code of Procedure, its evidentiary effectiveness remains significantly compromised by systemic deficiencies. This research comprehensively analyzes the causes and effects of this ineffectiveness through a mixed study combining normative, jurisprudential, and doctrinal analysis. The methodology included examination of 18 fundamental norms, 32 landmark judgments, and 35 specialized works, in addition to interviews with 18 justice operators. The results reveal three critical areas of deficiency: normative insufficiency characterized by the absence of specific technical protocols and homogeneous evaluation criteria; procedural deficiencies manifested in inadequate digital chain of custody protocols and scarce specialized training; and jurisprudential restrictions evidenced in disparate interpretative criteria among judicial instances. Jurisprudential analysis demonstrates that 60% of investigations involving digital evidence face admissibility problems. This situation generates severe impacts on justice administration, including evidentiary inadmissibility, procedural prolongation, and inequity, contributing to impunity rates of 90% in 2023. A comprehensive reform model is proposed encompassing specific normative modifications, standardized technical-legal protocols according to international ISO 27037 standards, specialized training programs, and strengthening of technological infrastructure to optimize digital evidentiary effectiveness.

Keywords: digital evidence, Ecuadorian criminal procedure, evidentiary effectiveness, digital chain of custody, admissibility, procedural reform

.

INTRODUCCIÓN

La era digital ha transformado fundamentalmente la naturaleza de la evidencia en los sistemas de justicia penal a nivel global. Actualmente, la evidencia digital está presente en aproximadamente el 90% de los casos criminales, abarcando desde homicidios y robos hasta delitos sexuales y corrupción (Evidence Management Institute, 2024). El FBI reportó en 2024 un total de 14 millones de delitos procesados por más de 16,000 agencias, donde la evidencia digital incluye registros telefónicos, videos de seguridad, mensajes de texto y datos de ubicación en la mayoría de investigaciones (FBI, 2024). Sin embargo, existe un atraso crítico de más de 4 millones de casos en tribunales, con miles desestimados por problemas en el manejo de evidencia digital (NiCE Public Safety & Justice, 2024).

Los sistemas judiciales mundiales enfrentan desafíos estructurales que comprometen la eficacia probatoria digital en toda clase de delitos. Una encuesta a 50 fiscales estadounidenses reveló que se autoevaluaron con puntuaciones de 3-4 en competencia para manejar evidencia digital, mientras investigadores los calificaron con solo 2-3, evidenciando disparidades del 25-50% (Richardson et al., 2023). El 65% de fiscales reportó incrementos significativos en atrasos, con 10% manejando más de 1,000 casos pendientes, independientemente del tipo de delito (NiCE Public Safety & Justice, 2024). Los departamentos policiales reportan demoras de 1-4 años en análisis forense digital, con 90% de evidencia digital generada en los últimos dos años superando capacidades procesales (ADF Solutions, 2024).

La cadena de custodia digital es significativamente más compleja y volátil que la evidencia física tradicional, afectando desde casos de homicidio con análisis de teléfonos hasta investigaciones de corrupción con sistemas informáticos (Richardson et al., 2023). Los problemas de admisibilidad constituyen preocupación global: en State of Connecticut v. Eleck, mensajes de Facebook en violencia doméstica fueron rechazados por falta de autenticación; en United States v. Vayner, perfiles sociales en fraude fueron inadmitidos por no probar autoría (PageFreezer, 2024). El NIJ encontró que procesar un millón de archivos requiere 39 horas, superando capacidades agenciales (NIJ, 2023).

Los sistemas latinoamericanos intensifican estos desafíos independientemente del tipo delictivo. La región presenta brechas tecnológicas significativas y sistemas educativos con altas tasas de deserción que afectan la formación de operadores capaces de manejar evidencia digital (Arias Ortiz et al., 2024). La heterogeneidad normativa genera inconsistencias: mientras algunos países desarrollaron marcos específicos para investigación forense digital aplicable a todos los delitos, otros mantienen legislaciones fragmentarias (Vadell et al., 2021).

Ecuador representa un caso paradigmático de tensiones entre disponibilidad de evidencia digital y eficacia probatoria. A pesar de que el COIP y COGEP reconocen la validez de prueba digital para cualquier delito, existen deficiencias sistémicas limitando su eficacia práctica (Navas Abad, 2025). El país experimentó incremento dramático en criminalidad: homicidios aumentaron 429% entre 2019-2024, registrando 3,036 en primer semestre de 2024, alcanzando 44.5 por 100,000 habitantes (Human Rights Watch, 2025). Cada caso potencialmente genera evidencia digital determinante.

Los análisis jurisprudenciales revelan que 60% de investigaciones penales que involucran evidencia digital enfrentan problemas de admisibilidad por falencias en cadena de custodia y autenticación técnica (Fuentes Tenorio, 2025). La extorsión, generando grabaciones telefónicas y mensajes, se duplicó entre enero-junio 2023, alcanzando 4,600 denuncias, incrementándose a 10,700 hasta septiembre 2024 (Human Rights Watch, 2024-2025). Los secuestros, produciendo evidencia de comunicaciones y ubicación, aumentaron 2,512% entre enero-febrero 2024 (CSIS, 2024).

La problemática se agudiza con 90% de impunidad en 2023, reflejando deficiencias sistémicas en procesamiento evidencial que afectan desde delitos menores hasta crímenes complejos (USCRI, 2025). El costo económico aumentó 76% entre 2018-2023, alcanzando 19.7 mil millones USD, con impacto per cápita de 1,595 USD en 2023 (Statista, 2024).

El COIP establece reconocimiento genérico de prueba digital para cualquier delito, mientras el COGEP regula aspectos procedimentales generales. Sin embargo, la ausencia de regulación específica sobre protocolos genera vacíos normativos afectando eficacia probatoria independientemente del tipo delictivo (Navas Abad, 2025). Esta deficiencia impacta uniformemente investigaciones de homicidios con dispositivos móviles, corrupción con sistemas informáticos, delitos sexuales con evidencia fotográfica digital, y robos con videos de seguridad.

La Fiscalía carece de protocolos estandarizados aplicables a evidencia digital, limitando capacidad operativa por recursos insuficientes y ausencia de estándares ISO 27037:2012. Los operadores carecen de formación sistemática para manejar evidencia digital independientemente del delito investigado. La infraestructura presenta limitaciones transversales: ausencia de laboratorios certificados y herramientas especializadas comprometen integridad y autenticidad sin distinción del delito investigado.

Delitos tradicionales como homicidio, robo, violencia sexual, extorsión, corrupción y tráfico de drogas frecuentemente producen evidencia digital determinante, pero su utilización eficaz se compromete por deficiencias sistémicas que afectan uniformemente el tratamiento probatorio independientemente del tipo delictivo investigado.

¿Cuáles son las causas estructurales y operativas que determinan la ineficacia de la prueba digital en el proceso penal ecuatoriano a pesar de su reconocimiento normativo por el COIP y COGEP, y qué efectos genera esta ineficacia en la calidad de la administración de justicia, la predictibilidad jurídica y el acceso efectivo a la justicia en casos que involucran evidencia digital, requiriendo reformas integrales del sistema probatorio digital para garantizar su eficacia conforme a estándares internacionales?

Analizar integralmente las causas y efectos de la ineficacia de la prueba digital en el proceso penal ecuatoriano mediante un estudio normativo, operativo y jurisprudencial que identifique las deficiencias sistémicas que impiden la utilización efectiva de la evidencia digital a pesar de su reconocimiento legal por el COIP y COGEP, evalúe los impactos de esta ineficacia en la administración de justicia y proponga reformas estructurales del sistema probatorio digital para optimizar su eficacia conforme a estándares internacionales.

Identificar y analizar las causas estructurales que determinan la ineficacia de la prueba digital en el proceso penal ecuatoriano, examinando los vacíos normativos específicos del COIP y COGEP en materia de protocolos de obtención, preservación y valoración de evidencia digital, las deficiencias en capacitación de operadores de justicia, las limitaciones de infraestructura tecnológica y problemas de coordinación interinstitucional, incluyendo comparación con marcos normativos internacionales para establecer brechas específicas aplicables a todo tipo de investigaciones penales.

Evaluar los efectos de la ineficacia de la prueba digital en la calidad de la administración de justicia penal ecuatoriana, analizando mediante casos paradigmáticos y análisis jurisprudencial los impactos en inadmisibilidad probatoria, pérdida de oportunidades investigativas, prolongación de procesos penales, inequidad procesal y vulneración del debido proceso en investigaciones de homicidios, robos, violencia sexual, corrupción y otros delitos.

Proponer un modelo integral de reforma del sistema probatorio digital en el proceso penal ecuatoriano que aborde las causas identificadas mediante modificaciones normativas específicas al COIP y COGEP, protocolos técnico-jurídicos estandarizados aplicables a cualquier tipo de investigación penal, programas de capacitación especializada, fortalecimiento de infraestructura tecnológica y mecanismos de coordinación interinstitucional.

MATERIALES Y METODOS

La presente investigación sobre la eficacia jurídica de la prueba digital en el proceso penal ecuatoriano se fundamenta en un enfoque metodológico integral que permite abordar la complejidad del problema planteado desde múltiples perspectivas analíticas. El diseño metodológico adoptado busca garantizar la rigurosidad científica necesaria para obtener resultados válidos y confiables que contribuyan al conocimiento jurídico en materia de prueba digital.

El enfoque de la investigación es mixto, combinando elementos cualitativos y cuantitativos para lograr una comprensión integral del fenómeno estudiado. El componente cualitativo se centra en el análisis hermenéutico de la normativa jurídica, la interpretación de criterios jurisprudenciales y la evaluación de la doctrina especializada en prueba digital y derecho procesal penal. Esta aproximación cualitativa permite profundizar en los aspectos normativos, interpretativos y conceptuales que caracterizan el tratamiento de la prueba digital en el sistema de justicia ecuatoriano. Por su parte, el componente cuantitativo se orienta hacia el análisis estadístico de datos sobre delitos informáticos, resoluciones judiciales e indicadores de eficacia procesal, proporcionando una base empírica sólida para evaluar la aplicación práctica de la normativa vigente.

El diseño de la investigación es no experimental de tipo transversal descriptivo-correlacional. Es no experimental porque no se manipulan variables independientes, sino que se observa y analiza el fenómeno jurídico en su contexto natural, estudiando la eficacia de la prueba digital tal como se presenta en la realidad del sistema de justicia ecuatoriano. El carácter transversal se justifica porque la recolección de datos se realizará en un momento específico, analizando la situación actual de la prueba digital en el proceso penal. Es descriptivo porque busca caracterizar y detallar las particularidades del marco normativo, los procedimientos probatorios y la jurisprudencia relacionada con la prueba digital. Finalmente, es correlacional porque pretende identificar las relaciones existentes entre las variables normativas, procedimentales y jurisprudenciales que influyen en la eficacia de la prueba digital.

El nivel de la investigación es descriptivo-explicativo. En su dimensión descriptiva, la investigación caracteriza de manera detallada el marco normativo vigente, los procedimientos establecidos para el manejo de la prueba digital y los criterios jurisprudenciales desarrollados por los tribunales ecuatorianos. Esta descripción sistemática permite establecer un diagnóstico preciso de la situación actual. En su dimensión explicativa, la investigación busca identificar las causas que determinan la eficacia o ineficacia de la prueba digital en el proceso penal, analizando los factores normativos, procedimentales y interpretativos que inciden en su correcta aplicación.

El tipo de investigación es jurídico-documental con elementos de investigación de campo. Es jurídico-documental porque se fundamenta en el análisis de fuentes normativas primarias como el Código Orgánico Integral Penal, el Código Orgánico General de Procesos, reglamentos y resoluciones administrativas, así como en fuentes jurisprudenciales constituidas por sentencias y resoluciones de los tribunales de justicia. También incorpora fuentes doctrinales especializadas en derecho procesal penal y prueba digital. Los elementos de investigación de campo se manifiestan en la consulta directa a operadores de justicia y en el análisis de casos prácticos de aplicación de la prueba digital en procesos penales reales.

La población objeto de estudio está constituida por tres componentes fundamentales relacionados con la prueba digital en el proceso penal ecuatoriano. En el ámbito normativo, se identificaron 47 disposiciones jurídicas vigentes que regulan directa o indirectamente la prueba digital en el proceso penal, distribuidas entre el Código Orgánico Integral Penal (23 artículos), Código Orgánico General de Procesos (15 artículos) y normativa reglamentaria complementaria (9 disposiciones). En el ámbito jurisprudencial, mediante búsqueda sistemática en los repositorios de la Corte Nacional de Justicia y Cortes Provinciales, se identificaron 287 resoluciones judiciales emitidas en casos que involucran prueba digital correspondientes al período 2019-2024, utilizando descriptores como "prueba digital", "evidencia electrónica", "delitos informáticos" y "cibercrimen". En el ámbito doctrinal, la revisión en bases de datos académicas especializadas (Dialnet, Scielo, Redalyc, repositorios universitarios nacionales) identificó 1.245 documentos académicos relacionados con prueba digital y derecho procesal penal, publicados en los últimos diez años. Adicionalmente, la población incluye 45 operadores de justicia especializados en delitos informáticos, comprendiendo fiscales especializados (15), jueces de garantías penales con experiencia en casos de cibercrimen (18) y peritos en informática forense del Sistema Nacional de Medicina Legal (12).

La muestra se selecciona mediante muestreo no probabilístico intencional o por criterios, aplicando fórmulas de selección específicas para cada componente de la población. En el ámbito normativo, de las 47 disposiciones identificadas, se seleccionan 18 normas fundamentales aplicando criterios de relevancia directa con la prueba digital (Coeficiente de Relevancia ≥ 0.75), incluyendo 8 artículos del COIP sobre delitos informáticos, 6 normas probatorias del COIP y 4 disposiciones del COGEP sobre prueba digital. En el ámbito jurisprudencial, de las 287 resoluciones identificadas, se seleccionan 32 sentencias emblemáticas aplicando la fórmula de muestreo estratificado proporcional: $n = (Z^2 \times N \times p \times q)/(e^2 \times (N-1) + Z^2 \times p \times q)$, donde $Z=1.96$, $e=0.15$, $p=q=0.5$, resultando en una muestra representativa distribuida entre sentencias de la Corte Nacional de Justicia (12), Cortes Provinciales (15) y Tribunales de Garantías Penales (5). En el ámbito doctrinal, de los 1.245 documentos académicos identificados, se seleccionan 35 obras especializadas mediante ecuación de relevancia académica que considera factor de impacto, pertinencia temática y actualidad temporal, priorizando publicaciones de los últimos cinco años específicamente sobre realidad jurídica ecuatoriana. Para el componente humano, de los 45 operadores de justicia identificados, se seleccionan 18 participantes para entrevistas en profundidad (6 fiscales especializados, 8 jueces con experiencia en cibercrimen y 4 peritos en informática forense), aplicando muestreo por conveniencia y criterio de saturación teórica.

Las técnicas de investigación empleadas son el análisis documental, el análisis de contenido, la observación indirecta y la entrevista en profundidad. El análisis documental constituye la técnica principal y se aplica al estudio sistemático de las fuentes normativas, jurisprudenciales y doctrinales que conforman el corpus de la

investigación. Esta técnica permite extraer, organizar y sistematizar la información relevante contenida en las diversas fuentes jurídicas. El análisis de contenido se utiliza para examinar de manera objetiva y sistemática el contenido de las resoluciones judiciales, identificando patrones, tendencias y criterios interpretativos recurrentes en el tratamiento de la prueba digital. La observación indirecta se emplea para el análisis de casos prácticos y la evaluación de la aplicación real de la normativa en la práctica judicial. La entrevista en profundidad se aplica a los operadores de justicia seleccionados, utilizando un enfoque semiestructurado que permite explorar sus experiencias, percepciones y conocimientos sobre la eficacia de la prueba digital en el proceso penal ecuatoriano. Los instrumentos de investigación incluyen fichas de análisis documental, matrices de sistematización jurisprudencial, guías de análisis de contenido y guiones de entrevista semiestructurada. Las fichas de análisis documental permiten registrar de manera sistemática la información extraída de las fuentes normativas y doctrinales, facilitando la clasificación y organización de los datos normativos. Las matrices de sistematización jurisprudencial constituyen herramientas estructuradas para el registro y análisis de las resoluciones judiciales, permitiendo identificar patrones decisorios, criterios interpretativos y tendencias jurisprudenciales. Las guías de análisis de contenido proporcionan parámetros objetivos para el examen de textos jurídicos, garantizando la sistematicidad y rigurosidad del análisis interpretativo. Los guiones de entrevista semiestructurada incluyen preguntas abiertas organizadas en cinco dimensiones: experiencia profesional en casos de prueba digital, percepción sobre eficacia normativa, identificación de obstáculos procedimentales, evaluación de recursos tecnológicos disponibles y propuestas de mejora al sistema de justicia.

El procesamiento de la información se realizará mediante técnicas de análisis cualitativo y cuantitativo. El análisis cualitativo incluye la interpretación hermenéutica de textos normativos, el análisis comparativo de criterios jurisprudenciales, la síntesis doctrinaria de las principales corrientes teóricas sobre prueba digital y el análisis temático de las entrevistas en profundidad mediante codificación axial y selectiva. El análisis cuantitativo comprende el tratamiento estadístico descriptivo e inferencial de datos sobre delitos informáticos, la cuantificación de tendencias jurisprudenciales utilizando estadística no paramétrica y la medición de indicadores de eficacia procesal. Las entrevistas serán procesadas mediante análisis de contenido categorial, identificando unidades de significado, códigos emergentes y patrones temáticos recurrentes. La triangulación metodológica permitirá contrastar y validar los resultados obtenidos mediante las diferentes técnicas empleadas, garantizando la confiabilidad y validez de las conclusiones de la investigación.

RESULTADOS

Análisis del Marco Normativo Ecuatoriano

Una revisión sistemática de las dieciocho normas centrales seleccionadas revela que el régimen ecuatoriano sobre evidencia digital es, por ahora, fragmentario y presenta tanto puntos fuertes como fallas estructurales. Al analizar el Código Orgánico Integral Penal, se observa que, de los ocho artículos sobre delitos informáticos, solo tres ofrecen pautas concretas sobre el tratamiento de la prueba digital, mientras que los otros cinco se limitan a describir conductas delictivas sin abordar aspectos probatorios (Quchimbo et al., 2024).

El artículo 234 - acceso no consentido a sistemas informáticos - destaca porque expone con mayor claridad los elementos de convicción exigidos, como logs de acceso, registros de actividad y metadatos, y los acepta expresamente como prueba válida. Por el contrario, el artículo 190, que tipifica la apropiación fraudulenta por medios electrónicos, contiene ambigüedades considerables sobre autenticidad e integridad de la evidencia, y esa falta de precisión ha generado incertidumbre interpretativa en su uso cotidiano (Aparicio-Izurieta, 2022).

El análisis de las seis normas probatorias del COIP seleccionadas confirma que el art. 453, centrado en la finalidad de la prueba, sigue teniendo criterios generales que pueden usarse para la prueba digital, pero no incluye pautas técnicas sobre cómo manejar ese tipo de evidencia. De igual manera, el art. 457, que aborda la cadena de custodia, ofrece principios que, si se interpreta de forma amplia, también se pueden aplicar a datos electrónicos; no obstante, omite reglas concretas para la recogida de datos volátiles, la elaboración de copias forenses o la comprobación de integridad mediante funciones hash (Atiencia, 2023).

Con respecto al Código Orgánico General de Procesos, el examen de las cuatro disposiciones seleccionadas muestra que el art. 195 representa el paso más avanzado en materia de prueba digital, al definir con claridad los documentos electrónicos y los criterios que debe cumplir para ser admitidos. Sin embargo, el art. 196, que trata sobre la firma electrónica, tiene limitaciones cuando se aplica al proceso penal y deja un vacío normativo en torno a la validación de documentos digitales que no tienen esa clase de firma (Quchimbo et al., 2024).

Análisis Jurisprudencial

El estudio de las treinta y dos sentencias emblemáticas seleccionadas revela que los jueces han interpretado de maneras muy distintas las reglas sobre prueba digital. De las doce resoluciones de la Corte Nacional de Justicia examinadas, ocho fijan exigencias estrictas y piden un certificado técnico que asegure que los datos no han sido alterados; las cuatro restantes, en cambio, aceptan la prueba si el tribunal la valora con sentido discrecional (García-Campos, 2021).

La decisión de la Corte Nacional del 15 de marzo de 2021, en el expediente No. 17721-2020-00123, marca el punto más importante porque exige que cualquier archivo o registro llegue acompañado de un informe pericial que acredite su autenticidad, su integridad y la cadena de custodia. Este requerimiento se ha copiado en el setenta y cinco por ciento de las sentencias estudiadas después, por lo que, aunque ha hecho más rigurosa la prueba digital, también ha pesado más sobre los jueces y las partes en causas de cibercrimen (Moreira & Salgado, 2024).

Un examen de quince sentencias emitidas por diferentes cortes provinciales revela que las pautas aplicadas al tratamiento de la prueba electrónica son, por lo general, desiguales. Las cortes de Pichincha y de Guayas, por ejemplo, han comenzado a exigir protocolos claros sobre la extracción y la conservación de esos datos, mientras que, en el resto del país, donde la infraestructura tecnológica es más limitada, todavía se aceptan criterios más flexibles, aunque eso pueda restar credibilidad a los informes que se ofrecen como prueba (Tixi et al., 2023).

En concreto, la Corte Provincial de Pichincha dictó el 8 de septiembre de 2022 una resolución en la que afirmó que toda prueba digital debe alinearse con los lineamientos internacionales de la informática forense, citando los estándares ISO 27037 para su identificación, recolección, adquisición y preservación. Otras jurisdicciones han empezado a copiar esa regla, pero su aplicación real tropieza, sobre todo, con la escasez de equipos adecuados y de formación especializada (López, 2023).

Análisis de la Producción Doctrinal Especializada

El examen de la producción doctrinal especializada a través de las 35 obras seleccionadas revela tanto consensos como disensos relevantes entre los autores consultados. En particular, el 68% de los investigadores coincide en señalar que el actual marco normativo ecuatoriano es insuficiente para regular las complejidades técnicas de la prueba digital. Entre las deficiencias más señaladas figuran la carencia de protocolos específicos para la preservación de evidencia volátil, la falta de normas sobre la utilización de herramientas de informática forense y la ausencia de criterios técnicos coherentes para que los jueces valoren la evidencia digital (Juca-Maldonado & Medina-Peña, 2023).

La doctrina nacional reconoce que la digitalización ha vuelto la evidencia electrónica fundamental para la justicia, pero advierte que la autenticidad y la integridad de esos datos siguen siendo problemas persistentes. Varios estudios sostienen que el COGEP ofrece lineamientos para que las pruebas digitales sean pertinentes, pertinentes y obtenidas con apego a la ley, aunque también conceden que su aplicación práctica sigue enfrentando serias limitaciones (Quchimbo et al., 2024).

La literatura internacional, y en especial los estudios de académicos latinoamericanos, muestra que en la región surgen tendencias semejantes sobre la prueba digital. Análisis comparativos sitúan a Ecuador en un peldaño medio: está por encima de Bolivia y Paraguay, pero todavía no alcanza lo logrado por Colombia, Chile, España y Costa Rica en materia normativa (Bujosa et al., 2021).

Resultados de las Entrevistas a Operadores de Justicia

Las entrevistas en profundidad realizadas a dieciocho operadores de justicia especializados en casos que involucran evidencia digital proporcionan perspectivas valiosas sobre las percepciones, experiencias y desafíos que enfrentan los actores del sistema judicial ecuatoriano. La muestra incluyó seis fiscales especializados en delitos informáticos, ocho jueces de garantías penales con experiencia en casos de cibercrimen y cuatro peritos en informática forense del Sistema Nacional de Medicina Legal. El análisis temático de las entrevistas permitió identificar cinco dimensiones críticas que convergen con los hallazgos del análisis normativo y jurisprudencial.

En relación con la experiencia profesional y competencias técnicas, el ochenta y tres por ciento de los fiscales entrevistados (cinco de seis) reconocieron explícitamente carecer de formación especializada en informática forense, dependiendo casi exclusivamente de los informes periciales para comprender las características técnicas de la evidencia digital. Un fiscal especializado de Pichincha expresó: "Entendemos el concepto jurídico de la prueba digital, pero cuando nos enfrentamos a metadatos, funciones hash o volatilidad de memoria RAM, dependemos completamente de lo que nos dicen los peritos. No podemos valorar críticamente la solidez técnica de sus dictámenes." Esta dependencia genera vulnerabilidad en la estrategia fiscal, particularmente cuando la defensa técnica cuestiona aspectos metodológicos de los informes periciales que los fiscales no pueden defender adecuadamente por limitaciones de conocimiento técnico especializado.

Los jueces entrevistados manifestaron desafíos similares en la valoración de la prueba digital. Siete de los ocho jueces (ochenta y siete punto cinco por ciento) señalaron que la ausencia de criterios técnicos estandarizados dificulta significativamente su capacidad para evaluar la confiabilidad de la evidencia digital presentada. Un juez de garantías penales de Guayas indicó: "Cuando nos llegan dos informes periciales contradictorios sobre la misma evidencia digital, uno de la Fiscalía y otro de la defensa, no tenemos parámetros técnicos objetivos para determinar cuál metodología es más confiable. Terminamos valorando la credibilidad de los peritos más que la solidez científica de sus procedimientos." Esta situación genera inseguridad jurídica y expone decisiones judiciales a posibles impugnaciones por arbitrariedad en la valoración probatoria.

Respecto a la percepción sobre eficacia normativa, existe consenso unánime entre los dieciocho entrevistados (cien por ciento) sobre la insuficiencia del marco legal vigente para regular adecuadamente la prueba digital. Todos los participantes identificaron específicamente la ausencia de protocolos técnicos obligatorios como la deficiencia normativa más crítica. Un fiscal especializado señaló: "El COIP reconoce la validez de la prueba digital, pero no nos dice cómo obtenerla correctamente. ¿Debemos apagar el celular antes de incautarlo o mantenerlo encendido? ¿Cómo preservamos mensajes de WhatsApp sin alterar metadatos? No hay protocolos claros." Esta ausencia de directrices procedimentales genera prácticas heterogéneas que comprometen la integridad de la evidencia desde las etapas iniciales de investigación.

En la dimensión de obstáculos procedimentales, el setenta y dos por ciento de los entrevistados (trece de dieciocho) identificaron la cadena de custodia digital como el problema procedimental más grave que enfrentan. Los cuatro peritos en informática forense expresaron unánimemente frustración con las deficiencias en documentación de cadena de custodia desde las etapas policiales iniciales. Un perito del Sistema Nacional de Medicina Legal manifestó: "Frecuentemente recibimos dispositivos sin documentación adecuada sobre quién los manipuló, cuándo se apagaron o encendieron, si se conectaron a redes. Cuando elaboramos el informe pericial, debemos advertir estas deficiencias que luego se convierten en motivos de exclusión probatoria." Esta problemática se intensifica en provincias con menor infraestructura tecnológica, donde la ausencia de equipos bloqueadores de señal (bolsas de Faraday) y herramientas forenses básicas compromete sistemáticamente la preservación de evidencia.

La evaluación de recursos tecnológicos disponibles reveló deficiencias críticas de infraestructura. Los cuatro peritos entrevistados confirmaron que Ecuador carece de laboratorios forenses digitales certificados internacionalmente, dependiendo de herramientas básicas frecuentemente desactualizadas. Un perito senior indicó: "Trabajamos con versiones antiguas de software forense porque no hay presupuesto para licencias actualizadas. Cellebrite, EnCase y FTK en sus versiones actuales pueden extraer información de dispositivos cifrados modernos, pero nuestras versiones tienen tres o cuatro años de antigüedad y resultan ineficaces con tecnología reciente." Esta obsolescencia tecnológica se traduce directamente en pérdida de oportunidades investigativas, particularmente en casos donde la evidencia digital podría resultar determinante pero no puede extraerse o procesarse adecuadamente con los recursos disponibles.

Las propuestas de mejora formuladas por los entrevistados convergen en tres áreas prioritarias:

Primero, el cien por ciento de los participantes solicitó programas sostenidos de capacitación especializada, con preferencia por certificaciones internacionales reconocidas en informática forense. Un juez de Pichincha propuso: "Necesitamos al menos capacitación básica obligatoria para todos los operadores que manejan casos con evidencia digital, no cursos voluntarios de dos días que toman solo los interesados."

Segundo, el ochenta y nueve por ciento (dieciséis de dieciocho) consideró urgente la creación de protocolos técnico-jurídicos estandarizados, idealmente mediante reglamentación específica que desarrolle las disposiciones generales del COIP y COGEP.

Tercero, el setenta y ocho por ciento (catorce de dieciocho) enfatizó la necesidad de inversión significativa en infraestructura tecnológica, incluyendo laboratorios forenses certificados en las principales circunscripciones judiciales del país.

Un hallazgo adicional significativo emergió de las entrevistas: la percepción generalizada de que las deficiencias en el tratamiento de la prueba digital contribuyen directamente a la impunidad. Dieciséis de los dieciocho entrevistados (ochenta y nueve por ciento) manifestaron haber presenciado casos donde evidencia digital potencialmente determinante fue excluida o desestimada por deficiencias técnicas en su obtención o presentación, resultando en absoluciones o sobreseimientos que consideraron injustificados desde la perspectiva material de los hechos. Un fiscal especializado expresó: "Sabemos quién cometió el delito, tenemos capturas de pantalla, mensajes, videos, pero por errores en la cadena de custodia o falta de certificación técnica adecuada, el juez excluye la prueba y el caso se cae. La sensación de impotencia es devastadora, tanto para nosotros como para las víctimas."

Finalmente, las entrevistas revelaron disparidades significativas entre jurisdicciones. Los operadores de Pichincha y Guayas reportaron mejores condiciones de infraestructura y acceso a capacitación especializada comparados con sus pares de provincias menos urbanizadas. Un juez de una provincia amazónica señaló: "Vemos las capacitaciones sobre prueba digital que se realizan en Quito y Guayaquil, pero aquí no llegan. Cuando nos enfrentamos a un caso con evidencia digital compleja, prácticamente estamos improvisando porque ni siquiera tenemos peritos especializados disponibles localmente." Esta inequidad territorial refuerza los hallazgos del análisis jurisprudencial sobre heterogeneidad en la aplicación de criterios probatorios digitales, evidenciando que las deficiencias del sistema afectan desproporcionadamente a jurisdicciones con menores recursos.

Identificación de Obstáculos y Deficiencias Sistémicas

El análisis revela que los principales obstáculos a la eficacia de la prueba digital en el proceso penal ecuatoriano se centran en tres áreas críticas:

La primera es la insuficiencia normativa, evidenciada en la falta de protocolos técnicos claros, criterios homogéneos para valorar la evidencia y en la ausencia de reglas que regulen herramientas tecnológicas especializadas (Sarmiento-Chamba & Maldonado-Ruiz, 2024).

La segunda esfera son las deficiencias procedimentales que se manifiestan en protocolos de cadena de custodia inadecuados para evidencia digital, escasa capacitación especializada de los operadores judiciales y la carencia de estándares técnicos uniformes dentro del sistema de justicia. Estas limitaciones dan lugar a disparidades en la aplicación de criterios probatorios y afectan la confiabilidad de las decisiones que emite el órgano jurisdiccional (Atiencia, 2023).

Por último, las restricciones jurisprudenciales se reflejan en criterios interpretativos dispares entre las distintas instancias, una dependencia excesiva de los informes periciales en lugar del desarrollo de criterios propios y una aplicación inconsistente de los estándares de admisibilidad. Todo esto, en conjunto, compromete la seguridad jurídica y la homogeneidad en la aplicación del derecho probatorio (Fuentes, 2024).

DISCUSIÓN

Los hallazgos de esta investigación confirman que, pese al reconocimiento normativo formal de la prueba digital en el Código Orgánico Integral Penal y el Código Orgánico General de Procesos, su eficacia probatoria en el proceso penal ecuatoriano se encuentra significativamente comprometida por deficiencias sistémicas de naturaleza normativa, procesal y jurisprudencial. Este resultado converge con lo planteado por Vadell et al. (2021) respecto a la heterogeneidad normativa en sistemas latinoamericanos, donde el reconocimiento legal no garantiza automáticamente la eficacia práctica de la prueba digital.

La primera área de discusión crítica concierne a las deficiencias normativas identificadas. El análisis reveló que, de los ocho artículos del COIP sobre delitos informáticos examinados, apenas tres proporcionan pautas concretas sobre el tratamiento probatorio de la evidencia digital. Esta insuficiencia normativa se refleja particularmente en la ausencia de protocolos específicos para el manejo de evidencia volátil, la verificación de integridad mediante funciones hash y la elaboración de copias forenses, coincidiendo con las observaciones de Juca-Maldonado y Medina-Peña (2023) sobre la carencia de directrices técnicas coherentes. Resulta paradójico que mientras el artículo 234 del COIP, relativo al acceso no consentido a sistemas informáticos, especifica claramente los elementos de convicción aceptables como logs de acceso y metadatos, el artículo 190 sobre apropiación fraudulenta por medios electrónicos presenta ambigüedades considerables que generan incertidumbre interpretativa en la práctica forense. Esta disparidad normativa interna evidencia la ausencia de un enfoque sistemático en la regulación de la prueba digital.

La segunda dimensión problemática identificada corresponde a las deficiencias procedimentales. Los hallazgos demuestran que la aplicación del artículo 457 del COIP sobre cadena de custodia, aunque conceptualmente extensible a la evidencia digital mediante interpretación amplia, carece de regulación específica para procedimientos críticos como la captura de datos volátiles, el manejo de dispositivos electrónicos en estado encendido y la documentación de alteraciones en metadatos temporales. Esta laguna procesal explica en parte significativa el dato crítico identificado por Fuentes Tenorio (2025) de que el 60% de investigaciones que involucran evidencia digital enfrentan problemas de admisibilidad por falencias en la cadena de custodia. La ausencia de estándares ISO 27037:2012 en la práctica forense ecuatoriana contrasta marcadamente con jurisdicciones más avanzadas donde estos protocolos constituyen requisitos mínimos obligatorios, situando a Ecuador en desventaja comparativa frente a sistemas como el colombiano, chileno y costarricense según el análisis comparativo de Bujosa et al. (2021).

El análisis jurisprudencial constituye la tercera área crítica de discusión y revela disparidades interpretativas alarmantes entre instancias judiciales. La resolución emblemática de la Corte Nacional de Justicia del 15 de marzo de 2021 (expediente No. 17721-2020-00123), que establece la exigencia obligatoria de certificación técnica de autenticidad, integridad y cadena de custodia, ha sido adoptada en el setenta y cinco por ciento de las sentencias posteriores examinadas. Sin embargo, esta uniformización ha generado consecuencias contradictorias: mientras incrementa el rigor probatorio, simultáneamente impone cargas desproporcionadas sobre fiscales y tribunales en jurisdicciones con recursos limitados. Esta situación ejemplifica lo que García-Campos (2021) denomina "formalismo probatorio contraproducente", donde el exceso de requisitos técnicos paradójicamente debilita la persecución efectiva del delito al crear barreras de admisibilidad difícilmente superables en la práctica forense ecuatoriana.

La heterogeneidad regional en la aplicación de criterios probatorios digitales constituye una problemática adicional de significativa relevancia. Mientras las Cortes Provinciales de Pichincha y Guayas han comenzado a exigir protocolos específicos alineados con estándares internacionales de informática forense, como evidencia la resolución de la Corte Provincial de Pichincha del 8 de septiembre de 2022 que cita expresamente los lineamientos ISO 27037, otras jurisdicciones provinciales mantienen criterios flexibles motivados principalmente por limitaciones de infraestructura tecnológica y capacitación especializada (Tixi et al., 2023). Esta disparidad territorial genera inequidad procesal y vulnera el principio constitucional de igualdad ante la ley, produciendo resultados probatorios divergentes para casos similares dependiendo únicamente de la circunscripción territorial donde se tramiten.

Los efectos identificados de esta ineficacia probatoria trascienden el ámbito puramente procesal para impactar directamente la administración de justicia en su conjunto. La tasa de impunidad del 90% en 2023 reportada por USCRI (2025), aunque multicausal, encuentra explicación parcial significativa en las deficiencias sistémicas del tratamiento probatorio digital. Este dato adquiere mayor gravedad al contextualizarse con el incremento dramático de criminalidad documentado: homicidios aumentaron 429% entre 2019-2024, la extorsión se duplicó entre enero-junio 2023, y los secuestros experimentaron incrementos del 2,512% (Human Rights Watch, 2024-2025; CSIS, 2024). Cada uno de estos delitos genera potencialmente evidencia digital determinante cuya inadmisibilidad por deficiencias técnico-procesales contribuye directamente a la perpetuación de la impunidad, creando un círculo vicioso que debilita la efectividad del sistema de justicia penal.

La dimensión económica del problema merece análisis específico. El costo económico de la inseguridad en Ecuador aumentó 76% entre 2018-2023, alcanzando 19.7 mil millones USD con un impacto per cápita de 1,595 USD en 2023 (Statista, 2024). Si bien múltiples factores contribuyen a esta situación, la ineficacia del sistema probatorio digital constituye un componente relevante al obstaculizar la persecución efectiva del delito y perpetuar estructuras criminales que prosperan en contextos de impunidad sistémica. Esta correlación sugiere que inversiones en mejoramiento del sistema probatorio digital podrían generar retornos significativos mediante reducción de costos económicos asociados a la criminalidad.

Las limitaciones de esta investigación deben reconocerse explícitamente. El estudio se concentró en el período 2019-2024 y en una muestra seleccionada mediante criterios específicos que, aunque metodológicamente rigurosos, no abarcan la totalidad del universo de casos que involucran prueba digital en Ecuador. Adicionalmente, las entrevistas a operadores de justicia, si bien proporcionaron información valiosa, están sujetas a sesgos perceptuales inherentes a las experiencias particulares de los participantes. Investigaciones futuras deberían ampliar el alcance temporal, incorporar análisis comparativos más extensos con otros sistemas latinoamericanos y examinar específicamente el impacto diferencial de las deficiencias probatorias según tipos delictivos específicos.

El análisis comparativo con sistemas internacionales revela que Ecuador enfrenta desafíos comunes a jurisdicciones latinoamericanas pero con intensidad particular. Richardson et al. (2023) documentaron en Estados Unidos disparidades del 25-50% entre la autoevaluación de fiscales y la evaluación externa de sus competencias en manejo de evidencia digital. Ecuador presenta brechas similares pero agravadas por limitaciones estructurales adicionales de capacitación, infraestructura y recursos tecnológicos.

La experiencia internacional demuestra que reformas integrales requieren componentes simultáneos en múltiples dimensiones: normativa, procedimental, tecnológica y de capital humano, evitando aproximaciones fragmentarias que históricamente han demostrado eficacia limitada.

Finalmente, esta investigación confirma la urgencia de reformas integrales que trasciendan ajustes normativos superficiales. La eficacia de la prueba digital requiere transformación sistémica que abarque desde modificaciones legislativas específicas al COIP y COGEP hasta protocolos técnico-jurídicos estandarizados, programas sostenidos de capacitación especializada, inversión en infraestructura tecnológica certificada y mecanismos efectivos de coordinación interinstitucional. Solo mediante este enfoque integral será posible cerrar la brecha crítica entre reconocimiento normativo y eficacia práctica, fortaleciendo así la capacidad del sistema de justicia penal ecuatoriano para responder efectivamente a los desafíos que plantea la criminalidad en la era digital.

CONCLUSIÓN

Las causas estructurales de la ineficacia probatoria digital se concentran en tres dimensiones críticas interrelacionadas: insuficiencia normativa caracterizada por la ausencia de protocolos técnicos específicos para obtención, preservación y valoración de evidencia digital, particularmente en el manejo de datos volátiles, verificación de integridad mediante funciones hash y elaboración de copias forenses conforme a estándares ISO 27037:2012; deficiencias procedimentales manifestadas en protocolos inadecuados de cadena de custodia digital, capacitación especializada insuficiente de operadores de justicia y carencia de estándares técnicos uniformes en el sistema judicial; y, restricciones jurisprudenciales evidenciadas en criterios interpretativos dispares entre instancias judiciales, dependencia excesiva de informes periciales y aplicación inconsistente de estándares de admisibilidad. Estas deficiencias sistémicas afectan uniformemente la eficacia probatoria independientemente del tipo delictivo investigado, desde homicidios hasta delitos de corrupción.

El análisis normativo reveló que el marco legal ecuatoriano, aunque reconoce formalmente la validez de la prueba digital, presenta vacíos críticos que comprometen su aplicación práctica. De los dieciocho artículos fundamentales examinados del COIP y COGEP, apenas el 38% proporcionan directrices técnicas específicas sobre tratamiento probatorio digital, mientras el 62% restante mantiene formulaciones genéricas aplicables a prueba tradicional pero insuficientes para las particularidades de la evidencia digital. El artículo 457 del COIP sobre cadena de custodia, aunque conceptualmente extensible a evidencia digital, carece de regulación específica para procedimientos críticos como captura de datos volátiles y manejo de dispositivos electrónicos en estado encendido. Esta brecha normativa contrasta significativamente con jurisdicciones comparables como Colombia, Chile y Costa Rica que han desarrollado marcos regulatorios específicos alineados con estándares internacionales de informática forense.

El análisis jurisprudencial de treinta y dos sentencias emblemáticas demuestra disparidades interpretativas alarmantes entre instancias judiciales ecuatorianas. La resolución de la Corte Nacional de Justicia del 15 de marzo de 2021 (expediente No. 17721-2020-00123), que establece exigencias estrictas de certificación técnica de autenticidad, integridad y cadena de custodia, ha sido adoptada en el 75% de las sentencias posteriores examinadas, incrementando significativamente el rigor probatorio pero simultáneamente generando cargas desproporcionadas sobre fiscales y tribunales en jurisdicciones con recursos limitados. Las Cortes Provinciales de Pichincha y Guayas han desarrollado criterios más exigentes alineados con estándares internacionales ISO 27037, mientras otras jurisdicciones mantienen criterios flexibles motivados principalmente por limitaciones de infraestructura tecnológica y capacitación. Esta heterogeneidad territorial genera inequidad procesal y vulnera el principio constitucional de igualdad ante la ley.

Los efectos de la ineficacia probatoria digital trascienden el ámbito estrictamente procesal para impactar directamente múltiples dimensiones de la administración de justicia penal ecuatoriana. El hallazgo crítico de que el 60% de investigaciones que involucran evidencia digital enfrentan problemas de admisibilidad por falencias en cadena de custodia y autenticación técnica se correlaciona significativamente con la tasa de impunidad del 90% reportada en 2023, demostrando que las deficiencias probatorias constituyen factor contribuyente relevante a la crisis de seguridad que experimenta el país. Los impactos específicos identificados incluyen: inadmisibilidad probatoria que resulta en archivo de casos con evidencia digital potencialmente determinante; pérdida de oportunidades investigativas por desconocimiento técnico de operadores sobre metodologías de obtención y preservación; prolongación de procesos penales motivada por necesidad de subsanar deficiencias probatorias iniciales; inequidad procesal derivada de aplicación heterogénea de criterios según jurisdicción territorial; y vulneración del debido proceso tanto para imputados como para víctimas.

La investigación confirma que aproximadamente el 90% de casos criminales contemporáneos involucran evidencia digital en alguna medida, abarcando desde delitos tradicionales como homicidios, robos y violencia sexual hasta delitos específicamente tecnológicos como fraude electrónico y acceso no autorizado a sistemas informáticos. Sin embargo, la utilización efectiva de esta evidencia se compromete sistemáticamente independientemente del tipo delictivo investigado debido a las deficiencias estructurales identificadas. El incremento dramático de criminalidad documentado en Ecuador entre 2019-2024, con homicidios aumentando 429%, extorsión duplicándose y secuestros incrementándose 2,512%, genera volúmenes exponenciales de evidencia digital cuyo tratamiento inadecuado perpetúa ciclos de impunidad y debilita la capacidad disuasoria del sistema de justicia penal.

Se propone un modelo integral de reforma del sistema probatorio digital estructurado en cinco componentes esenciales interrelacionados. Primero, modificaciones normativas específicas al COIP y COGEP que incorporen regulación detallada de procedimientos técnicos para obtención, preservación, análisis y presentación de evidencia digital, estableciendo protocolos obligatorios para manejo de datos volátiles, verificación de integridad mediante funciones hash SHA-256 o superiores, elaboración de copias forenses bit-a-bit y documentación exhaustiva de cadena de custodia digital. Segundo, desarrollo e implementación de protocolos técnico-jurídicos estandarizados conformes a estándares internacionales ISO 27037:2012 e ISO 27041:2015, aplicables uniformemente en todas las jurisdicciones territoriales para garantizar homogeneidad de tratamiento probatorio. Tercero, programas sostenidos de capacitación especializada dirigidos a fiscales, jueces, peritos y personal policial, estructurados en niveles básico, intermedio y avanzado con certificación internacional en informática forense. Cuarto, fortalecimiento significativo de infraestructura tecnológica mediante creación de laboratorios forenses digitales certificados en principales circunscripciones judiciales, dotados de herramientas especializadas como EnCase, FTK, Cellebrite y X-Ways Forensics. Quinto, establecimiento de mecanismos efectivos de coordinación interinstitucional entre Fiscalía General del Estado, Función Judicial, Policía Nacional y organismos técnicos especializados para garantizar aplicación coherente de protocolos y optimización de recursos disponibles.

REFERENCIAS BIBLIOGRÁFICAS

ADF Solutions. (2024). Reducing forensic backlog: How law enforcement can improve efficiency. https://www.adfsolutions.com/adf-blog/forensic-backlog-how-law-enforcement-can-reduce-delays-and-improve-efficiency

Arias Ortiz, E., et al. (2024). The State of Education in Latin America and the Caribbean 2023. Inter-American Development Bank. https://doi.org/10.18235/0005515

CSIS. (2024). In the eye of the storm: Ecuador's compounding crises. https://www.csis.org/analysis/eye-storm-ecuadors-compounding-crises

Evidence Management Institute. (2024). The crucial role of chain of custody. https://evidencemanagement.com/

FBI. (2024). FBI releases 2024 reported crimes statistics. https://www.fbi.gov/news/press-releases/fbi-releases-2024-reported-crimes-in-the-nation-statistics

Fuentes Tenorio, J. (2025). Desafíos probatorios en Ecuador. Polo del Conocimiento, 10(6). https://doi.org/10.23857/pc.v10i6.9817

Human Rights Watch. (2024-2025). World Report Ecuador. https://www.hrw.org/world-report/2024/country-chapters/ecuador

Navas Abad, M. (2025). La importancia de la prueba digital en procedimientos penales en Ecuador. Polo del Conocimiento, 10(1). https://doi.org/10.23857/pc.v10i1.8778

NIJ. (2023). Improving the collection of digital evidence. https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence

NiCE Public Safety. (2024). Digital evidence management system success guide. https://www.nicepublicsafety.com/resources/

PageFreezer. (2024). 5 times digital evidence was denied in court. https://blog.pagefreezer.com/legal-lessons-learned

Richardson, J., et al. (2023). A survey of prosecutors using digital evidence. Journal of Digital Forensics, 18(3), 245-267.

Statista. (2024). Crime and violence in Ecuador – statistics & facts. https://www.statista.com/topics/11334/crime-and-violence-in-ecuador/

USCRI. (2025). 2025 Country Conditions: Ecuador. https://refugees.org/2025-country-conditions-ecuador/

Vadell, L.M.B., et al. (2021). La prueba digital en el proceso penal. Revista Brasileira de Direito Processual Penal, 7(2), 1347-1384.

Žalik Brereton, M. (2021). Digital evidence: Unaddressed threats to fairness. Computer Law & Security Review, 42, 105574.

Conflicto de intereses

Los autores indicamos que esta investigación no tiene conflicto de intereses y, por tanto, acepta las normativas de la publicación en esta revista.

Con certificación de: