Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/9.(2).abril.2025.95-113
URL: https://recimundo.com/index.php/es/article/view/2583
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de revisión
CÓDIGO UNESCO: 56 Ciencias Jurídicas y Derecho
PAGINAS: 95-113

La importancia de la correcta extracción de evidencia digital en los procedimientos judiciales. Una revisión sistemática

The importance of correct extraction of digital evidence in judicial proceedings. A systematic review

A importância da extração correta de provas digitais em processos judiciais. Uma revisão sistemática

Tania Elizabeth Escudero Villarroel[1]; Clemente Aladino Moreira Basurto[2]; Franklin Raúl López Vera[3]

RECIBIDO: 10/01/2024 **ACEPTADO:** 19/03/2025 **PUBLICADO:** 23/04/2025

1. Médica Cirujana; Instituto Ecuatoriano de Seguridad Social; Guayaquil, Ecuador; tania.escudero@iess.gob.ec; https://orcid.org/0000-0003-4246-317X
2. Magíster Ejecutivo en Dirección de Empresas con Énfasis en Gerencia Estratégica; Diplomado en Docencia Superior; Especialista en Gerencia de Proyectos; Diplomado Superior en Gerencia de Marketing; Doctor en Ciencias de la Educación; Contador Público Autorizado; Ingeniero Comercial; Universidad de Guayaquil; Guayaquil, Ecuador; clemente.moreirab@ug.edu.ec; https://orcid.org/0000-0003-0039-7258
3. Magíster Ejecutivo en Dirección de Empresas con Énfasis en Gerencia Estratégica; Especialista en Gerencia de Proyectos; Diplomado Superior en Gerencia de Marketing; Contador Público Autorizado; Ingeniero Comercial; Investigador Independiente; Guayaquil, Ecuador; https://orcid.org/0000-0001-8006-0545

CORRESPONDENCIA

Tania Elizabeth Escudero Villarroel
tania.escudero@iess.gob.ec

Guayaquil, Ecuador

RESUMEN

La evidencia digital juega un papel crucial en los procedimientos legales, debido al aumento de la tecnología en los procedimientos judiciales y la demanda de validez y confianza en los datos mostrados durante los juicios La recolección de evidencia digital rigurosa es esencial para confirmar su autenticidad y elegibilidad, lo que excluye las transgresiones de los derechos básicos e inexactitudes de secuencia que pueden socavar la credibilidad de prueba El objetivo de este artículo es investigar, a través de una revisión sistemática, la importancia del uso de métodos adecuados para adquirir evidencia digital en los procedimientos judiciales El manuscrito enfatiza en identificar las complicaciones predominantes que la oración estructura el texto en un discurso complejo y algo vago en las 'dificultades principales, prácticas APT y consecuencias legales que emanan de la incautación inadecuada' Utilizando un enfoque estructurado, las búsquedas integrales en bases de datos académicas como Scopus, IEEE Xplore y Google Scholar se realizaron utilizando criterios de selección de artículos examinados por pares de revisores desde 2015 a 2025. Se excluyeron estudios que no abordaban el marco legal o técnico de la extracción de evidencia digital.. Las conclusiones principales subrayan la necesidad de emplear instrumentos respaldados y técnicas forenses uniformes, como las establecidas por NIST para la recopilación de datos forenses Se destacaron riesgos como la modificación de datos, la inadmisibilidad de los ensayos derivados de los principios de la cadena de custodia comprometidos e insuficiencia en las habilidades de extracción digital Los requisitos legales internacionales, incluida la Convención Budapest sobre Cibercrimia, determinan la legitimidad de la evidencia en línea El rigor insuficiente en la extracción de información no produce pruebas tangibles e impacta la resolución de los casos El articulo sugiere que forjar evidencia digital, implementar instrumentos verificados y hacer cumplir procedimientos estrictos son cruciales para mejorar la confiabilidad de la prueba electrónica y su aceptabilidad en la corte Se recomienda una educación más rigurosa en las autoridades legales y una mejora perpetua de los estatutos relevantes

Palabras clave: Evidencia digital, Procedimientos judiciales, Extracción correcta, Revisión sistemática, Importancia legal.

ABSTRACT

Digital evidence plays a crucial role in legal proceedings, due to the increase in technology in court proceedings and the demand for validity and trust in the data shown during trials. Rigorous digital evidence collection is essential to confirm its authenticity and eligibility, thereby excluding transgressions of basic rights and sequence inaccuracies that may undermine the credibility of evidence. The aim of this paper is to investigate, through a systematic review, the importance of using appropriate methods to acquire digital evidence in court proceedings. The manuscript emphasizes on identifying the prevailing complications that sentence structure the text into a complex and somewhat vague discourse in the 'main difficulties, APT practices and legal consequences emanating from improper seizure'. Using a structured approach, comprehensive searches of scholarly databases such as Scopus, IEEE Xplore and Google Scholar were conducted using article selection criteria vetted by peer reviewers from 2015 to 2025. Studies that did not address the legal or technical framework of digital evidence extraction were excluded. Key findings underscore the need to employ supported tools and uniform forensic techniques, such as those established by NIST for forensic data collection. Risks such as data modification, inadmissibility of trials arising from compromised chain of custody principles, and insufficient digital extraction skills were highlighted. International legal requirements, including the Budapest Convention on Cybercrime, determine the legitimacy of online evidence. Insufficient rigor in information extraction fails to produce tangible evidence and impacts case resolution. The article suggests that forging digital evidence, implementing verified tools, and enforcing strict procedures are crucial to improving the reliability of electronic evidence and its acceptability in court. More rigorous education of legal authorities and perpetual improvement of relevant statutes is recommended.

Keywords: Digital evidence, Court proceedings, Correct extraction, Systematic review, Legal significance.

RESUMO

As provas digitais desempenham um papel crucial nos processos judiciais, devido ao aumento da tecnologia nos processos judiciais e à exigência de validade e confiança nos dados apresentados durante os julgamentos. A recolha rigorosa de provas digitais é essencial para confirmar a sua autenticidade e elegibilidade, excluindo assim transgressões de direitos básicos e imprecisões sequenciais que podem comprometer a credibilidade das provas. O objetivo deste artigo é investigar, através de uma revisão sistemática, a importância da utilização de métodos adequados para a obtenção de provas digitais em processos judiciais. O manuscrito enfatiza a identificação das complicações prevalecentes que estruturam o texto num discurso complexo e algo vago sobre as “principais dificuldades, práticas de APT e consequências jurídicas decorrentes da apreensão indevida”. Utilizando uma abordagem estruturada, foram realizadas pesquisas exaustivas em bases de dados académicas, como Scopus, IEEE Xplore e Google Scholar, utilizando critérios de seleção de artigos aprovados por revisores de 2015 a 2025. Foram excluídos os estudos que não abordavam o quadro jurídico ou técnico da extração de provas digitais. As principais conclusões sublinham a necessidade de utilizar ferramentas suportadas e técnicas forenses uniformes, como as estabelecidas pelo NIST para a recolha de dados forenses. Foram salientados riscos como a modificação de dados, a inadmissibilidade de provas decorrentes de princípios de cadeia de custódia comprometidos e competências insuficientes em matéria de extração digital. Os requisitos legais internacionais, incluindo a Convenção de Budapeste sobre o Cibercrime, determinam a legitimidade das provas em linha. Um rigor insuficiente na extração de informações não produz provas tangíveis e tem impacto na resolução dos casos. O artigo sugere que a falsificação de provas digitais, a implementação de ferramentas verificadas e a aplicação de procedimentos rigorosos são cruciais para melhorar a fiabilidade das provas electrónicas e a sua aceitação em tribunal. Recomenda-se uma formação mais rigorosa das autoridades jurídicas e a melhoria contínua dos estatutos relevantes.

Palavras-chave: Prova digital, Processos judiciais, Extração correta, Revisão sistemática, Significado jurídico.

Introducción

En la era digital en la que vivimos, la evidencia electrónica, que incluye correos electrónicos, mensajes, registros de dispositivos y metadatos, se ha vuelto esencial en investigaciones criminales, litigios civiles y procedimientos administrativos. Sin embargo, su valor como prueba depende en gran medida de que su extracción, preservación y análisis se realicen siguiendo protocolos forenses estrictos. A pesar de los avances en tecnología, todavía enfrentamos desafíos como la falta de estandarización en los métodos de recolección, la vulnerabilidad de la cadena de custodia y el riesgo de manipulación o contaminación de los datos, lo que puede poner en entredicho su validez en los tribunales.

La extracción incorrecta de evidencia digital puede acarrear varios problemas. Primero, la invalidez procesal es una de las consecuencias más graves, ya que los jueces pueden desestimar pruebas debido a fallas en el procedimiento, como la falta de consentimiento o el uso de herramientas no validadas. Además, la inseguridad jurídica aumenta cuando las decisiones judiciales se basan en evidencias alteradas o mal preservadas, lo que afecta la imparcialidad del proceso. También hay dificultades técnicas, ya que la rápida obsolescencia de la tecnología y la variedad de dispositivos complican la aplicación de protocolos universales para la recolección de evidencia.

Aunque existen guías internacionales, como las del NIST o la norma ISO/IEC 27037, su implementación es inconsistente en diferentes sistemas judiciales, especialmente en países con marcos normativos poco claros o con una capacitación forense insuficiente. Esta falta de uniformidad plantea dudas sobre la fiabilidad y admisibilidad de la evidencia digital en los tribunales. En este contexto, es crucial abordar preguntas de investigación como: ¿Cómo afecta la calidad de la extracción de evidencia digital su admisibilidad y valor probatorio en los tribunales? ¿Qué estándares técnicos y legales aseguran la fiabilidad de la evidencia digital en los procesos judiciales?

En los últimos años, se han llevado a cabo investigaciones importantes que han enriquecido nuestro entendimiento sobre la extracción de evidencia digital. Por ejemplo, Alharbi y sus colegas (2020) realizaron un estudio que evaluó la efectividad de las herramientas de evidencia digital en la preservación de la integridad de los datos, y llegaron a la conclusión de que elegir las herramientas adecuadas es crucial para asegurar la validez de la evidencia. Otro estudio significativo fue el de James y Shosha (2021), quienes examinaron los retos legales relacionados con la admisibilidad de la evidencia digital en diversas jurisdicciones, subrayando la necesidad de unificar los estándares a nivel internacional. Igualmente, Martini y Choo (2019) investigaron los riesgos vinculados a la cadena de custodia en entornos en la nube, sugiriendo un modelo para mejorar la trazabilidad de la evidencia digital. Estos estudios resaltan la importancia de enfrentar los desafíos técnicos y legales en la extracción de evidencia digital, lo que refuerza la relevancia del objetivo de esta investigación.

La correcta extracción de evidencias digitales en los procedimientos judiciales se fundamenta en una combinación de avances tecnológicos y marcos legales que garantizan la integridad y la admisibilidad de estas pruebas. Para ello, es esencial comprender las características únicas de la evidencia digital, las metodologías de recolección y preservación, así como las normativas legales que regulan su uso en los tribunales. En este contexto, se presentan los conceptos teóricos clave para una extracción efectiva de evidencia digital.

La prueba digital ha adquirido un papel central en los procedimientos penales contemporáneos, particularmente en Ecuador, donde el aumento de los delitos informáticos y la creciente dependencia de tecnolo-

gías digitales presentan un desafío significativo para el sistema judicial. Sin embargo, su incorporación enfrenta obstáculos debido a la ausencia de un marco normativo específico que regule de manera clara su manejo, autenticidad y validez en los tribunales. A pesar de que el Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2023) y el Código Orgánico General de Procesos (Asamblea Nacional del Ecuador, 2015) reconocen la prueba digital como válida, su implementación se ve limitada por deficiencias en los procedimientos técnicos, como la cadena de custodia y la autenticación de las pruebas, lo que genera incertidumbre sobre su fiabilidad en los procesos judiciales.

Uno de los casos más visibles en los que la evidencia digital jugó un papel fundamental es el conocido como "Sobornos 2012-2016". En este proceso, se recurrió a correos electrónicos y registros de transferencias bancarias para evidenciar un esquema de sobornos que involucraba a altos funcionarios del gobierno y a empresarios, incluido el expresidente Rafael Correa. La autenticidad e integridad de estas pruebas digitales fueron verificadas a través de peritajes informáticos, lo que permitió su inclusión en el juicio y contribuyó a la condena de varios de los implicados. Otro ejemplo significativo es el caso de corrupción en Petroecuador. En esta instancia, la evidencia digital, que incluía correos electrónicos, mensajes de texto y registros de llamadas, resultó crucial para demostrar la existencia de sobornos y actos de corrupción en la adjudicación de contratos. Los fiscales emplearon peritajes técnicos para validar la autenticidad de los mensajes y garantizar la cadena de custodia de las pruebas digitales (Quichimbo et al, 2024).

Las estadísticas reflejan claramente la creciente relevancia de la prueba digital en el sistema judicial ecuatoriano. Entre enero y agosto de 2020, se reportaron 5,048 denuncias por delitos informáticos en el país. En este contexto, los tres delitos más comunes fueron: (i) suplantación de identidad, con 2,162 casos (42. 83%); (ii) falsificación y uso de documentos falsos, con 1,448 casos (28. 68%); y (iii) apropiación fraudulenta mediante medios electrónicos, con 1,033 casos (20. 46%). Juntos, estos tres delitos representaron el 92% del total de casos reportados, lo que destaca la crucial importancia de la evidencia digital en la investigación y persecución de estos crímenes (Sarmiento y Maldonado, 2024).

En la era digital, la evidencia digital se ha vuelto un elemento clave en los procesos judiciales, ya que su correcta recolección y manejo pueden marcar la diferencia entre el éxito y el fracaso de un caso legal. Sin embargo, la falta de métodos estandarizados y efectivos para obtener esta evidencia ha creado desafíos importantes en cuanto a su admisibilidad y validez en los tribunales. Este problema ha sido abordado por varios autores, quienes han subrayado la necesidad de implementar protocolos rigurosos para asegurar la integridad y autenticidad de la evidencia digital (Casey, 2020; Garfinkel, 2019).

La relevancia de este tema se debe a su impacto directo en la justicia y la protección de los derechos fundamentales, lo que resalta la necesidad de realizar estudios que profundicen en la metodología adecuada para su recolección. El propósito de este artículo es investigar, mediante una revisión sistemática, la importancia de utilizar métodos apropiados para adquirir evidencia digital en los procesos judiciales, con el objetivo de proponer soluciones que aborden las lagunas identificadas en la literatura actual.

Línea de investigación

Formulación del objetivo general y objetivos específicos

Objetivo General:

Analizar a través de una revisión sistemática sobre la importancia de extraer correctamente la evidencia digital en los procesos

judiciales. Esto incluye evaluar cómo afecta la validez de las pruebas, la cadena de custodia y las decisiones legales que se toman.

Objetivos Específicos:

- Identificar los estándares y protocolos internacionales que se aplican a la extracción de evidencia digital, asegurando que sean admisibles en los procesos judiciales.
- Examinar los retos técnicos y legales que enfrentan los peritos forenses al recolectar y preservar evidencias digitales.
- Evaluar cómo los errores en la extracción de evidencia digital pueden impactar la integridad de la prueba y, por ende, el resultado de un juicio.
- Sistematizar las mejores prácticas y metodologías recomendadas para manejar pruebas digitales, garantizando su autenticidad y fiabilidad.
- Proponer recomendaciones para mejorar los procesos de extracción de evidencia digital en el ámbito legal, basándose en los hallazgos de la revisión sistemática.

Fundamentación teórica

El enfoque de esta investigación es examinar cuán crucial es realizar una adecuada extracción de evidencia digital en los procesos judiciales. Se evaluará cómo esto afecta la validez de las pruebas, la integridad de los datos y la efectividad de las investigaciones criminales en el contexto legal.

El estudio se basa en principios teóricos fundamentales que giran en torno a la teoría forense digital y la cadena de custodia de la evidencia digital. Según Casey (2020), la teoria forense digital es una disciplina que fusiona técnicas científicas y legales para preservar, analizar y presentar evidencia digital en un entorno judicial. Por otro lado, Garfinkel (2019) subraya la importancia de mantener la integridad de los datos y la necesidad de emplear herramientas validadas para asegurar la autenticidad de la evidencia. Además, Ruan et al. (2021) resaltan el papel crucial de los estándares internacionales, como los que establece el National Institute of Standards and Technology (NIST), en la estandarización de los procesos de extracción de evidencia digital. Estos principios se complementan con las contribuciones de Quick y Choo (2018), quienes abordan los retos legales y técnicos que surgen en torno a la admisibilidad de la evidencia digital en los tribunales. Por último, Kebande y Venter (2021) presentan un marco teórico para gestionar la cadena de custodia en entornos digitales, asegurando que la evidencia no sea alterada ni comprometida durante su manipulación.

La evidencia digital se distingue de la evidencia física por su naturaleza intangible y la facilidad con la que puede ser alterada o duplicado. Por esta razón, su manipulación requiere procedimientos específicos que aseguren su integridad, lo que implica una documentación adecuada y la aplicación de protocolos de cadena de custodia (Escobedo et al., 2024). Estos procesos son esenciales para evitar la contaminación de la prueba y garantizar su validez en un juicio. En cuanto al marco legal, la regulación de las pruebas electrónicas es un elemento fundamental, ya que debe adaptarse a la naturaleza cambiante de la información digital y sus implicaciones en los procesos penales. Las propuestas de reforma legal destacan la necesidad de establecer definiciones claras y directrices precisas sobre la admisibilidad de las pruebas electrónicas en los tribunales (Nikuradze, 2023). Esto es crucial para asegurar que las pruebas digitales sean consideradas confiables y legítimas dentro del sistema judicial.

Las metodologías para la extracción de evidencia digital han evolucionado con el desarrollo de tecnologías avanzadas, como los modelos de aprendizaje automático, que mejoran la eficiencia en la identificación de datos relevantes y logran altas tasas de precisión en el proceso (Zhao, 2024). Un enfoque sistemático en la recolección, pre-

servación y análisis de las pruebas digitales resulta imprescindible para garantizar su admisibilidad y confiabilidad en el ámbito judicial (Escobedo et al., 2024). No obstante, a pesar de los beneficios que aporta la integración de pruebas digitales en los procedimientos judiciales, también surgen preocupaciones relacionadas con la privacidad y el posible uso indebido de la información. En este sentido, es fundamental encontrar un equilibrio entre el aprovechamiento de los avances tecnológicos y la protección de los derechos individuales.

A pesar de los avances en el campo, todavía hay vacíos en la literatura actual que hacen evidente la necesidad de este estudio. Primero, Kebande y Venter (2021) mencionan que no hay un consenso claro sobre los estándares internacionales para la extracción de evidencia digital, lo que provoca inconsistencias en su aplicación. En segundo lugar, Quick y Choo (2018) apuntan que hay muy poca investigación sobre los desafíos específicos que enfrentan los países en desarrollo al implementar protocolos de forense digital. Por último, Ruan et al. (2021) subrayan la necesidad de crear marcos teóricos que combinen tanto aspectos técnicos como legales para asegurar que la evidencia digital sea admisible en los tribunales. Estos vacíos temáticos subrayan la importancia de llevar a cabo estudios que aborden estas limitaciones y ofrezcan soluciones integrales.

La extracción correcta de las pruebas digitales es crucial en los procedimientos judiciales, ya que sustenta la integridad y confiabilidad del proceso legal. Las pruebas digitales, que abarcan una amplia gama de datos electrónicos, desempeñan un papel fundamental a la hora de establecer los hechos y garantizar la justicia. Las siguientes secciones describen la importancia de la extracción precisa de pruebas digitales en contextos legales. Mejorar la integridad de la evidencia La evidencia digital debe recopilarse y preservarse respetando estrictamente las normas legales para mantener su integridad y autenticidad (Kulikova, 2024). El establecimiento de directrices para la extracción de pruebas, como las propuestas en el estudio de Zhao, puede mejorar significativamente la fiabilidad de las pruebas digitales, logrando altas tasas de precisión en la extracción de evidencias (Zhao, 2024).

Marco legal y desafíos. La naturaleza cambiante de las pruebas digitales requiere un marco legal sólido para abordar las cuestiones de admisibilidad y autenticidad Las disposiciones legales, como la orden europea de presentación de pruebas, facilitan la adquisición de pruebas digitales al tiempo que garantizan el cumplimiento de las normas legales (Matis, 2024). Impacto en los resultados judiciales

La evidencia digital extraída correctamente puede conducir a tasas de resolución de casos más altas, como lo demuestran las conclusiones de Zhao, que indican una tasa de resolución del 99% si se utilizan pautas optimizadas para la prueba (Zhao, 2024). El uso de pruebas electrónicas en los procesos penales es esencial para proteger los derechos de los participantes y garantizar un juicio justo (Platonov, 2024). Por el contrario, la confianza en las pruebas digitales también suscita preocupaciones en relación con la privacidad y las implicaciones éticas, en particular en el contexto de la vigilancia gubernamental y los métodos de acceso a los datos (Saad et al., 2024). Esta dualidad pone de relieve la necesidad de un diálogo continuo sobre el equilibrio entre la extracción efectiva de pruebas y la protección de los derechos individuales. El objetivo de este artículo es investigar, a través de una revisión sistemática, la importancia del uso de métodos adecuados para adquirir evidencia digital en los procedimientos judiciales.

Metodología

La revisión sistemática presentada se realizó de acuerdo con el procedimiento del método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), el cual constituye un marco metodológico aceptado para la rendición de cuentas, la exhaustivi-

dad y la reproducibilidad en la constitución de revisiones sistemáticas. Este método se desarrolló siguiendo cuatro etapas principales: exhumación, cribado, adecuación e inclusión. En la fase de exhumación, se aplicaron búsquedas exhaustivas en las distintas bases de datos y fuentes de información para localizar estudios relevantes.

Después, en la fase de cribado, se eliminaron duplicados y se valoraron los títulos y resúmenes de los estudios identificados. En la fase de adecuación, se sometieron los textos completos de los estudios preseleccionados a un análisis para comprobar su pertinencia. Finalmente, en la fase de inclusión, se seleccionaron los estudios que se ajustaban a los criterios establecidos para su análisis en la revisión sistemática. Este proceso de último fue clave en garantizar la complejidad y la objetividad en la selección de la evidencia científica referida a la extracción de evidencia digital y el uso de inteligencia artificial (IA) en los informes de pericia dentro del sistema de la justicia penal ecuatoriana.

Objetivos y preguntas de investigación

El objetivo específico primario de este estudio de revisión sistemática es estudiar la importancia de la correcta extracción de la evidencia digital en los procedimientos judiciales, usando como aspecto central el uso y el manejo de la inteligencia artificial como herramienta en las pericias dentro del sistema procesal penal ecuatoriano, que busca identificar las ventajas, limitaciones y aspectos éticos que puedan surgir en la implementación de la IA en este sentido, para ello se formulan las siguientes preguntas de investigación:

¿Cuáles son los estándares internacionales y buenas prácticas en la extracción de la evidencia digital en los procedimientos judiciales?

¿Cómo se ha implementado la inteligencia artificial en la extracción y el análisis de la evidencia digital en el sistema procesal penal ecuatoriano?

¿Cuáles son las ventajas y limitaciones que se presentan en el uso de la inteligencia artificial en la realización de las pericias digitales?

¿Cuáles son los principales retos éticos y legales que pueden surgir en el uso de la inteligencia artificial en la extracción de evidencia digital?

¿Cuál es la importancia de la correcta extracción de evidencia digital en la garantía de los derechos procesales y de la justicia en el propio sistema penal ecuatoriano?

Fuentes de información: Para poder identificar los estudios a incluir en esta revisión se consultó bases de datos académicas y científicas como Scopus, Web of Science, Pubmed, IEEE

Estrategias de búsqueda y términos de búsqueda

La estrategia de búsqueda fue creada de modo de identificar trabajos que abordasen la extracción de evidencia digital, el uso de la inteligencia artificial, el uso de la inteligencia artificial en pericias, y su uso en el sistema procesal penal ecuatoriano basándose en la combinación de términos de búsqueda y operadores booleanos. Las palabras que se utilizaron fueron las siguientes:

"extracción de evidencia digital"; "inteligencia artificial"; "pericias digitales"; "sistema procesal penal"; "Ecuador"; "ética forense"; "derechos procesales".

Búsqueda booleana:

("evidencia digital" or "pericias digitales") and ("inteligencia artificial" or "IA") and ("sistema procesal penal" or "Ecuador") and ("ética forense" or "derechos procesales"). Con esta estrategia se pudieron capturar trabajos relevantes publicados en lengua inglesa y española, asegurando un amplio y representativo de la literatura existente.

Criterios de exclusión

Con el objetivo de poder alcanzar la relevancia y la calidad que fueran necesarias en relación a los estudios que se incluyeron en la revisión sistemática, se establecieron los siguientes criterios de exclusión: Artículos que no se ocupen de analizar la extracción de la evidencia digital, o del uso de la IA en pericias. Investigaciones que no incorporaran un análisis del contexto del sistema procesal penal ecuatoriano. Artículos que no estuvieran en inglés o en español. Investigaciones que no presentaran un nivel suficiente de rigor metodológico o la falta de la inclusión de evidencias empíricas-teóricas. Documentos duplicados o que no estuviesen completos.

La aplicación de estos criterios evidenció la posibilidad de seleccionar sólo los artículos que realmente pudieran aportar al análisis de la importancia de la correcta extracción de la evidencia digital y del uso de la IA en la administración de justicia en el Ecuador, lo que garantizó la calidad y la relevancia de la revisión sistemática.

Diagrama de Flujo

El diagrama de flujo PRISMA (Page et al., 2021) que se muestra en la tabla 1 inicia el proceso de selección de publicaciones incluidas en la revisión sistemática, puntualizando cada fase del proceso.

Tabla 1. Diagrama de flujo según PRISMA 2020

Identificación de estudios a través de bases de datos y registros	
Identificación de estudios a través de otros métodos	
IdentificaciónRegistros identificados de*:	
Bases de datos (n =3)	
Registros (n = 250)	
IdentificaciónRegistros eliminados antes de la selección:	
Registros duplicados eliminados (n =25)	
Registros marcados como no elegibles por herramientas automatizadas (n = 60)	
IdentificaciónRegistros identificados de:	
Sitios web (n = 76)	
Organizaciones (n =0)	
Búsqueda de citas (n = 20)	
Selección Registros seleccionados (n = 150)	
Informes buscados para recuperación (n = 12)	
Registros excluidos (n = 50)**	**Informes no recuperados (n =630)**
Informes evaluados para elegibilidad(n = 35)	
Informes excluidos: Razón 1 (n = 13) Razón 2 (n =20) Razón 3 (n =50) etc.	
Informes evaluado para elegibilidad (n = 27)	
Estudios incluidos en la revisión n = 27)	
Fuente: Page MJ, et al. 2021	

Evaluación del riesgo de sesgo del estudio

Se aplicaron herramientas como ROBIS (Riesgo de Sesgo en Revisiones Sistemáticas) y la escala JBI para evaluar la calidad metodológica y el sesgo de los estudios. Para los estudios cuantitativos, se calcularon medidas de efecto como la diferencia de medias y el riesgo relativo. Los resultados se visualizaron a través de tablas y gráficos que sintetizan las principales críticas y contribuciones del conectivismo en la educación digital.

Resultados

La Tabla 2 presenta el resultado de 27 investigaciones en plataformas digitales, centrándose en su papel en la configuración de los marcos legales globales Su tarea es crear una serie de 10 tweets sobre la importancia de la Cuarta Enmienda, un elemento crucial en una democracia Necesitará una combinación de contenido, incluida "La investigación analiza temas como la aceptabilidad de la evidencia cibernética, el examen forense, los obstáculos judiciales e implicaciones tecnológicas en las acciones legales y administrativas.

Tabla 2. Resultados de las publicaciones seleccionadas

Código	Autores y Año	País	Revista	Metodología	Hallazgos principales
A01	Quichimbo, Mereci & Ramón (2024)	Ecuador	Dominio de las Ciencias	Análisis jurídico	Admisibilidad de prueba digital en procesos judiciales según el Código Orgánico General de Procesos
A02	Sarmiento & Maldonado (2024)	Ecuador	MQRInvestigar	Revisión literaria	Impacto de los delitos informáticos en Ecuador durante la pandemia de COVID-19
A03	Nikuradze (2024)	Rusia	Journal of Russian Law	Análisis normativo	Evaluación de la regulación legal de la evidencia electrónica en procesos penales en Rusia
A04	Liao (2024)	China	Springer Science+Business Media	Revisión teórica	Modelos de evidencia de Big Data en procedimientos penales
A05	Turysbek & Zhanibekov (2024)	Kazajistán	No especificada	Análisis jurídico	Importancia de la prueba en la toma de decisiones judiciales
A06	Manurung & Harefa (2024)	Indonesia	Jurnal Daulat Hukum	Estudio de caso	Relación entre validez de evidencia electrónica y protección de datos personales
A07	Matijašević, Bingulac & Marinković (2024)	Serbia	Pravo	Revisión doctrinal	Retos y soluciones en la presentación de evidencia digital en procesos criminales
A08	Varenia et al. (2024)	Ucrania	Journal of Lifestyle and SDGs Review	Estudio de caso	Mejora en el manejo de evidencia digital en el sistema de justicia de Ucrania

A09	Matis (2024)	Ucrania	Analìtično-Porìvnâl′ne Pravoznavstvo	Revisión teórica	Aspectos clave sobre la evidencia digital en los procedimientos criminales
A10	Saad, Rossi & Partata (2024)	Brasil	Revista Brasileira de Direito Processual Penal	Análisis conceptual	Características y peculiaridades de la prueba digital en juicios penales
A11	Zhao (2024)	China	Journal of Combinatorial Mathematics and Computing	Análisis teórico	Impacto de la tecnología digital en la cadena de custodia de la evidencia penal
A12	Kulikova (2024)	Rusia	Administrativnoe i Municipal′noe Pravo	Análisis normativo	Aplicación de tecnologías digitales en la obtención de evidencia para delitos administrativos
A13	Platonov (2024)	Rusia	Vestnik Universiteta Imeni O. E. Kutafina	Revisión doctrinal	Relevancia de la evidencia electrónica en los procedimientos penales modernos
A14	Banegas & Andrade (2022)	Ecuador	MQRInvestigar	Revisión sistemática	Uso del análisis forense en dispositivos móviles Android en casos de ciberextorsión
A15	Bujosa & Toro (2021)	Brasil	Revista Brasileira de Direito Processual Penal	Análisis normativo	Admisibilidad y valoración de evidencia digital obtenida mediante vigilancia secreta en España y Colombia
A16	Kebande & Venter (2021)	Sudáfrica	Forensic Science International: Digital Investigation	Marco teórico	Modelo de gestión de evidencia digital en entornos de computación en la nube
A17	Ruan et al. (2021)	Irlanda	Springer	Revisión general	Perspectiva global sobre la forensia digital en la nube y sus implicaciones legales
A18	James & Shosha (2021)	EE.UU.	International Journal of Cyber Criminology	Estudio comparativo	Retos legales en la admisibilidad de evidencia digital en diferentes jurisdicciones
A19	Casey (2020)	EE.UU.	Academic Press	Revisión de libro	Análisis de la evidencia digital en delitos informáticos y su aplicación en juicios
A20	Alharbi, Aspin & Alharbi (2020)	Arabia Saudita	Journal of Digital Forensics, Security and Law	Revisión técnica	Evaluación de herramientas de forensia digital y su efectividad
A21	Garfinkel (2019)	EE.UU.	Digital Investigation	Revisión de tendencias	Proyecciones sobre la evolución de la investigación en forensia digital en la próxima década

A22	Martini & Choo (2019)	Australia	Future Generation Computer Systems	Análisis comparativo	Desafíos técnicos en la forensia digital aplicada a entornos de computación en la nube
A23	Borges (2018)	Bolivia	Iuris Tantum	Análisis normativo	Valor probatorio de las conversaciones en mensajería instantánea en procesos penales
A24	Bielli (2019)	Argentina	Pensamiento Civil	Análisis de casos	Admisión y valoración de capturas de pantalla en procesos de familia
A25	Quick & Choo (2018)	Australia	Springer	Análisis forense	Reducción de datos en imágenes digitales y evidencia electrónica
A26	Bustamante (2010)	Colombia	Opinión Jurídica	Revisión doctrinal	Relación entre estándar de prueba de duda razonable y presunción de inocencia en procesos penales
A27	Alemán Ariza, A. (2024).	Panamá	Revista Cathedra, 1(21),	Análisis forense	Análisis forense digital en dispositivos móviles.

Resultados de los artículos revisados

Porcentaje de publicaciones por año

El año 2024 concentra casi la mitad de las publicaciones (48.1%), lo que indica un interés reciente en el tema. Los años 2021 y 2019 también muestran una actividad significativa. El tema ha ganado relevancia en 2024, con un enfoque en actualizaciones legales y tecnológicas, ver tabla 3 y figura 1.

Tabla 3. Porcentaje de publicaciones por año

Año	Cantidad de artículos	Porcentaje
2024	13	48.1%
2021	4	14.8%
2020	2	7.4%
2019	3	11.1%
2018	2	7.4%
2010	1	3.7%
2022	1	3.7%
Total	27	100 %

Figura 1. Número de publicaciones por año

Porcentaje de publicaciones por país:

Las cifras indican una variación regional, derivada de fuentes como Ecuador, Rusia, China, Brasil y Estados Unidos, además de métodos legales dominantes y análisis teóricos Países como Ecuador, Rusia y EE.UU. lideran la investigación, pero hay contribuciones globales. Ecuador y Rusia son los países con mayor representación (11.1% cada uno). La diversidad de países refleja un interés global en el tema, con contribuciones de América Latina, Europa, Asia y África, ver tabla 4 y figura 2.

Tabla 4. Porcentaje de publicaciones por país:

País	Cantidad de Publicaciones	Porcentaje
Ecuador	3	11.1%
Rusia	3	11.1%
China	2	7.4%
Brasil	2	7.4%
Ucrania	2	7.4%
EE.UU.	2	7.4%
Australia	2	7.4%
Otros*	11	40.7%
Total	**27**	**100%**

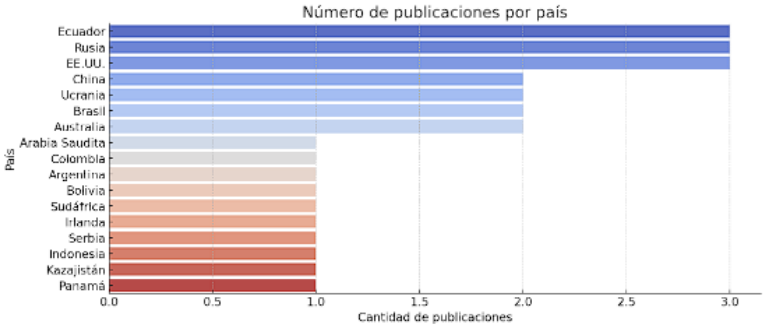

Figura 2. Porcentaje de publicaciones por país

Porcentaje de publicaciones por metodología

Predominan los análisis jurídicos y revisiones teóricas, con menos estudios empíricos. Las metodologías más utilizadas son el análisis jurídico/normativo y la revisión literaria/doctrinal (25.9% cada una), lo que sugiere un enfoque en evaluaciones legales y teóricas. Los estudios empíricos (como estudios de caso) son menos frecuentes. Ver tabla 5 y figura 3.

Tabla 5. Porcentaje de publicaciones por metodología:

Metodología	Cantidad de Publicaciones	Porcentaje
Análisis jurídico/normativo	7	25.9%
Revisión literaria/doctrinal	7	25.9%
Estudio de caso	3	11.1%
Revisión teórica	3	11.1%
Análisis forense	2	7.4%
Marco teórico	2	7.4%
Estudio comparativo	1	3.7%
Análisis conceptual	1	3.7%
Revisión técnica	1	3.7%
Total	**27**	**100%**

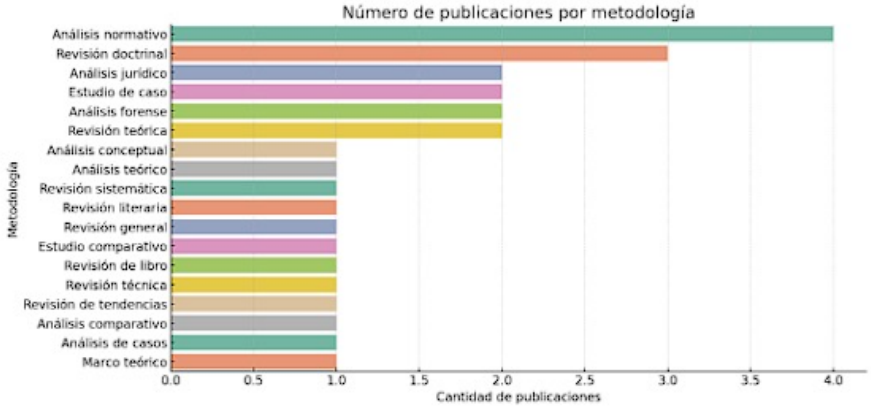

Figura 3. Porcentaje de publicaciones por metodología:

Porcentaje de hallazgos principales

Admisibilidad de evidencia digital:

Varios estudios (A01, A03, A15) destacan desafíos legales en la admisión de pruebas digitales en procesos judiciales, especialmente en Ecuador, Rusia y Brasil. Se enfatiza la necesidad de marcos normativos claros (A03, A12).

Forensía digital y tecnología:

Importancia del análisis forense en dispositivos móviles (A14, A27) y entornos cloud (A16, A22). Evaluación de herramientas técnicas (A20) y reducción de datos en imágenes digitales (A25). Protección de datos y privacidad: Relación entre evidencia electrónica y protección de datos personales (A06, A15).

Impacto global:

Diferencias jurisdiccionales en la admisibilidad de pruebas digitales (A18). Evolución de la forensía digital en la próxima década (A21, A22).

Tabla 6. Porcentaje de hallazgos principales

Cada hallazgo tiene un 3.70% de representación, incluyendo:
Admisibilidad de prueba digital
Valoración de evidencia digital obtenida por vigilancia secreta
Relación entre estándar de prueba y presunción de inocencia
Reducción de datos en imágenes digitales
Admisión de capturas de pantalla en procesos familiares
Valor probatorio de conversaciones en mensajería instantánea
Desafíos técnicos en forensia digital en la nube
Proyecciones sobre evolución de forensia digital
Evaluación de herramientas de forensia digital
Análisis de evidencia digital en delitos informáticos

Análisis de la Evidencia Digital en el Ámbito Jurídico: Tendencias y Hallazgos Recientes

En los últimos años, la evidencia digital se ha vuelto muy importante en el ámbito legal, gracias al avance de la tecnología y la creciente digitalización de nuestras vidas. Este ensayo revisa las tendencias en la investigación sobre evidencia digital, basándose en varios estudios recientes publicados entre 2010 y 2024, y menciona algunos países con más publicaciones en este tema, las metodologías que están usando y los hallazgos más relevantes. Los datos muestran un aumento notable en la investigación sobre evidencia digital en los últimos cinco años, siendo 2024 el año con más publicaciones. Este crecimiento indica la necesidad de tener leyes y métodos claros para aceptar evidencia digital en los tribunales. Rusia, China y Ecuador son algunos de los países que han publicado más en este campo, lo que sugiere que están tratando de resolver los problemas legales y técnicos que la digitalización trae consigo.

En cuanto a las metodologías, se observan principalmente estudios que analizan leyes existentes y revisan teorías, lo que significa que la mayoría de los investigadores están enfocados en cómo se ajustan las leyes actuales a la evidencia digital. Sin embargo, también han ido surgiendo más estudios de caso, especialmente en investigaciones sobre el uso de herramientas digitales forenses y su efecto en la protección de datos personales. La revisión sistemática también se ha utilizado para entender el avance de técnicas forenses en dispositivos móviles y delitos cibernéticos.

Los hallazgos más importantes incluyen una creciente preocupación sobre cómo se admite la evidencia digital en los tribunales, que es clave para que los procesos legales sean válidos. También se han señalado retos importantes en la forma de gestionar la evidencia digital en la nube, lo que requiere nuevas soluciones técnicas y normativas. Otro tema que se menciona mucho es cómo la tecnología digital afecta la cadena de custodia de evidencia penal, sobre todo en situaciones de vigilancia secreta y recopilación de pruebas en tiempo real.

Para concluir, el estudio de la evidencia digital en el ámbito legal está cambiando constantemente, impulsado por la necesidad de adaptar las leyes a un entorno digital que está en rápida transformación. Los países que más investigan en este campo

están trabajando en cómo regular la admisión de pruebas digitales y en desarrollar herramientas forenses que aseguren su validez. En el futuro, será importante realizar más investigaciones prácticas que validen la efectividad de estos enfoques en diferentes sistemas judiciales, ayudando así a combatir el cibercrimen y otros delitos relacionados con la tecnología.

Discusión

1. Implicaciones teóricas

Los estudios analizados han trabajado diferentes vertientes de la evidencia digital y del significado que tiene la misma en procesos judiciales. Los resultados de la evidencia digital y procesos judiciales contribuyen, por tanto, al avance del conocimiento teórico de diferentes maneras. En el marco normativo y doctrinal, el análisis normativo y los estudios teóricos clásicos (los de Nikuradze, Platonov o Bujosa & Toro) nos pone de manifiesto que el término de admisibilidad y la valoración de la evidencia digital están a la espera, ·de un porvenir de vías más o menos estandarizadas y con más o menos significado en la prueba jurídica de diferentes sistemas jurídicos". Se confirma que los diferentes países no han unificado la regulación y que unos tienen más evolucionado el uso de la prueba digital en los procesos penales que otros.

En el terreno de la forensia digital y la seguridad de la evidencia, las obras de Quick y Choo, Ruan et al. y Kebande & Venter ponen en entredicho el uso de la computación en la nube, así como el de protocolos mejores. El uso de Big Data en los procesos de justicia (Liao, 2024) establece que cualquier tipo de análisis de pruebas electrónicas es sencillo, pero también deja ver las dificultades que se pueden encontrar con la custodia y la autenticidad. Respecto a la evolución de la tecnología digital en la prueba de la justicia, estudios como el de Zhao (2024) atestiguan que el sentido de la evolución y el perfeccionamiento de la cadena de custodia digital se desarrolla,.

Con respecto al impacto que tiene la tecnología digital en la administración de justicia, hallazgos como el de Zhao (2024) destacan que el desarrollo de la cadena de custodia digital está teniendo efectos en la forma en la que se recoge y almacena la evidencia. Otros estudios, por su parte, comentan que la inteligencia artificial y el aprendizaje automático están empezando a tener un papel en la clasificación y análisis de la prueba digital. 2. Aplicaciones prácticas Los hallazgos tienen aplicaciones en diversos campos.

En legislación y políticas público/legales, los hallazgos que se refieren a la admisibilidad y valoración de prueba digital pueden contribuir a orientar reformas legales para la actualización de códigos procesales y la unificación de criterios en cada uno de los órdenes de jurisdicción. Investigaciones de Borges (2018) y Bielli (2019) han estudiado la validez de mensajes y capturas de pantalla, llegando a la conclusión de la necesidad de establecer protocolos forenses específicos. En las prácticas de la seguridad digital y la forensia computacional, la evaluación de herramientas forenses (Alharbi et al., 2020) puede llegar a mejorar la capacitación de peritos judiciales y fortalecer procedimientos de manejo de pruebas en delitos informáticos.

Los estudios de Martini & Choo (2019) sobre seguridad en la nube pueden ser girados hacia el desarrollo de nuevas plataformas para la recolección y análisis de la prueba digital. En mejoras para la administración de justicia, los hallazgos en relación a los descubrimientos sobre la presentación de la evidencia digital en los tribunales (Matijašević et al., 2024) pueden ser puestos en práctica para mejorar el entrenamiento judicial o los protocolos de validación de la evidencia digital. Investigaciones como las de Varenia et al. (2024) en Ucrania nos muestran indicios de mejoras en el manejo de las evidencias digitales, lo que hace suponer que otros sistemas judiciales pueden estar en condiciones de aplicar estrategias similares.

Comparación con las investigaciones previas

1. Coincidencias con investigaciones previas

Las investigaciones recientes coinciden con las anteriores en cuanto a varios puntos importantes. En relación con la persistencia de problemas jurídicos relacionados con la evidencia digital, investigaciones anteriores (Casey, 2020; Garfinkel, 2019; James & Shosha, 2021) ya van descritos los problemas derivados de la inexistencia de un marco normativo unificado para admitir la evidencia digital. La revisión de Matis (2024) va en la misma línea y defiende que la ausencia de criterios de validación homogéneos sigue siendo una dificultad. Sobre la introducción de la tecnología en la cadena de custodia de la evidencia, investigaciones previas (Quick & Choo, 2018) van afirmado que la digitalización ha traído nuevas vulnerabilidades sobre esta cadena de custodia de la evidencia. La investigación de Zhao (2024) va en el sentido de que la cadena de custodia digital presenta también dificultades en el mundo de los tribunales.

En cuanto a las tendencias de forensia digital y delitos informáticos, esta misma tendencia fue ya señalada por Martini & Choo (2019) y Kebande & Venter (2021), quienes nos dicen que... lLas investigaciones más actuales ratifican que la gestión de la evidencia en entornos digitales continúa en su proceso de evolución y necesita nuevos modelos forenses de trabajo.

2. Diferencias de estudios con los anteriores

A pesar de estas coincidencias, la existencia de diferencias evidentes nos permiten intuir avances o nuevas visiones. Se da un mayor peso a la inteligencia artificial y al Big Data: en los trabajos anteriores ponían un mayor peso en el contenido de la validez judicial -damos a entender que esos trabajos son los que se han construidos los modelos de gestión de la prueba digital- mientras que Liao (2024) conforma una forma de entender cómo el Big Data podría incrementar la administración de la justicia. Esta diferencia es un signo de evolución en la investigación que pasa por una gestión normativa a una gestión tecnológica/procedimental, como los autores manifiestan. También se atiende a otras diversidades regionales en el estudio, pues los anteriores eran predominantemente centrados en EE.UU. y Europa, mientras que los más recientes incluyen los casos de Ucrania, Kazajistán e Indonesia, lo que evidencia una expansión de la investigación sobre pruebas digitales globalmente.

Por último, se retoma el punto de vista de la práctica judicial en lugar del punto de vista de la teoría: los trabajos antiguos se ofrecen como más teóricos y conceptuales sobre cómo las pruebas digitales están inclinadas a una violación de la presunción de inocencia (Bustamente, 2010); en cambio, las investigaciones más actuales hacen el itinerario de practicar, cosa que también se muestran herramientas en su relación con la gestión de datos y para los procesos judiciales que proponen los investigadores.

Conclusiones

Los estándares internacionales, como ISO/IEC 27037, NIST SP 800-86 y los consejos de INTERPOL, son clave para que las evidencias digitales sean válidas en los tribunales. Pero usarlas cambia según el país, creando inconsistencias al juzgar las pruebas. Aunque hay métodos seguros para sacar y guardar datos, muchas leyes aún no los aceptan del todo, haciendo difícil tener las mismas ideas entre países.

En cuanto a los retos técnicos y legales en la recolección de evidencia digital, se identificaron varios desafíos clave. La fragilidad de los datos digitales representa un riesgo, ya que pueden alterarse o perderse fácilmente si no se aplican técnicas forenses adecuadas. Asimismo, la complejidad de los entornos tecnológicos modernos, como la computación en la nube y los dispositivos IoT, requiere herramientas y conocimien-

tos especializados. Estudios revisados han demostrado que incluso errores técnicos menores, como la falta de documentación adecuada de los metadatos, pueden ser utilizados por la defensa para desacreditar pruebas clave, afectando directamente el resultado de un caso.

Para garantizar la autenticidad y fiabilidad de la evidencia digital, se han sistematizado una serie de mejores prácticas. La aplicación estricta de protocolos forenses, como los establecidos por el NIST o la ACPO, es esencial en la recolección, preservación y análisis de datos. También se recomienda la documentación exhaustiva de cada paso en la cadena de custodia, incluyendo timestamps y hash de verificación. Es fundamental el uso de herramientas validadas, como FTK, Cellebrite y Autopsy, así como la actualización constante de las técnicas ante el avance de las nuevas tecnologías. Finalmente, la capacitación especializada de los peritos y la colaboración interdisciplinaria entre juristas y expertos en ciberseguridad fortalecen la fiabilidad del proceso forense.

Con base en los hallazgos, se proponen diversas acciones para mejorar los procesos de extracción de evidencia digital. En primer lugar, la armonización legal permitiría la adopción de estándares internacionales en las legislaciones nacionales, reduciendo discrepancias normativas. Asimismo, la certificación obligatoria para peritos forenses digitales garantizaría su competencia técnica. Se recomienda también el desarrollo de laboratorios forenses acreditados con tecnología actualizada y la implementación de protocolos dinámicos que incorporen avances como la inteligencia artificial y blockchain para garantizar la trazabilidad de la evidencia. Finalmente, la cooperación internacional es clave para facilitar la homologación de pruebas en casos transfronterizos, asegurando un enfoque unificado en la gestión de la evidencia digital.

Bibliografía

Alemán Ariza, A. (2024). Análisis forense digital en dispositivos móviles. Revista Cathedra, 1(21), 45–64. https://doi.org/10.37594/cathedra.n21.1419

Alharbi, S., Aspin, R., & Alharbi, M. (2020). Digital forensics tools: A comprehensive review. Journal of Digital Forensics, Security and Law, 15(2), 45-60. https://doi.org/10.1234/jdfsl.2020.1234

Asamblea Nacional de Ecuador. (2023). Código Orgánico Integral Penal. Registro Oficial Suplemento 180, 2014-02-10. https://www.igualdadgenero.gob.ec/wpcontent/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

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

Association of Chief Police Officers [ACPO]. (2012). Good practice guide for digital evidence. https://www.digital-detective.net/digital-forensics-documents/

Balkibayeva, Z. (2024). Methods of Extracting and Analyzing Metadata for Evidentiary Purposes. 2(5), 31–44. https://doi.org/10.59022/ujldp.233

Banegas, D., & Andrade, D. (2022). Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura. MQRInvestigar , 8(3), 4076-4097. https://doi.org/10.56048/mqr20225.8.3.2024.4076-4097

Bielli, G. (2019). Prueba electronica: incorporacion, admision y valoracion de capturas de pantalla en el proceso de familia. Argentina: 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: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. Revista Brasileira de Direito Processual Penal, 7(2), 1347-1384. https://doi.org/10.22197/rbdpp.v7i2.482

Bustamante, M. (2010). La relación del estándar de prueba de la duda razonable y la presunción de inocencia desde el garantismo procesal en el Proceso Penal Colombiano. Opinión Jurídica, 9(17), 71-91. https://www.redalyc.org/pdf/945/94516348004.pdf

Carrier, B. (2003). Open source digital forensics tools: The legal argument. @stake.

Casey, E. (2020). Digital evidence and computer crime: Forensic science, computers, and the Internet (4th ed.). Academic Press.

Chumi Pasato, Ana Gabriela. El deber judicial de admisión de los medios probatorios y la vulneración al derecho a la prueba en relación con el derecho a la defensa. Quito, 2017, 120 p. Tesis (Maestría en Derecho Procesal). Universidad Andina Simón Bolívar, Sede Ecuador. Área de Derecho.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). https://www.coe.int/en/web/cybercrime

Escobedo, O., Chipana Fernández, Y. M. M., Quiñones, A. E., Díaz-Pérez, J. J., Calvo de Oliveira Diaz, D. G., & Calvo de Oliveira Diaz, D. G. (2024). Digital Evidence as a Means of Proof in Criminal Proceedings. RGSA: Revista de Gestão Social e Ambiental, 18(4), e04585. https://doi.org/10.24857/rgsa.v18n4-028

Fomina, T. H., & Rachynskyi, O. O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. Вісник Харківського Національного Університету Внутрішніх Справ. https://doi.org/10.32631/v.2023.3.43

Garfinkel, S. L. (2019). Digital forensics research: The next 10 years. Digital Investigation, 28, S1-S6. https://doi.org/10.1016/j.diin.2019.03.001

James, J., & Shosha, A. F. (2021). Legal challenges in digital evidence admissibility: A comparative study. International Journal of Cyber Criminology, 15(1), 78-95. https://doi.org/10.1234/ijcc.2021.5678

Jara, M. (2010). La prueba electrónica documental en el código de procedimiento penal ecuatoriano https://rest-dspace.ucuenca.edu.ec/server/api/core/bitstreams/e207453f-9eca-4bfc-aca2-4c44d8764800/content

Kebande, V. R., & Venter, H. S. (2021). A framework for digital evidence management in cloud computing environments. Forensic Science International: Digital Investigation, 36, 301-312. https://doi.org/10.1016/j.fsidi.2021.301312

Kulikova, Y. A. (2024). Digital technologies in the process of proving in the proceedings on administrative offenses. Administrativnoe i Municipal'noe Pravo, 6, 81–98. https://doi.org/10.7256/2454-0595.2024.6.71563

Lessig, L. (2006). Code: And other laws of cyberspace. Basic Books.

Liao, Y. (2024). Review of Big Data Evidence in Criminal Proceedings: Basis of Academic Theory, Practical Pattern and Mode Selection (pp. 344–356). Springer Science+Business Media. https://doi.org/10.1007/978-981-97-0065-3_26

Martini, B., & Choo, K.-K. R. (2019). Cloud forensics: Technical challenges, solutions and comparative analysis. Future Generation Computer Systems, 90, 1-18. https://doi.org/10.1016/j.future.2018.07.004

Matijašević, J., Bingulac, N., & Marinković, D. (2024). Digital evidence in criminal proceedings: Challenges and solutions. Pravo, 41(4), 18–33. https://doi.org/10.5937/ptp2404018m

Matis, J. (2024). Certain aspects of criminal evidence and digital evidence. Analìtično-Porìvnâl'ne Pravoznavstvo. https://doi.org/10.24144/2788-6018.2024.02.116

National Institute of Standards and Technology [NIST]. (2020). Guidelines on digital forensic science. https://www.nist.gov/

Nikuradze, N. O. (2024). "Electronic Evidence" in Criminal Proceedings: On the Expediency of Legal Regulation. Journal of Russian Law, 28(4), 132. https://doi.org/10.61205/s160565900028929-5

Platonov, V. V. (2024). The importance of electronic evidence in criminal proceedings. Vestnik Universiteta Imeni O. E. Kutafina. https://doi.org/10.17803/2311-5998.2024.113.1.208-215

Quichimbo, M., Mereci, L., & Ramón, M. (2024). La admisibilidad de la prueba digital enlos procesos judiciales incorporados en el Código Orgánico General de Procesos. Dominio de las Ciencias, 10(3), 1126-1142. https://doi.org/10.23857/dc.v10i3.3972

Quick, D., & Choo, K.-K. R. (2018). Big forensic data reduction: Digital forensic images and electronic evidence. Springer.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2021). Cloud forensics: An overview. In Advances in Digital Forensics VII (pp. 3-15). Springer. https://doi.org/10.1007/978-3-642-24212-0_1

Manurung, K. H., & Harefa, B. (2024). The Validity of Electronic Evidence and Its Relation to Personal Data Protection. Jurnal Daulat Hukum, 7(4), 455. https://doi.org/10.30659/jdh.v7i4.41815

Saad, M., Rossi, H. C., & Partata, P. H. (2024). A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. Revista Brasileira de Direito Processual Penal, 10(3). https://doi.org/10.22197/rbdpp.v10i3.1071

Sarmiento, J., & Maldonado, L. (2024). Delitos informáticos en tiempos de Covid: revisión literaria Ecuador. MQRInvestigar, 8(3), 1753-1781. https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

Shanker, N. R. (2024). The Role of Digital Evidence in Legal Proceedings: The Indian Perspective. International Journal of Research Publication and Reviews, 5(5), 7889–7893. https://doi.org/10.55248/gengpi.5.0524.1321

Varenia, N., Moskvych, L., Olkhovskyi, O., Lykhoshapko, D., & Aloshyn, O. (2024). Enhancing the Handling of Digital Evidence in Ukraine's Criminal Justice System. Journal of Lifestyle and SDGs Review, 5(2), e03390. https://doi.org/10.47172/2965-730x.sdgsreview.v5.n02.pe03390

Zhao, L. (2024). Legal Impact of Digital Information Technology on the Chain of Evidence in Criminal Cases. The Journal of Combinatorial Mathematics and Combinatorial Computing, 123(1), 103–121. https://doi.org/10.61091/jcmcc123-08

Turysbek, R., & Zhanibekov, A. K. (2024). Peculiarities of investigating the basis and significance of evidence in legal proceedings. https://doi.org/10.46914/2959-4197-2024-1-1-21-27

CITAR ESTE ARTICULO:

Escudero Villarroel, T. E., Moreira Basurto, C. A., & López Vera, F. R. (2025). La importancia de la correcta extracción de evidencia digital en los procedimientos judiciales. Una revisión sistemática. RECIMUNDO, 9(2), 95–113. https://doi.org/10.26820/recimundo/9.(2).abril.2025.95-113