

Innovaciones

tecnológicas y su impacto en el proceso judicial.

Technological innovations and their impact on the judicial process.

Recibido: 30/04/25

Aceptado: 08/05/25

Publicado: 13/05/25

Paúl Orlando Piray Rodríguez^{1*}

E-mail: ur.paulpr13@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0003-4600-7999>

Evelyn Nayelli Santiago Basantes¹

E-mail: evelynsb76@uniandes.edu.ec

ORCID: <https://orcid.org/0009-0000-6640-4006>

Brayan Gabriel Taday Guamán¹

E-mail: brayantg95@uniandes.edu.ec

ORCID: <https://orcid.org/0009-0000-0426-5864>

Carlos Daniel Siza Pillajo¹

E-mail: dr.carlosdsp07@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0002-8457-7012>

¹Universidad Regional Autónoma de Los Andes, Riobamba, Ecuador.

*Autor para correspondencia.

Cita sugerida (APA, séptima edición)

Piray Rodríguez, P. O., Santiago Basantes, E. N., Taday Guamán, B. G., y Siza Pillajo, C. D. (2025). Innovaciones tecnológicas y su impacto en el proceso judicial. *Revista Científica Cultura, Comunicación y Desarrollo*, 10, e749. <http://rccd.ucf.edu.cu/index.php/rccd/article/view/749>

RESUMEN

La evolución tecnológica ha transformado la gestión de pruebas digitales en el ámbito judicial, al generar tanto oportunidades como desafíos relacionados con la autenticidad y validez de las evidencias. Por ello, el presente estudio se ha orientado en analizar el impacto de estas tecnologías en la gestión y autenticidad de las pruebas digitales, al destacar las oportunidades, los desafíos y la necesidad de una adaptación normativa para garantizar su validez. Para ello, se realizó una revisión de la literatura y un análisis de casos, al complementarlo con el uso del método RAFSI-AHP de Saaty, a fin de evaluar y priorizar los riesgos asociados a la manipulación y alteración de evidencias digitales. Los resultados obtenidos mostraron que la integración de tecnologías avanzadas, como blockchain, inteligencia artificial y criptografía, ha mejorado la verificación y preservación de las pruebas. Sin embargo, también se identificaron barreras regulatorias y desafíos técnicos, como la generación de deepfakes y los sesgos en los modelos de análisis, que afectan la autenticidad de las evidencias. Se concluyó que la adopción de soluciones digitales y la actualización de los marcos normativos son fundamentales para garantizar la integridad y validez de las pruebas digitales. Así como la prioridad de capacitar a los actores judiciales y fomentar la cooperación internacional para enfrentar los desafíos emergentes en el entorno digital.

Palabras clave:

Derecho, Innovaciones tecnológicas, Evidencia digital, Transparencia judicial.

ABSTRACT

Technological evolution has transformed the management of digital evidence in the judicial field, generating both opportunities and challenges related to the authenticity and validity of evidence. Therefore, this study has focused on analyzing the impact of these technologies on the management and authenticity of digital evidence, by highlighting the opportunities, challenges and the need for regulatory adaptation to guarantee its validity. To this end, a literature review and case analysis were carried out, complemented with the use of Saaty's RAFSI-AHP method, in order to evaluate and prioritize the risks associated with the manipulation and alteration of digital evidence. The results obtained showed that the integration of advanced technologies, such as blockchain, artificial intelligence and cryptography, has improved the verification and preservation of evidence. However, regulatory barriers and technical challenges were also identified, such as the generation of deepfakes and biases in analysis models, which affect the authenticity of the evidence. It was concluded that the adoption of digital solutions and the updating of regulatory frameworks are essential to ensure the integrity and validity of digital evidence. As well as the priority of training judicial actors and promoting international cooperation to face emerging challenges in the digital environment.

Keywords:

Law, Technological innovations, Digital evidence, Judicial transparency.

INTRODUCCIÓN

La transformación digital ha redefinido la naturaleza de las pruebas judiciales al incorporar evidencias en formatos electrónicos (Alcocer-Proañó y Batista-Hernández, 2024) (Revilla y Ajila, 2024). Tradicionalmente, la veracidad de las pruebas se garantizaba mediante métodos convencionales, pero la irrupción de la inteligencia artificial (IA) ha generado nuevos desafíos (Ventura-González y Robles-Pagador, 2024). Aunque la IA facilita la recopilación y análisis de grandes volúmenes de datos, también ha dado lugar a tecnologías que permiten la manipulación casi imperceptible de contenido audiovisual, al comprometer la autenticidad y fiabilidad de las pruebas presentadas en los tribunales.

Por otra parte, las pruebas digitales, que incluyen correos electrónicos, registros electrónicos y archivos multimedia, han adquirido un papel crucial en el ámbito judicial (Avila Contreras et al., 2024) (Loján, 2024). Sin embargo, su manipulación y evaluación requieren metodologías especializadas para garantizar su integridad y admisibilidad legal. Este escenario exige la adaptación de normativas y procedimientos tradicionales para abordar las particularidades de la evidencia digital, al asegurar su correcta recolección, preservación y análisis (Cueva y de la Torre, 2024) (Vaca y Dulce-Villarreal, 2024).

De hecho, el valor de la prueba digital radica en su capacidad para reflejar con precisión hechos y comportamientos en tiempo real (Roman et al., 2024) (Stoykova, 2024). No obstante, su fiabilidad enfrenta riesgos significativos, dada la facilidad con la que los datos son alterados, eliminados o manipulados (Santiago-Basantes et al., 2024). Por ende, el presente estudio tiene como objetivo analizar el impacto de la evolución tecnológica en el manejo, la evaluación de pruebas digitales en el entorno judicial y las principales teorías sobre su autenticidad. Para ello, se propone identificar las oportunidades, retos e implicaciones asociados con su integración, así como la necesidad de una adaptación normativa para garantizar su admisibilidad, autenticidad e integridad en el proceso judicial contemporáneo.

MATERIALES Y MÉTODOS

La investigación se desarrolló a partir de la revisión de la literatura sobre derecho digital y tecnología, al utilizar bases de datos académicas como SCOPUS, JSTOR y Google Scholar, y emplear palabras claves como "derecho digital", "blockchain", "deepfakes" y "pruebas digitales" (Zhang et al., 2023). Para ello, se priorizó la selección de estudios empíricos, teóricos actuales y relevantes (Song et al., 2024). Inclusive, se realizó un análisis de casos judiciales recientes relacionados con pruebas digitales, al utilizar el análisis de contenido cualitativo para evaluar cómo se presentaron y valoraron estas evidencias en los tribunales.

Método RAFSI-AHP de Saaty.

El método RAFSI (Ranking of Alternatives through Functional mapping of Similarity Indices) permiten identificar, evaluar y priorizar los retos e implicaciones asociados con la veracidad y la integridad de las pruebas digitales (Božanić et al., 2021). A continuación, se describe los pasos para su modelación (Irvanizam y Zahara, 2024):

- Identificación de los retos e implicaciones clave relacionados con las pruebas digitales en el ámbito judicial.
- Definición de criterios de evaluación: para evaluar cada reto o implicación, se deben establecer criterios de evaluación que permitan medir su impacto.
- Aplicación de comparaciones por pares: en este paso, se utiliza el Método AHP de Saaty para asignar pesos relativos a cada criterio mediante una matriz de comparación por pares (según la metodología consultada (Sarwar y Bashir, 2024) (Kumar et al., 2023) (Carra et al., 2023). Para ello, se realizan comparaciones entre los criterios, al utilizar una escala de 1 a 9, donde 1 indica igualdad de importancia y 9 denota una importancia extrema de un criterio sobre otro. De este modo, las comparaciones se agrupan en una matriz de evaluación que permite calcular los pesos de cada criterio.
- Normalización de la matriz de decisión: después de obtener las comparaciones por pares, se normalizan los valores para obtener una matriz de valoración de los retos y criterios. De hecho, se debe tener en cuenta que para elaborar la matriz de decisión se deben emplear los términos lingüísticos que se muestran en la tabla 1.

Tabla 1: Términos lingüísticos empleados para evaluar los retos e implicaciones.

Puntuación	Criterios					
	C1	C2	C3	C4	C5	C6
0.9	Alto	Frecuente	Alto	Alto	Mayor	Alto
0.6	Medio	Ocasional	Moderado	Medio	Moderado	Medio
0.3	Bajo	Raro	Bajo	Bajo	Menor	Bajo

Fuente: Elaboración propia.

- Cálculo de la puntuación global: La puntuación global de cada reto o implicación se calcula mediante la fórmula de suma ponderada (ver ecuación 1). Este paso genera una puntuación global para cada reto, al priorizar aquellos que tienen un mayor impacto en la veracidad y autenticidad de las pruebas digitales.

$$S_i = \sum_{j=1}^n w_j \cdot n_{ij} \quad (1)$$

- Donde S_i es la puntuación global de cada reto e implicación ii y w_j es el peso del criterio ii (al indicar la importancia relativa del criterio), y n_{ij} es el valor normalizado de la alternativa ii bajo el criterio jj .
- Análisis de resultados y priorización de retos e implicaciones: Una vez calculadas las puntuaciones globales de cada reto, se realiza un análisis de resultados para identificar cuáles son los retos más significativos. La priorización de los retos se basa en las puntuaciones globales, al permitir a los responsables del sistema judicial enfocar sus esfuerzos en los desafíos más críticos.
- Aplicación de voto por consenso: En caso de discrepancias en la evaluación, se aplica un voto por consenso entre los expertos para asegurar que los resultados reflejan el acuerdo colectivo sobre la importancia de los retos e implicaciones. Este paso mejora la fiabilidad del proceso, al evitar sesgos y garantizar que las decisiones reflejan un juicio colectivo de expertos.

RESULTADOS-DISCUSIÓN

Principales corrientes teóricas sobre la autenticidad de las pruebas judiciales.

En el campo de las pruebas digitales, varias teorías han emergido para garantizar su autenticidad y validez. La Teoría de la Cadena de Custodia destaca la necesidad de mantener y registrar el control de las pruebas desde su recolección hasta su presentación en el tribunal. Este proceso es esencial para evitar que las pruebas sean alteradas, al asegurar su admisibilidad en juicio.

Otra teoría relevante es la de la Preservación de Datos, que acentúa la necesidad de mantener la integridad de los datos digitales mediante técnicas como la creación de copias forenses exactas y el cifrado. El almacenamiento seguro y los controles de acceso juegan un papel fundamental en

la prevención de alteraciones no autorizadas. Asimismo, la tecnología de cadena de bloques (blockchain) ha emergido como una herramienta prometedora para garantizar la inmutabilidad y trazabilidad de las pruebas digitales. De modo que proporciona un registro transparente y verificable de cada paso en el manejo de las pruebas.

Avances recientes en el campo de la era digital.

El desarrollo de nuevas herramientas y software especializados ha permitido mejorar la capacidad de los analistas forenses para examinar y recuperar datos de diversas fuentes. Herramientas como Magnet AXIOM y X1 Social Discovery facilitan el análisis de datos provenientes de dispositivos móviles, redes sociales y sistemas en la nube. Estas innovaciones también permiten la recuperación de datos eliminados y la reconstrucción de archivos dañados, al optimizar el análisis forense en grandes volúmenes de datos.

Por otra parte, los avances en métodos de verificación, como el uso de algoritmos de hash criptográfico y análisis de metadatos, han mejorado la autenticidad de las pruebas digitales. Estos métodos ayudan a garantizar que los datos no hayan sido alterados y proporcionan una verificación continua durante el proceso de recolección y análisis.

Además, la incorporación de Inteligencia Artificial (IA) y Machine Learning (ML) ha transformado el análisis forense digital. Estas tecnologías permiten detectar patrones y anomalías en grandes conjuntos de datos que serían difíciles de identificar mediante métodos tradicionales. No obstante, su implementación plantea retos e implicaciones que deben ser gestionados cuidadosamente para asegurar que los resultados sean justos y confiables.

Retos e implicaciones en la veracidad de las pruebas digitales.

La incorporación de las pruebas digitales en los procesos judiciales ha transformado sustancialmente la administración de justicia, pero también ha introducido retos significativos, en particular en relación con la veracidad de dichas pruebas. A continuación, se identifican los principales retos e implicaciones asociados a la autenticidad y fiabilidad de las pruebas digitales, al establecer además los criterios de medición que determinan su impacto y grado de incidencia en el proceso judicial (ver tabla 2 y 3).

Tabla 2: Retos e implicaciones para la veracidad de las pruebas digitales.

Elemento	Reto/implicación	Descripción
RI-1	Manipulación y alteración de las pruebas	La facilidad con la que las pruebas digitales son alteradas o manipuladas representa un riesgo significativo para su integridad y autenticidad.
RI-2	Preservación de la integridad de las pruebas	La preservación de las pruebas digitales requiere el uso de metodologías, como la creación de copias forenses exactas, para evitar alteraciones durante su almacenamiento y transporte.
RI-3	Autenticidad de los datos	La autenticidad de las pruebas digitales debe ser garantizada mediante la validación de su origen, al asegurar que los datos no han sido modificados o falsificados antes de ser presentados en los tribunales.

RI-4	Uso indebido de la evidencia digital	El riesgo de que se reúnan pruebas sin seguir los procedimientos legales adecuados, como el acceso no autorizado a dispositivos o plataformas, compromete la validez de la evidencia.
RI-5	Interoperabilidad de herramientas forenses	Las herramientas forenses no siempre están diseñadas para trabajar juntas de manera eficiente, al generar inconsistencias en los análisis de las pruebas digitales.
RI-6	Desafíos asociados al almacenamiento en la nube	El uso de plataformas de almacenamiento en la nube plantea riesgos relacionados con el acceso no autorizado, la jurisdicción y la integridad de los datos almacenados en estos entornos.
RI-7	Obsolescencia tecnológica	La rápida evolución de las tecnologías hace que los dispositivos y los formatos de almacenamiento se vuelvan obsoletos. De modo que complican el acceso y la validez de las pruebas digitales a lo largo del tiempo.
RI-8	Impacto de los deepfakes	El uso de tecnologías de deepfake compromete la autenticidad de las pruebas, ya que permite crear contenidos falsificados altamente realistas, al representar un reto significativo para la veracidad de las pruebas.
RI-9	Desafíos éticos de la inteligencia artificial (IA) y machine learning (ML)	Las tecnologías de IA y ML, si bien mejoran la eficiencia en el análisis de grandes volúmenes de datos, presenta problemas éticos, como sesgos en los algoritmos y falta de transparencia, al afectar la fiabilidad de las conclusiones.
RI-10	Protección de los derechos digitales de los acusados	El manejo de pruebas digitales debe garantizar que se respeten los derechos fundamentales de los individuos, en especial en lo relacionado con la privacidad y la protección de datos personales durante el proceso judicial.
RI-11	Entorno cultural y social en la interpretación de pruebas	Las pruebas digitales se encuentran sujetas a diferentes interpretaciones según el entorno cultural o social de los usuarios involucrados, al complicar la validación y autenticidad de dichas pruebas en los tribunales.

Fuente: Elaboración propia.

Tabla 3: Criterios para medir los retos e implicaciones de las pruebas digitales en el ámbito judicial.

Código	Nombre del criterio	Descripción del criterio	Rangos de medición
C1	Impacto en la integridad de las pruebas	Evalúa cómo un riesgo afecta la autenticidad y la inalterabilidad de las pruebas digitales en el proceso judicial.	Bajo, medio, alto
C2	Probabilidad de manipulación o alteración	Determina la probabilidad de que las pruebas digitales sean manipuladas o alteradas antes de ser presentadas en los tribunales.	Rara, ocasional, frecuente
C3	Costo de mitigación del riesgo	Estima el gasto necesario para implementar medidas de seguridad y procedimientos que aseguren la validez de las pruebas.	Bajo, moderado, alto
C4	Probabilidad de falsificación de pruebas digitales	Mide la probabilidad de que las tecnologías emergentes alteren o falsifiquen contenido digital utilizado como prueba.	Bajo, medio, alto
C5	Impacto en la confianza pública	Considera el efecto de los riesgos sobre la percepción pública de la justicia y la confianza en la veracidad de las pruebas digitales.	Menor, moderado, mayor
C6	Cumplimiento normativo y legal	Evalúa el riesgo de incumplimiento de las normativas legales y estándares internacionales relacionados con la recolección y manejo de pruebas digitales.	Bajo, medio, alto

Fuente: Elaboración propia.

Modelación del método RAFSI-AHP de Saaty.

Para garantizar un análisis estructurado y objetivo de los retos e implicaciones asociados a la autenticidad y fiabilidad de las pruebas digitales, se empleó la modelación del método AHP de Saaty. De modo que permite establecer una jerarquización de criterios mediante comparaciones por pares, al asignar pesos (w) relativos a cada factor identificado (ver tabla 4 y 5).

Tabla 4: Matriz normalizada.

Criterio	C1	C2	C3	C4	C5	C6	PESO
C1	0.38	0.56	0.38	0.25	0.21	0.26	0.34
C2	0.13	0.19	0.38	0.25	0.21	0.26	0.24
C3	0.13	0.06	0.13	0.25	0.21	0.26	0.17
C4	0.13	0.06	0.04	0.08	0.07	0.09	0.08
C5	0.13	0.06	0.04	0.08	0.07	0.03	0.07
C6	0.13	0.06	0.04	0.08	0.21	0.09	0.10

Fuente: Elaboración propia.

Tabla 6: Matriz de decisión inicial.

Elemento	C1	C2	C3	C4	C5	C6
RI-1	Alto	Frecuente	Alto	Alto	Alto	Medio
RI-2	Alto	Ocasional	Moderado	Medio	Moderado	Alto
RI-3	Alto	Ocasional	Alto	Alto	Medio	Alto
RI-4	Medio	Frecuente	Moderado	Medio	Alto	Alto
RI-5	Medio	Ocasional	Moderado	Bajo	Moderado	Medio
RI-6	Alto	Frecuente	Alto	Alto	Mayor	Alto
RI-7	Medio	Raro	Bajo	Medio	Moderado	Bajo
RI-8	Alto	Frecuente	Alto	Alto	Mayor	Alto
RI-9	Medio	Ocasional	Moderado	Medio	Moderado	Medio
RI-10	Bajo	Ocasional	Bajo	Bajo	Alto	Medio
RI-11	Medio	Raro	Bajo	Bajo	Moderado	Bajo

Fuente: Elaboración propia.

Tabla 7: Matriz normalizada.

Elemento	C1	C2	C3	C4	C5	C6
w	0.34	0.24	0.17	0.08	0.07	0.10
RI-1	0.34	0.24	0.17	0.08	0.07	0.05
RI-2	0.34	0.12	0.09	0.04	0.00	0.10
RI-3	0.34	0.12	0.17	0.08	0.00	0.10
RI-4	0.17	0.24	0.09	0.04	0.07	0.10
RI-5	0.17	0.12	0.09	0.00	0.00	0.05
RI-6	0.34	0.24	0.17	0.08	0.07	0.10
RI-7	0.17	0.00	0.00	0.04	0.00	0.00
RI-8	0.34	0.24	0.17	0.08	0.07	0.10
RI-9	0.17	0.12	0.09	0.04	0.00	0.05
RI-10	0.00	0.12	0.00	0.00	0.07	0.05
RI-11	0.17	0.00	0.00	0.00	0.00	0.00

Fuente: Elaboración propia.

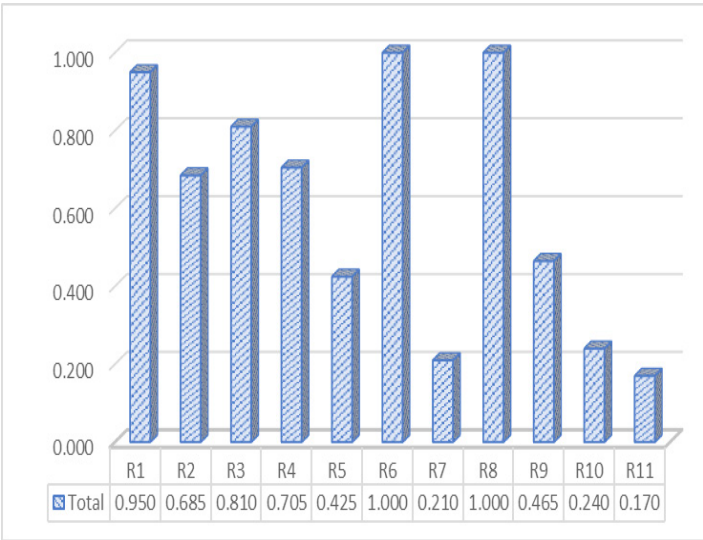
Tabla 5: Análisis de la consistencia del ejercicio.

Criterio		Valores propios aproximados	Valor propio= 6.4923563 IC=0.10 RC=0.08<=0.10 Consistente
C1	2.32	6.817082583	
C2	1.62	6.864170066	
C3	1.12	6.42897966	
C4	0.50	6.354467927	
C5	0.43	6.266836086	
C6	0.64	6.222601765	

Fuente: Elaboración propia.

Los pesos calculados reflejan la importancia relativa de cada criterio en la evaluación de los riesgos e implicaciones de las pruebas digitales en el ámbito judicial. Por otro lado, el análisis de la consistencia del método, se obtuvo un RC de 0.8, por tanto, se validan los datos en la modelación. Una vez definido los pesos, se procede a la modelación del método RAFSI. Para ello, se definen la matriz de decisión y normalizada (Ver tabla 6 y 7), así como la puntuación global de cada reto e implicación (ver figura 1).

Fig. 1: Puntuación global para los retos e implicaciones.



Fuente: Elaboración propia.

En la figura 1 se muestra que los retos con mayor puntuación global se centran principalmente en aspectos que afectan la autenticidad y la integridad de las pruebas digitales, que son fundamentales para garantizar la veracidad en el sistema judicial. Estos retos e implicaciones se destacan por los siguientes motivos:

- Almacenamiento en la nube: La complejidad de gestionar datos distribuidos globalmente y la falta de control efectivo sobre el almacenamiento en la nube genera

un alto riesgo de alteración o acceso no autorizado, al comprometer la veracidad de las pruebas almacenadas en la nube.

- Manipulación y alteración de las pruebas: Cualquier modificación no autorizada de las pruebas digitales invalida su valor como evidencia en un juicio, al afectar directamente el principio de justicia. La facilidad de alteración en los datos digitales y la falta de mecanismos de detección efectivos explican su alta prioridad en la matriz.
- Tecnologías emergentes (Deepfakes): Dado que los deepfakes crean falsificaciones de alta calidad de contenido visual y auditivo, este reto resalta la vulnerabilidad de las pruebas digitales, en particular en casos donde las pruebas audiovisuales son claves. La capacidad de falsificación ha desbordado la capacidad de verificación actual, al plantear un riesgo directo para la fiabilidad del sistema judicial.

En conjunto, estos retos reflejan las vulnerabilidades críticas que existen en la gestión de pruebas digitales en el entorno judicial contemporáneo. Al abordarlos adecuadamente es crucial para garantizar que las pruebas digitales sean fiables, legítimas y transparentes, al permitir que el sistema judicial mantenga su integridad. Por tanto, se proponen las siguientes acciones para mitigar el impacto de los retos e implicaciones identificados (ver tabla 8). De hecho, se deben tener como prioridad los retos e implicaciones de mayor puntuación global, identificados en la modelación.

Tabla 8: Acciones para mitigar el impacto de los retos e implicaciones en la veracidad de las pruebas digitales.

Elemento	Acción	Responsable	Impacto esperado
RI-1	Implementar sistemas de autenticación y trazabilidad de las pruebas digitales, como algoritmos de hash criptográfico y firmas digitales.	Instituciones Judiciales, Equipos Forenses	Asegura la integridad de las pruebas digitales y evita su alteración antes del juicio.
RI-2	Desarrollar protocolos de cadena de custodia digital que garanticen la conservación segura de las pruebas desde su recolección hasta su presentación.	Instituciones Judiciales, Peritos Forenses	Mejora la fiabilidad de las pruebas, al asegurar su conservación sin alteraciones.
RI-3	Aplicar herramientas avanzadas de verificación, como análisis de metadatos y algoritmos de detección de alteraciones.	Peritos Forenses, Tecnologías de Información	Verificación de la autenticidad de las pruebas antes de su presentación judicial.
RI-4	Establecer regulaciones más estrictas sobre el acceso a pruebas digitales y la capacitación en manejo adecuado de pruebas.	Instituciones Judiciales, Agencias Reguladoras	Reduce el riesgo de acceso no autorizado y mejora el manejo ético de las pruebas.
RI-5	Desarrollar plataformas interoperables para la recolección, análisis y presentación de pruebas digitales entre diferentes entidades.	Empresas Tecnológicas, Organismos Judiciales	Mejora la eficacia y precisión en el análisis forense al unificar herramientas.
RI-6	Implementar políticas de cifrado de datos y acceso controlado en plataformas de almacenamiento en la nube.	Proveedores de Nube, Instituciones Judiciales	Asegura que los datos sean protegidos adecuadamente, al evitar accesos no autorizados.
RI-7	Establecer un plan de mantenimiento y actualización constante de los sistemas de almacenamiento y análisis forense digital.	Departamentos de TI Judicial, Proveedores de Tecnología	Evita la obsolescencia tecnológica, al asegurar la compatibilidad a largo plazo de las pruebas digitales.
RI-8	Desarrollar e implementar tecnologías de detección de deepfakes y contenidos sintéticos en el análisis forense.	Empresas Tecnológicas, Peritos Forenses	Facilita la detección de contenidos falsificados y protege la integridad de las pruebas audiovisuales.

RI-9	Establecer normativas éticas y garantizar transparencia algorítmica en los sistemas de IA utilizados para el análisis de pruebas.	Organismos Reguladores, Instituciones Judiciales	Mejora la fiabilidad y la justicia del proceso judicial, al evitar sesgos y falta de transparencia.
RI-10	Crear regulaciones claras para proteger la privacidad y el uso ético de las pruebas digitales personales.	Instituciones Judiciales, Abogados, Organismos no Gubernamentales	Garantiza el respeto a los derechos digitales y evita la violación de la privacidad en el proceso judicial.
RI-11	Capacitar a jueces y personal judicial en el contexto cultural de las pruebas digitales y su correcta interpretación.	Instituciones Judiciales, Académicos	Mejora la comprensión y el análisis de las pruebas digitales en diferentes contextos sociales y culturales.

Fuente: Elaboración propia.

DISCUSIÓN

El análisis de los resultados ha coincidido con estudios previos que han destacado la relevancia de la tecnología blockchain en la protección y verificación de pruebas digitales en el ámbito legal. Investigaciones recientes han confirmado que la utilización de mecanismos criptográficos ha reforzado la seguridad de la información, optimizado la trazabilidad y garantizado la inmutabilidad de los datos almacenados. Asimismo, se ha observado que el desarrollo de tecnologías basadas en redes neuronales profundas ha permitido la generación de contenido sintético altamente realista, conocido como deepfakes, al representar un desafío adicional para la integridad del sistema judicial. En consecuencia, se han reafirmado la necesidad de integrar soluciones digitales que aseguren la confiabilidad de los documentos en litigios y procesos judiciales.

Sin embargo, los resultados han mostrado que la implementación de estas tecnologías enfrenta barreras regulatorias y estructurales. La facilidad con la que se han manipulado imágenes, videos y audios ha comprometido la autenticidad de las evidencias presentadas en los tribunales, al generar incertidumbre en la administración de justicia. Asimismo, el uso de inteligencia artificial y aprendizaje automático en el análisis de datos forenses ha permitido mejorar la identificación de patrones y la detección de irregularidades. No obstante, estos avances han conllevado desafíos éticos y técnicos, tales como la opacidad en los algoritmos y los sesgos inherentes a los modelos utilizados, al afectar la objetividad de los resultados. En este sentido, la variabilidad en la aceptación legal de las pruebas digitales ha evidenciado la necesidad de armonizar los marcos regulatorios y actualizar los procedimientos tradicionales para facilitar la adopción de dichas tecnologías.

Por otro lado, se han evidenciado que la percepción de los actores judiciales requiere un mayor énfasis en la capacitación y en la implementación de normativas internacionales. La estandarización de protocolos forenses digitales ha permitido armonizar los procedimientos a nivel global y facilitar la cooperación entre jurisdicciones, al fortalecer la validez de las evidencias en litigios transnacionales. Asimismo, la aplicación rigurosa de estándares forenses y el desarrollo de marcos regulatorios han contribuido a minimizar el riesgo de manipulación y a garantizar que las pruebas sean admisibles en los tribunales. De este modo, la combinación de herramientas tecnológicas avanzadas con protocolos normativos adecuados ha demostrado ser esencial para preservar la transparencia, la trazabilidad y, en última

instancia, la confianza en la administración de justicia en el entorno digital actual.

CONCLUSIONES

La integración de tecnologías avanzadas, como blockchain e inteligencia artificial, ha demostrado ser fundamental para mejorar la seguridad, trazabilidad e inmutabilidad de las pruebas digitales en el ámbito judicial. Estos avances han ofrecido un marco para la protección de la integridad de la información, sin embargo, su implementación enfrenta desafíos regulatorios y estructurales que requieren atención urgente.

A pesar de los beneficios indiscutibles en la mejora de la fiabilidad de las pruebas, el uso de tecnologías emergentes como los deepfakes ha generado nuevas incertidumbres sobre la autenticidad de las evidencias presentadas en los tribunales. Este fenómeno acentúa la prioridad de desarrollar marcos normativos más actualizados que aborden las particularidades de las pruebas digitales y garanticen su validez.

El estudio ha puesto en evidencia la necesidad de la capacitación de los actores judiciales y la estandarización de protocolos forenses digitales para promover la cooperación internacional y minimizar el riesgo de manipulación de las pruebas. A medida que las tecnologías evolucionan, se hace imperativo el desarrollo de nuevos marcos regulatorios que aseguren la adopción eficiente y ética de estas herramientas en los procesos judiciales, tanto a nivel local como global.

REFERENCIAS BIBLIOGRÁFICAS

- Alcocer-Proañó, M. M., y Batista-Hernández, N. (2024). La garantía del debido proceso y la práctica de la prueba en las audiencias telemáticas. *Revista Metropolitana de Ciencias Aplicadas*, 7(3), 6-14. <http://remca.umet.edu.ec/index.php/REMCA/article/view/760>
- Avila Contreras, L. J., Serrano Campoverde, J. V., Escobar Jara, J. I., y Campos Cardenas, F. E. (2024). Eficacia de las pruebas electrónicas en el sistema judicial mediante criterios específicos de peritaje. *Serie Científica de la Universidad de las Ciencias Informáticas*, 17(11), 132-150. http://scielo.sld.cu/scielo.php?pid=S2306-24952024001100132&script=sci_abstract

- Božanić, D., Milić, A., Tešić, D., Salabun, W., y Pamučar, D. (2021). D NUMBERS – FUCOM – FUZZY RAFSI MODEL FOR SELECTING THE GROUP OF CONSTRUCTION MACHINES FOR ENABLING MOBILITY. *Facta Universitatis, Series: Mechanical Engineering*, 19(3), 447. <http://casopisi.junis.ni.ac.rs/index.php/FUMechEng/article/view/7578>
- Carra, M., Botticini, F., Filippo Carlo, P., Giulio, M., Pezzagno, M., y Barabino, B. (2023). A comparative cycling path selection for sustainable tourism in Franciacorta. An integrated AHP-ELECTRE method. *Transportation Research Procedia*, 69(February), 451-452. <https://www.sciencedirect.com/science/article/pii/S2352146523002041>
- Cueva, J. C. M., y de la Torre, G. L. G. (2024). Cadena de custodia: Valoración de prueba y tutela judicial efectiva en el procedimiento adversarial penal. *Ciencia Digital*, 8(2), 36-63. <https://www.cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/2966>
- Irvanizam, I., y Zahara, N. (2024). An improved RAFSI method based on single-valued trapezoidal neutrosophic number and its Harmonic and Arithmetic mean operators for healthcare service quality evaluation. *Expert Systems with Applications*, 248(August), 1-6. <https://www.sciencedirect.com/science/article/abs/pii/S0957417424002082>
- Kumar, R., Prinshu, Kumar Mishra, A., Dutta, S., y Kumar Singh, A. (2023). Optimization and prediction of response characteristics of electrical discharge machining using AHP-MOORA and RSM. *Materials Today: Proceedings*, 80(Part 1), 333-338. <https://www.sciencedirect.com/science/article/abs/pii/S2214785323006727>
- Loján, C. G. T. (2024). WhatsApp como herramienta de prueba en litigios por obligaciones financieras: Una mirada al sistema judicial ecuatoriano. *Revista Lex*, 7(25), 496-511. <https://revistalex.org/index.php/revistalex/article/view/273>
- Revilla, J. A. I., y Ajila, L. A. A. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano. *Revista Lex*, 7(27), 1338-1350. <https://www.revistalex.org/index.php/revistalex/article/view/347>
- Roman, M. A. Q., Balcazar, L. S. M., y Merchán, M. E. R. (2024). La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos. *Dominio de las Ciencias*, 10(3), 1126-1142. <https://dominiodelasciencias.com/ojs/index.php/es/article/view/3972>
- Santiago-Basantes, E. N., Taday-Guamán, B. G., Paulan-Punguil, D. O., y Hernández-Ramos, E. L. (2024). Falsificación de pruebas a través de la inteligencia artificial [Falsification of evidence through artificial intelligence]. *Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales*, 3(especial4), 163-170. <https://www.revistasinstitutoperspectivasglobales.org/index.php/verdadyderecho/article/view/334>
- Sarwar, M., y Bashir, F. (2024). Design concept evaluation based on cloud rough model and modified AHP-VIKOR: An application to lithography tool manufacturing process. *Advanced Engineering Informatics*, 60(April), 102369. <https://www.sciencedirect.com/science/article/pii/S147403462400017X>
- Song, J., Chen, R., Wu, Z., Yin, Z., y Xu, M. (2024). A review of research methods for oil well cement corroded by carbon dioxide. *Geoenergy Science and Engineering*, 232(Part B, January), 1-5. <https://www.sciencedirect.com/science/article/pii/S2949891023010564>
- Stoykova, R. (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, 55(November), 1-14. <https://www.sciencedirect.com/science/article/pii/S0267364924001067>
- Vaca, P. A., y Dulce-Villarreal, E. R. (2024). Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático. *TecnoLógicas*, 27(60), e300. http://www.scielo.org.co/scielo.php?pid=S0123-77992024000200300&script=sci_arttext
- Ventura-González, C. I., y Robles-Pagador, M. E. (2024). Inteligencia artificial y la valoración de la prueba en el proceso penal peruano. *Cienciamatria. Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 10(19), 303-314. https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S2542-30292024000200303
- Zhang, C., Tian, L., y Chu, H. (2023). Usage frequency and application variety of research methods in library and information science: Continuous investigation from 1991 to 2021. *Information Processing and Management*, 60(6), 4-8. <https://www.sciencedirect.com/science/article/abs/pii/S0306457323002443>