Tipo de artículo: Artículo original

Eficacia de las pruebas electrónicas en el sistema judicial mediante criterios específicos de peritaje

Effectiveness of electronic evidence in the judicial system through specific expert criteria

Lida Jimena Avila Contreras [1*], https://orcid.org/0009-0001-6491-6240
José Vicente Serrano Campoverde [2], https://orcid.org/0009-0001-4531-4607
Johanna Irene Escobar Jara [3], https://orcid.org/0000-0002-9053-8060
Fátima Eugenia Campos Cardenas [4], https://orcid.org/0000-0003-4142-3010

[1] Universidad Bolivariana del Ecuador (UBE). Durán, Ecuador. Correo electrónico: ljavilac@ube.edu.ec
[2] Universidad Bolivariana del Ecuador (UBE). Durán, Ecuador. Correo electrónico: jvserranoc@ube.edu.ec
[3] Universidad Bolivariana del Ecuador (UBE). Durán, Ecuador. Correo electrónico: jiescobarj@ube.edu.ec
[4] Universidad Bolivariana del Ecuador (UBE). Durán, Ecuador. Correo electrónico: fecamposc@ube.edu.ec

*** Autor para correspondencia: ljavilac@ube.edu.ec**

Resumen

La creciente necesidad de pruebas digitales en el ámbito judicial es un fenómeno global que exige la implementación de un marco de preservación de pruebas electrónicas que sea confiable y efectivo. El correcto mantenimiento de la cadena de custodia es crucial para asegurar que se garantice la justicia en los tribunales. Sin embargo, es importante reconocer que los seres humanos representan el eslabón más vulnerable en cualquier cadena de confianza. En este contexto, la tecnología *blockchain* emerge como una solución prometedora para la preservación de pruebas electrónicas, especialmente en el ámbito del Internet de las Cosas (IoT). Blockchain permite almacenar y analizar datos de pruebas digitales de manera segura y confidencial, estableciendo un marco robusto de control de acceso que protege la integridad de la información. Al integrar esta tecnología en el proceso de gestión de evidencias, se puede minimizar el riesgo de manipulación y garantizar la trazabilidad y autenticidad de las pruebas, fortaleciendo así la confianza en el sistema judicial. En esta investigación se definió un conjunto de seis criterios específicos de peritaje para que sean incluidos en la normativa procesal ecuatoriana. Adicionalmente se propuso un marco de preservación de pruebas electrónicas basado en blockchain para el IoT que implementa la cadena de custodia y utiliza la plataforma *Ethereum* para resforzar los principios de descentralización y transparencia que son fundamentales para la tecnología *blockchain*. La viabilidad de la propuesta se realizó mediante criterio de expertos, la cual fue evaluada como muy pertinente.

Palabras clave: pruebas electrónicas; Ethereum; Blockchain; criterios específicos de peritaje

Abstract

The growing need for digital evidence in the judicial field is a global phenomenon that demands the implementation of a reliable and effective electronic evidence preservation framework. Correctly maintaining the chain of custody is crucial to ensure that justice is guaranteed in court. However, it is important to recognize that humans represent the most vulnerable link in any chain of trust. In this context, blockchain technology emerges as a promising solution for the preservation of electronic evidence, especially in the field of the Internet of Things (IoT). Blockchain allows digital evidence data to be stored and analyzed in a secure and confidential manner, establishing a robust access control framework that protects the integrity of the information. By integrating this technology into the evidence management process, the risk of manipulation can be minimized and the traceability and authenticity of evidence can be guaranteed, thus strengthening trust in the judicial system. In this research, a set of six specific

expert criteria were defined to be included in the procedural regulations. Additionally, a blockchain-based electronic evidence preservation framework for the IoT was proposed that implements the chain of custody and uses the Ethereum platform to reinforce the principles of decentralization and transparency that are fundamental to blockchain technology. The feasibility of the proposal was carried out through expert judgment, which was evaluated as very pertinent.

Keywords: *electronic evidence; Ethereum; Blockchain; specific expert criteria*

Recibido: 22/09/2024
Aceptado: 18/11/2024
En línea: 19/11/2024

Introducción

En la era digital actual, la integridad y la fiabilidad de las pruebas electrónicas son fundamentales en los procedimientos legales, las investigaciones penales y los incidentes de ciberseguridad. Sin embargo, la preservación y presentación de evidencia digital enfrenta varios desafíos significativos, dado que se debe garantizar la integridad, ya que cualquier alteración, incluso mínima, puede cuestionar su credibilidad y autenticidad a lo largo del proceso de investigación (Acosta-León, 2023). Además, autenticar pruebas electrónicas es complejo, dado que pueden ser manipuladas o falsificadas con facilidad, por lo que los tribunales requieren métodos confiables que demuestren su veracidad (Paredes & Paredes, 2022). Por último, la admisibilidad de estas pruebas en los tribunales depende del cumplimiento de estrictos requisitos legales; el incumplimiento puede resultar en la consideración de la evidencia como inadmisible.

La eficacia de las pruebas electrónicas en el sistema judicial ecuatoriano es un tema importante en el contexto actual ya que está marcado por el creciente uso de la tecnología y la necesidad de adaptar los sistemas legales a estas nuevas realidades. Los métodos tradicionales de almacenamiento y gestión de pruebas a menudo dan como resultado documentos que pueden alterarse fácilmente. La autenticidad, seguridad y trazabilidad de las pruebas electrónicas no solo dependen de una correcta interpretación normativa, sino también de la inclusión de criterios específicos de peritaje que garanticen la fiabilidad de estas evidencias.

La cadena de custodia desempeña un papel fundamental en este proceso, pero las personas son el eslabón más débil de cualquier cadena de confianza. La cadena de custodia se refiere al rastro documentado e ininterrumpido de personas que han tenido contacto con una pieza de evidencia desde el momento en que se recopila hasta que se presenta ante el tribunal (Al-Khateeb et al., 2019). Su propósito principal es garantizar que la evidencia permanezca intacta, inalterada y confiable durante todo su recorrido a través del sistema legal. La tecnología *blockchain* se puede utilizar para almacenar y analizar datos de pruebas digitales de forma segura y confidencial, con un control de acceso adecuado (Khan et al., 2021).

La incorporación de la tecnología *blockchain* en el ámbito de la investigación forense digital presenta oportunidades significativas para mejorar la autenticidad, el rastreo y la protección de las pruebas digitales (Lone & Mir, 2019). Sin embargo, es fundamental reconocer que la mera adopción de esta tecnología no garantiza resultados efectivos. Para maximizar su potencial, es esencial establecer criterios periciales específicos que guíen su implementación. Sin una definición clara de estos parámetros, la eficacia del sistema puede verse comprometida, lo que podría llevar a la desconfianza en los procesos de validación y en la integridad de las pruebas recolectadas. Por lo tanto, la combinación de *blockchain* con un marco regulatorio y metodológico bien definido es crucial para asegurar que esta herramienta innovadora cumpla su promesa en la mejora de la investigación forense digital.

El desarrollo de criterios periciales específicos es un tema que ha captado la atención de varios investigadores. (Shurson, 2020) destaca que, dentro del derecho comparado realizado con normativas de algunos países de la Unión Europea, estos han adoptado diversas estrategias para proteger las evidencias electrónicas, como procedimientos de validación rigurosos y tecnologías avanzadas de verificación. Esto se conecta con la argumentación de (Elyas et al., 2015), quien señala que la actualización constante de las prácticas periciales es indispensable para enfrentar los desafíos que presentan las tecnologías emergentes, como el Internet de las Cosas (IoT) y el blockchain (Li et al., 2019). De esta manera, se busca no solo proteger la integridad de las pruebas, sino también garantizar que estas cumplan con los estándares legales requeridos.

Sin embargo, en diversos sistemas judiciales, se han emitido fallos que cuestionan la eficacia de las pruebas electrónicas debido a preocupaciones sobre su autenticidad y fiabilidad (Fernández et al., 2022). Por ejemplo, en España, la Sentencia del Tribunal Supremo 300/2015 de 19 de mayo analizó la validez de una conversación en Tuenti, destacando la necesidad de certificar la autenticidad de las comunicaciones electrónicas para su admisibilidad como prueba (Bueno de Mata, 2015).

En el sistema judicial ecuatoriano, la admisibilidad y eficacia de las pruebas electrónicas han sido objeto de análisis en diversas resoluciones. Aunque no se dispone de un compendio específico de jurisprudencia que declare la ineficacia de la prueba electrónica, existen casos donde los tribunales han evaluado su validez y pertinencia. La situación actual en Ecuador, como señala (Lema Morocho, 2018), refleja la urgencia de estas reformas. El Código Orgánico General de Procesos (COGEP) no aborda de manera específica el tratamiento de pruebas electrónicas, lo que genera inseguridades jurídicas y posibles vulneraciones de derechos.

Basado en este escenario, en la presente investigación se define un conjunto de criterios de peritaje específicos para las pruebas electrónicas en la normativa ecuatoriana, siendo necesario proponer una modificación al artículo 195 del COGEP, que detalle los criterios específicos de peritaje. Con esta investigación se busca fortalecer la integridad y

fiabilidad del proceso judicial, proteger los derechos procesales de las partes involucradas e incentivar a proponer reformas normativas que modernicen el sistema legal ecuatoriano, posicionándolo a la vanguardia en la gestión de evidencias electrónicas. Con este fin, se realizó el siguiente marco de la investigación:

Problema de la investigación: ¿Cómo fortalecer la eficacia de las pruebas electrónicas en el sistema judicial ecuatoriano mediante la inclusión de criterios específicos de peritaje en la normativa procesal?

Hipótesis: La inclusión de criterios específicos de peritaje para la evaluación de pruebas electrónicas en la normativa procesal ecuatoriana causará un aumento en la autenticidad, seguridad y trazabilidad de estas pruebas, mejorando así su eficacia.

Objetivo general: Determinar cómo la inclusión de criterios de peritaje específicos en la normativa procesal ecuatoriana mejora la autenticidad, seguridad y trazabilidad de las pruebas electrónicas en el sistema judicial.

La investigación se desarrolló dentro de la provincia de Morona Santiago para examinar el desarrollo de la integración de la prueba electrónica dentro de los procesos judiciales.

Materiales y métodos

La implementación de un sistema de cadena de custodia basado en *blockchain* es una iniciativa esencial para las organizaciones que buscan fortalecer la integridad y la seguridad de las pruebas digitales. Este enfoque no solo mejora la trazabilidad y la autenticidad de las evidencias, sino que también aborda los desafíos asociados con la preservación y presentación de datos digitales en el ámbito judicial. A continuación, se presentan los pasos cruciales a seguir para llevar a cabo esta implementación de manera efectiva:

1. Selección de la plataforma *blockchain* adecuada: Es fundamental elegir una plataforma de *blockchain* que se adapte a las necesidades específicas de su organización y a la naturaleza de las evidencias digitales que se manejarán. Esta decisión impactará directamente en la eficiencia y eficacia del sistema.
2. Diseño de contratos inteligentes para el seguimiento de pruebas: Desarrollar contratos inteligentes es crucial, ya que estos son acuerdos que se ejecutan automáticamente mediante código. Estos contratos permitirán automatizar y garantizar el cumplimiento de las reglas que regulan la cadena de custodia, aumentando la confianza en el manejo de las evidencias.
3. Integración con herramientas forenses digitales existentes: Asegurar una integración fluida con las herramientas y software forenses que ya se utilizan es vital para facilitar la recolección y gestión de pruebas. Esta compatibilidad permitirá un flujo de trabajo más eficiente y efectivo en la preservación de la evidencia electrónica.

La cadena de custodia forma el vínculo forense de la secuencia de evidencia de control, transferencia y análisis para preservar la integridad de la evidencia y evitar su contaminación. *Blockchain* se puede aprovechar para ofrecer un sistema de evidencia digital seguro y descentralizado.

Para garantizar la seguridad de la informacion, se utilizará *Ethereum*. Ethereum es una plataforma de *blockchain* que permite la creación y ejecución de contratos inteligentes y aplicaciones descentralizadas (dApps). La custodia en la cadena de *Ethereum* se refiere a la capacidad de almacenar y gestionar activos digitales directamente en la *blockchain*, garantizando su seguridad y accesibilidad a través de claves criptográficas (Lone & Mir, 2018). Esta característica permite a los usuarios mantener un control total sobre sus activos sin depender de intermediarios, lo que refuerza los principios de descentralización y transparencia que son fundamentales para la tecnología *blockchain* y que son necesarios para la presente investigación.

Resultados y discusión

Tradicionalmente, la mayoría de los datos electrónicos se convierten en evidencia documental o se reconocen como otros tipos de evidencia, como material audiovisual para litigios. Los datos electrónicos no son confiables ante la corte, dado que se corrompen fácilmente y son expeditamente destructibles (Galvis & Bustamante 2019). La conversión de datos electrónicos en evidencia documentada socava el valor probatorio de los datos electrónicos, ya que la evidencia multimedia documentada no puede capturar con precisión el contenido de los datos electrónicos originales, los métodos de almacenamiento y otros elementos esenciales. En muchas situaciones, la mejora de los datos electrónicos no se reconoce como prueba admisible a efectos de procesamiento.

El proceso de investigación forense digital en el ámbito del Internet de las Cosas (IoT) se muestra en la figura 1. Este proceso se compone de diversas etapas fundamentales. Comienza con la identificación de los dispositivos y datos relevantes, seguido de la recopilación cuidadosa de la información necesaria. Una vez obtenidos, se procede a la preservación de la evidencia para garantizar su integridad. Posteriormente, se lleva a cabo un examen detallado de los datos, que culmina en un análisis exhaustivo para extraer conclusiones significativas. Los resultados se presentan a la corte de manera clara y concisa, facilitando su comprensión y uso en contextos legales o técnicos.

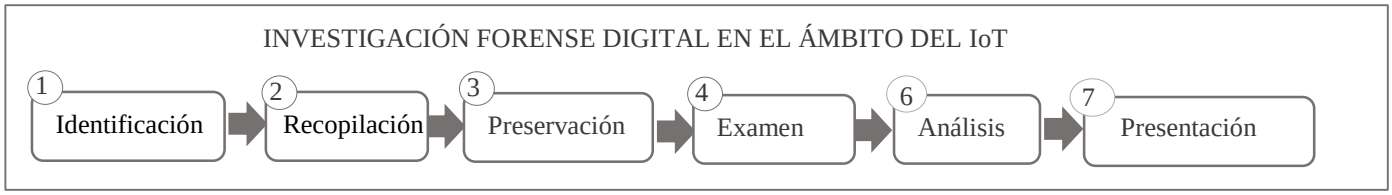

Figura 1. Proceso de investigación forense digital en el ámbito del Internet de las Cosas (IoT).

Dado que los dispositivos portátiles inteligentes contienen mucha información sobre los usuarios y las actividades que pueden utilizarse como evidencia multimedia digital, es crucial para resolver un caso criminal en la investigación digital de actividades delictivas o maliciosas. En la ciencia forense digital se generan varios casos en los que estos dispositivos actúan como evidencia útil para resolver una investigación forense digital. En la tabla 1 se ejemplifican diferentes dispositivos electrónicos y el tipo de prueba electrónica que pueden proporcionar en la resolución de un conflicto judicial:

Tabla 1. Tipos de pruebas electrónicas recuperadas de dispositivos digitales con IoT.

Dispositivo electrónico	Tipo de prueba electrónica aportada
Teléfono inteligente	Historial de llamadas, mensajes de texto, ubicación GPS
Tablet	Documentos, correos electrónicos y aplicaciones instaladas
Cámara de seguridad	Grabaciones de video que capturan eventos en tiempo real
Reloj inteligente	Datos de salud, como frecuencia cardíaca y patrones de actividad
Vehículo con sistema GPS	Rutas recorridas y datos de ubicación en tiempo real
Asistente de voz (Ej. Alexa)	Registros de comandos de voz y preguntas realizadas
Consola de videojuegos	Historial de juegos, interacciones en línea y chats de voz
Dispositivo de domótica	Registro de accesos y actividad en el hogar (puertas, luces)
Cámara de acción (Ej. GoPro)	Grabaciones de video que documentan actividades exteriores
Dron	Imágenes aéreas y grabaciones que pueden mostrar la escena del crimen

Esta tabla ilustra cómo distintos dispositivos pueden contribuir a la recopilación de pruebas electrónicas, lo que resulta fundamental en el proceso de investigación y resolución de delitos. Sin embargo, para que estas evidencias electrónicas sean admisibles en un tribunal, es crucial asegurar su integridad a través de un riguroso manejo de la cadena de custodia. Por ello, es fundamental establecer criterios de peritaje específicos dentro de la normativa del proceso ecuatoriano, lo cual contribuirá a mejorar la autenticidad, seguridad y trazabilidad de las pruebas digitales en el sistema judicial.

La ciencia forense digital se enfrenta a diversos desafíos, incluida la necesidad de un marco integrado para garantizar la preservación de las pruebas electrónicas, de manera que estas sean admisibles en los tribunales (Acosta-León, 2023). Un marco de este tipo debe cumplir varios requisitos, entre ellos: (1) la integridad de los datos, (2) la cadena de custodia, (3) las capacidades de auditoría y (4) la conservación de las pruebas.

La tecnología *blockchain* ofrece una posible solución a estos desafíos al permitir la verificación de la legalidad y la autenticidad de los métodos utilizados para la recopilación, el almacenamiento y la transferencia de pruebas electrónicas. Una *blockchain* es esencialmente una serie de estructuras de datos vinculadas conocidas como bloques, que se pueden utilizar para almacenar y monitorear el estado de los sistemas distribuidos en una red *peer to peer*. Cada

bloque está conectado a un bloque anterior llamado puntero *hash*, lo que da como resultado un historial permanente e irreversible que cualquier participante puede utilizar como un registro de auditoría en tiempo real para verificar la precisión de los registros con solo revisar los datos.

A partir de la evidencia recopilada, los autores de la presente investigación consideran que la modificación de las regulaciones actuales en el Ecuador, es crucial para incluir *Blockchain* y la IoT como parte de las infraestructuras de la ciencia forense digital. La tecnología blockchain se emplea para enfrentar diversos desafíos en la ciencia forense digital, ya que su diseño ofrece características como transparencia, autenticidad, seguridad y audibilidad. Estas cualidades la convierten en una herramienta valiosa para asegurar la cadena de custodia (CoC) de las pruebas electrónicas. Actualmente, se ha investigado su capacidad para verificar y almacenar evidencia digital, lo que la posiciona como un método prometedor en este campo.

Al desarrollar criterios específicos de peritaje para la evaluación de pruebas electrónicas en el contexto de la tecnología *blockchain*, es fundamental reconocer y abordar una serie de desafíos en distintos niveles, que pueden comprometer el proceso de recopilación y validación de evidencias. A continuación se presentan algunos de estos desafíos:

- Nivel de dispositivo: La recopilación de pruebas desde la memoria local de dispositivos IoT enfrenta dificultades como la variabilidad de las evidencias en comparación con las digitales tradicionales. La complejidad de la arquitectura informática, el uso de formatos específicos de proveedor y mecanismos de almacenamiento propietarios. Además, el almacenamiento limitado en los dispositivos puede reducir la cantidad de rastros digitales disponibles y aumentar el riesgo de pérdida de datos, lo que dificulta el mantenimiento adecuado de la cadena de custodia.
- Nivel de red: En este nivel, el análisis de las comunicaciones de los dispositivos IoT presenta retos como el incremento del tráfico de red cifrado y la utilización de múltiples protocolos. Esto requiere herramientas y software especializados, así como experiencia técnica adicional, complicando el proceso de recolección de evidencias.
- Nivel de nube: Cuando se busca recopilar datos de los servicios en la nube asociados a los dispositivos en investigación, se topa con desafíos significativos. La jurisdicción transfronteriza puede complicar la obtención de información, las evidencias pueden requerir mucho tiempo para ser recolectadas, los formatos de datos pueden ser diversos y los datos están distribuidos en múltiples capas.

Para superar estos desafíos, es esencial que los criterios de peritaje que se definan contemplen medidas específicas que faciliten la estandarización y la coherencia en la recopilación de evidencias, así como mecanismos claros de gestión de

la cadena de custodia. Esto no solo garantizará la integridad de las pruebas digitales, sino que también mejorará la eficacia del sistema judicial al manejar la complejidad inherente a las nuevas tecnologías.

Marco de preservación de pruebas electrónicas basado en *blockchain* para el IoT

El Internet de las cosas (IoT) ha hecho que las tareas cotidianas sean más eficientes gracias al uso de dispositivos inteligentes, que ahora forman parte integral de las rutinas diarias de las personas. Como resultado, ha habido un aumento en los servicios que admiten dispositivos inteligentes en diversas industrias, como la automatización del hogar, la atención médica y la agricultura, que requieren que los usuarios compartan su información personal. La cantidad de dispositivos inteligentes continúa creciendo, lo que aumenta la probabilidad de delitos digitales. La ciencia forense digital puede brindar una ventaja en la investigación de delitos relacionados con el IoT porque todos dejan rastros digitales.

El objetivo del marco de preservación de pruebas electrónicas basado en *blockchain* para el IoT que se propone en la presente investigación, es crear un entorno seguro que evite la manipulación de evidencia digital por parte de terceros hasta que se presente en el tribunal. El marco propuesto también mejora la transparencia y la rendición de cuentas en el examen forense de la prueba electrónica, lo que garantiza que se pueda confiar en los resultados de la investigación.

En la figura 2 se muestra la estructura general del marco de preservación de pruebas electrónicas basado en blockchain para el IoT, diseñado como soporte de la propuesta de modificación al artículo 195 del Código Orgánico General de Procesos de Ecuador:

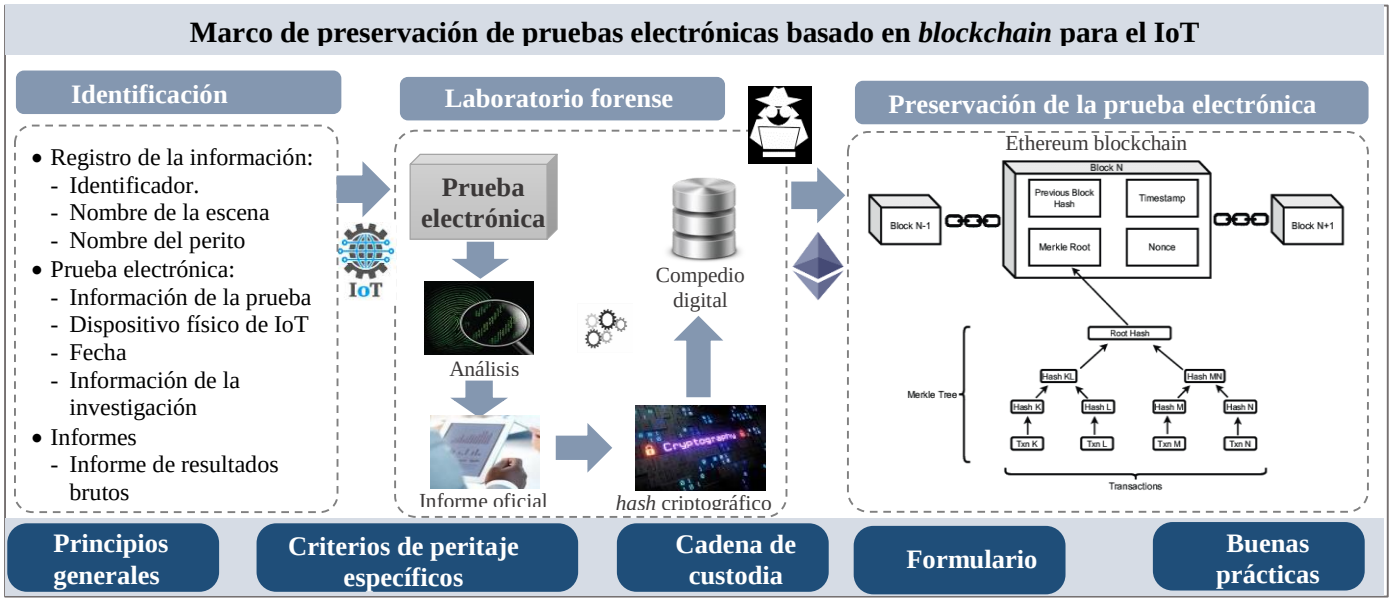

Figura 2. Marco de preservación de pruebas electrónicas basado en *blockchain* en Ecuador.

Gestión de evidencias de cadena de custodia basado en blockchain

La tecnología blockchain es empleada para almacenar metadatos de pruebas electrónicas mientras la evidencia se almacena en un medio de almacenamiento confiable. El marco está construido sobre una cadena de bloques Ethereum privada para documentar cada transmisión desde el momento en que se incauta la evidencia, lo que garantiza que solo las partes autorizadas puedan acceder o poseer la evidencia. El marco está integrado con el sistema de evidencia digital donde las pruebas electrónicas se almacenan físicamente y se bloquea mediante cerraduras inteligentes. Para asegurar la secuencia de envío y recuperación de evidencia, solo una parte autorizada puede poseer la clave para desbloquear la evidencia.

- **Recopilación de pruebas:**

La cadena de custodia comienza con la recopilación de pruebas. Esto incluye la identificación y el registro de la información relevante y su verificación con las fuentes adecuadas. Las pruebas relevantes pueden incluir:

Tabla 2. Componentes de la recopilación de pruebas electrónicas.

Tipo de evidencia digital	Evidencia física	Fuente de la evidencia
• Archivos de datos informáticos • Registros de cifrado • Correos electrónicos • Mensajes de texto • Inventarios de activos de TI • Grabaciones de audio y video • Archivos de registro informáticos • Informes de borrado de datos	• Activos informáticos y equipos informáticos relacionados • Componentes informáticos, discos duros y medios • Fotografías de equipos • Dispositivos IoT	• Integridad de la evidencia • El momento en que descubrió y obtuvo la evidencia • Ubicación de la evidencia • El estado de la evidencia

- **Formulario de Cadena de Custodia**

Los formularios de cadena de custodia son herramientas esenciales que proporcionan un registro permanente sobre la obtención, gestión y entrega de evidencia digital. Es fundamental que estos formularios se actualicen cada vez que una nueva persona tenga acceso para examinar o analizar la evidencia digital confidencial. El formulario de la cadena de custodia tiene tres propósitos principales: (1) hacer preguntas relevantes sobre la evidencia al laboratorio analítico; (2) mantener un registro de la cadena de custodia; y (3) documentar que la muestra/evidencia fue manipulada únicamente por personal aprobado y no fue accesible para su manipulación antes del análisis. La información registrada en el formulario del marco propuesto incluye:

- Descripción de la evidencia electrónica: Esto generalmente abarca nombres de archivos, información sobre el hardware utilizado, y cualquier característica relevante de los datos.

- Métodos de recolección: Detallar cómo se obtuvo la evidencia, incluyendo procedimientos como la incautación de activos físicos o la extracción de datos de dispositivos.
- Ubicaciones de almacenamiento: Información sobre los lugares físicos o digitales donde se ha almacenado la evidencia, asegurando que su resguardo sea claro y accesible.
- Detalles de acceso: Registro de entradas y salidas que confirmen quién tuvo acceso a la evidencia en diferentes momentos, lo que es crucial para mantener la transparencia y la integridad de la cadena de custodia:
  - Identificador único
  - Nombre y firma del recolector de pruebas
  - Dirección oficial y número de contacto
- Detalles de cada prueba, incluyendo:
  - Identificador único y matriz
  - Fecha y hora de recogida
  - Tipo de análisis requerido
- Firmas de todos los involucrados en la cadena de posesión con fecha y hora.
- Fecha y forma de entrega
- Autorización para el análisis de la prueba
- Cualquier otra información sobre la prueba

Criterios generales para la implementación de la Cadena de Custodia en el marco de preservación de pruebas electrónicas

- Cumplimiento de normativas de protección de datos: La implementación de este marco debe cumplir con las regulaciones pertinentes en materia de protección de datos, como la Ley Orgánica de Protección de Datos, para proteger la privacidad de las personas involucradas.
- Protección de las pruebas electrónicas: La manipulación de las pruebas electrónicas está prohibida, y se deberá evitar cualquier acción sobre el original de la evidencia. La prueba original deberá ser conservada como copia maestra, permitiendo que los expertos realicen cualquier análisis exclusivamente sobre copias duplicadas.
- Acceso limitado: Limitar la cantidad de personas que pueden acceder a estos datos también es crucial. Esto ayudará a proteger cada pieza de evidencia de ser dañada durante el manejo.
- Integridad sostenible: Las acciones adoptadas para proteger y recopilar evidencia digital no deben afectar la integridad de dicha evidencia.

- Personal competente: Las personas que realicen un examen de evidencia digital deben recibir capacitación para tal fin.
- Documentación de todo el proceso: La actividad relacionada con la incautación, examen, almacenamiento o transferencia de evidencia digital debe documentarse, preservarse y estar disponible para su revisión.

Criterios de peritaje específicos:

Tabla 3. Definición de los criterios específicos de peritaje de las pruebas electrónicas.

Criterio	Descripción
Identificación de la fuente de datos	Este criterio implica determinar y documentar la procedencia de los datos electrónicos, asegurando que se pueda rastrear su origen. Es fundamental para establecer la credibilidad de la prueba y garantizar que proviene de una fuente confiable.
Verificación de los métodos de extracción	Se refiere a la necesidad de comprobar los procedimientos utilizados para extraer los datos de su fuente original. Evaluar si se han seguido protocolos adecuados y si se han utilizado herramientas y técnicas que aseguren la precisión y la fidelidad de la información extraída.
Registro de metadatos	Este criterio implica la recopilación y conservación de metadatos, que son datos que describen otros datos. Los metadatos deben incluir información sobre la creación, modificación y acceso a los documentos electrónicos, para poder establecer su contexto y autenticidad.
Descripción del dispositivo que ha generado los datos	Es esencial proporcionar información sobre el dispositivo IoT o sistema que produjo los datos electrónicos. Se deben incluir detalles sobre el hardware y software utilizados, ya que influyen en la validez de la prueba y en la posibilidad de replicar el proceso de generación de datos.
Verificación de integridad	Este criterio se centra en asegurar que los datos no han sido alterados o manipulados desde su creación hasta su presentación como prueba. En el marco propuesto se utilizan técnicas como *hash* y cadena de custodia para comprobar que la información se mantiene intacta y sin modificaciones.
Validación de la fuente	Implica confirmar que la fuente de los datos es legítima y confiable. Incluye la verificación de la identidad del autor o creador del documento electrónico, así como la autenticidad de la plataforma o sistema desde el cual se obtuvo la información.

Buenas prácticas recomendadas para la preservación de pruebas electrónicas:

La correcta preservación de las pruebas electrónicas es crucial para los asuntos legales. En la tabla 3 se presentan buenas prácticas recomendadas para asegurar que la evidencia sea manejada de la manera más segura y efectiva posible:

Tabla 4. Buenas prácticas recomendadas.

No.	Buenas prácticas
1.	Es esencial registrar el estado físico del dispositivo IoT que contiene los medios digitales. Tómese el tiempo para fotografiarlo y anote cualquier característica relevante, como daños visibles, ubicación física y la presencia de herramientas cercanas que pudieran haber sido utilizadas. Esta información debe ser almacenada en el mismo sistema de gestión de evidencias que el dispositivo.
2.	Reconocer la necesidad de expertos es vital. Aunque los técnicos y personal de seguridad pueden contribuir en la recolección inicial de la evidencia, el análisis y la conservación de datos requieren conocimientos forenses especializados.
3.	Es obligatorio documentar la transferencia de medios y pruebas digitales entre todas las personas y entidades que tengan contacto con ellas. La existencia de lagunas en esta documentación puede invalidar las pruebas en un contexto judicial. Se recomienda el uso de registros digitales fiables para asegurar la transparencia.
4.	Durante la identificación y recolección, se debe evitar cambiar el estado de energía del dispositivo. Manténgalo encendido si ya está así, y apáguelo únicamente si es absolutamente necesario, especialmente en dispositivos conectados a la corriente. Siempre que sea posible, consulte a expertos forenses antes de realizar cambios.
5.	Se debe garantizar una cadena de custodia adecuada con medidas de seguridad física robustas. Los dispositivos no deben ser dejados en áreas de acceso público y deben ser vigilados para prevenir la manipulación no autorizada.
6.	Evite manipular los medios originales directamente. Siempre que sea posible, realice el análisis sobre copias duplicadas para preservar metadatos valiosos que podrían perderse si se trabaja sobre el original.
7.	Aislar el dispositivo de redes externas y conexiones Wi-Fi es fundamental para preservar la integridad de los datos y metadatos. Minimice el riesgo de sobrescribir información valiosa al evitar la conexión de dispositivos externos.
8.	Evalúe la necesidad de almacenamiento externo para la gestión de evidencia a largo plazo o considere un sistema de gestión modular que pueda adaptarse a futuros cambios en necesidades de retención y espacio disponible.
9.	Es crucial registrar regularmente las transacciones relacionadas con la evidencia, lo que incluye la firma de personal para informes y consultas. Esto ayuda a mantener una cadena de custodia adecuada y puede ser facilitado por casilleros automatizados que simplifican el seguimiento.
10.	Dada la rápida evolución de la tecnología, es imprescindible revisar regularmente las prácticas de gestión de evidencia digital para asegurarse de que se adapten a nuevos tipos de dispositivos y métodos de almacenamiento que puedan surgir.
11.	Establecer formatos de datos comunes para la recolección y presentación de evidencias en dispositivos IoT, asegurando que la información recopilada sea fácilmente accesible y comprensible por los peritos forenses.
12.	La imagen será un clon bit a bit de la evidencia original cargada en la computadora forense para su investigación. Una vez cargada la imagen, se debe autentificar mediante un análisis de hash.

13.	Desarrollar protocolos claros que guíen la recolección de datos a partir de la memoria local de dispositivos IoT, garantizando que se minimice la pérdida de datos y que la integridad de la cadena de custodia sea mantenida sin interrupciones.
14.	Crear manuales y guías que detallen la arquitectura informática de diferentes dispositivos y sistemas, con el fin de capacitar a los peritos en la identificación y extracción de evidencias adecuadas de cada tipo de dispositivo.
15.	Implementar el uso de herramientas especializadas para el análisis del tráfico de red cifrado, facilitando la recolección de evidencias relacionadas con la comunicación de dispositivos y permitiendo la correcta interpretación de los datos transmitidos.
16.	Definir directrices sobre cómo gestionar la obtención de evidencias en situaciones con jurisdicción transfronteriza, incluyendo procedimientos de colaboración con entidades internacionales y protocolos legales a seguir.
17.	Establecer requisitos para la documentación exhaustiva de cada fase de la cadena de custodia, desde la recolección inicial hasta la presentación en la corte, asegurando que se registren todos los movimientos y accesos a la evidencia.
18.	Crear un programa de capacitación continua para peritos forenses que les permita mantenerse actualizados sobre las últimas tecnologías, herramientas y metodologías en la recolección y análisis de evidencias digitales.

Propuesta de modificación al artículo 195 del COGEP

Modificación del artículo 195 del Código Orgánico General de Procesos (COGEP) el cual menciona y explica la eficacia de la prueba documental.

Justificación:

La propuesta de modificación del artículo 195 del Código Orgánico General de Procesos (COGEP) se fundamenta en la necesidad de adaptar la normativa procesal a los avances tecnológicos y a la creciente relevancia de las pruebas electrónicas en el sistema judicial ecuatoriano. La inclusión de un numeral que exija un peritaje especializado busca asegurar que las pruebas electrónicas sean evaluadas con métodos rigurosos, como la identificación de la fuente de datos, la verificación de integridad y la validación de la fuente, protegiendo así los derechos procesales de las partes y contribuyendo a la modernización del sistema de justicia.

Objetivo:

Modificar el artículo 195 del COGEP para incluir criterios específicos de peritaje en la evaluación de pruebas documentales electrónicas, con el fin de garantizar su autenticidad, seguridad y trazabilidad.

Propuesta:

Agregar al artículo 195 del COGEP un numeral 4, el cual debe expresar lo siguiente:

> Para el cumplimiento de la eficacia de la prueba en el caso de documentos electrónicos se deben someter a peritaje que determinen la autenticidad del mismo. Los cuales incluirían identificación de la fuente de datos,

verificación de los métodos de extracción, registro de metadatos, descripción del dispositivo que ha generado los datos, verificación de integridad, validación de la fuente.

Validación de la propuesta

Se llevó a cabo un contacto con un grupo de 23 especialistas de la provincia de Morona Santiago, Ecuador, compuesto por peritos forenses, abogados, jueces y operadores jurídicos con amplia experiencia en el manejo de pruebas electrónicas en el ámbito judicial. Este panel de expertos aceptó participar en la validación de la propuesta de modificación al artículo 195 del Código Orgánico General de Procesos (COGEP), para lo cual se les proporcionó tanto la propuesta de modificación, como el marco detallado para la preservación de pruebas electrónicas y los criterios específicos de peritaje en la evaluación de pruebas documentales electrónicas. Su tarea consistió en analizar esta información, realizar una evaluación a través de encuestas y emitir recomendaciones fundamentadas sobre la propuesta presentada. Se les proporcionó una encuesta para ser respondida en una escala de Likert de cinco puntos donde: 1-Totalmente en desacuerdo y 5-Totalmente de acuerdo. La tabla 4 muestra los resultados alcanzados:

Tabla 4. Validación de la propuesta.

Criterio	M	DE
La normativa procesal actual carece de directrices adecuadas para la evaluación de pruebas electrónicas.	4.87	0.42
La inclusión de criterios específicos de peritaje en la normativa procesal ecuatoriana fortalecerá la autenticidad de las pruebas electrónicas.	4.36	0.67
La implementación de criterios específicos de peritaje mejorará la seguridad de las pruebas electrónicas en el sistema judicial.	4.96	0.11
La adopción de un marco claro para el peritaje electrónico contribuirá a aumentar la confianza en el sistema judicial ecuatoriano.	4.23	0.54
La inclusión de criterios específicos facilitará un manejo más efectivo y eficiente de las pruebas electrónicas durante los procesos judiciales.	3.17	1.98
La modificación del artículo 195 para incluir criterios específicos es necesaria para mejorar la eficacia del sistema judicial en relación con las pruebas electrónicas.	5	0.0
La claridad en los criterios de peritaje específico reducirá el riesgo de impugnaciones relacionadas con la validez de las pruebas electrónicas.	3.98	1.23
En general, considero que la propuesta presentada contribuirá significativamente a mejorar el manejo y evaluación de las pruebas electrónicas en el sistema judicial ecuatoriano.	4.62	0.56

Nota: n= 23 expertos; 1: Totalmente en desacuerdo; 2- En desacuerdo; 3-Neutro; 4: De acuerdo; 5 Totalmente de acuerdo; **M**: Media; **DE**: Desviación estándar.

Los resultados de la validación de la propuesta revelaron una valoración general muy positiva, con todos los expertos coincidiendo en que la modificación del artículo 195 para incorporar criterios específicos es esencial para mejorar la eficacia del sistema judicial en el manejo de pruebas electrónicas. Sin embargo, dos de los criterios evaluados recibieron puntuaciones más cautelosas, con valores de 3.17 y 3.98, respectivamente. Estos se referían a la posibilidad de que la inclusión de criterios específicos optimice el manejo de las pruebas electrónicas durante los procesos judiciales y a la expectativa de que una mayor claridad en dichos criterios disminuya el riesgo de impugnaciones sobre su validez. La reserva en estas puntuaciones sugiere que, aunque la propuesta es sólida, su efectividad también dependerá de factores externos que pueden influir en su implementación y aceptación dentro del sistema judicial.

Uno de los principales desafíos técnicos señalado por los expertos sobre el marco de preservación de pruebas electrónicas, es el uso de técnicas de cifrado, la ocultación de datos en el espacio de almacenamiento y el establecimiento de canales encubiertos. Los expertos en informática forense consultados, admitieron que en la actualidad se enfrentan dificultades para operar en entornos de nube presenta nuevos obstáculos, como la duración del proceso de archivo de datos, la falta de competencias especializadas en el personal, y el uso de esteganografía para proteger información delicada. Estos factores crean un entorno complejo que dificulta la recolección y preservación efectiva de evidencia digital en procedimientos judiciales.

Discusiones

En el ámbito del derecho comparado, (Vadell et al., 2021) explican que países como España han implementado regulaciones detalladas que aseguran la trazabilidad y la autenticidad de las pruebas electrónicas. Estas medidas incluyen la validación de la fuente de datos y la preservación de la cadena de custodia digital, lo que asegura que las pruebas mantengan su valor probatorio. De forma similar, (Yeboah-Ofori & Brown, 2020) describe cómo el sistema judicial estadounidense ha introducido reglas específicas que integran tecnologías de encriptación y auditoría para proteger la evidencia digital. Estas estrategias no solo garantizan la seguridad de las pruebas, sino que también contribuyen a decisiones judiciales más equitativas y fundamentadas.

El Código Orgánico General de Procesos (COGEP) de Ecuador establece disposiciones específicas sobre la admisibilidad de la prueba digital en el ámbito judicial (de Procesos, 2015). Este cuerpo legal reconoce la validez de las pruebas electrónicas, siempre que se presenten mediante mecanismos que garanticen su autenticidad e integridad (León et al., 2019). Entre estos mecanismos se incluyen el uso de firmas electrónicas y sellos de tiempo, aplicables a diversos tipos de evidencia digital, como correos electrónicos, mensajes de texto, imágenes y documentos digitales.

Para que una prueba digital sea aceptada en un proceso judicial, es fundamental que se asegure su integridad, lo que implica que no haya sido manipulada o alterada. Esto se puede conseguir mediante la verificación de firmas electrónicas,

registros de acceso y sistemas de encriptación, los cuales ayudan a respaldar la autenticidad de los documentos digitales presentados como evidencia.

En cuanto a la valoración de la prueba digital, el COGEP otorga a los jueces la facultad de evaluar estas pruebas según los principios de libre valoración. Sin embargo, para que la prueba digital sea considerada válida, la parte que la introduzca debe demostrar la confiabilidad de los medios electrónicos utilizados para su obtención (Puetate Paucar et al., 2021). Esto añade un nivel de rigor que busca garantizar la certeza y legalidad de la información presentada.

Además, en numerosas ocasiones, se requiere la intervención de peritos informáticos para validar las pruebas digitales, especialmente en casos donde la evidencia técnica es compleja, como el análisis de metadatos o la recuperación de información de dispositivos electrónicos. Estos expertos desempeñan un rol crucial al aportar su conocimiento técnico, lo que refuerza la credibilidad de las pruebas en un proceso judicial.

Sin embargo, el COGEP carece de criterios específicos en relación con el peritaje destinado a la evaluación de pruebas electrónicas. Esto resalta la necesidad de que en esta investigación se considerara la modificación del artículo 195, con el objetivo de incorporar lineamientos específicos que regulen el peritaje en el ámbito digital. Al hacerlo, se buscaría asegurar la autenticidad, seguridad y trazabilidad de dichas pruebas, lo que fortalecería la confianza en el sistema judicial al manejar evidencia electrónica.

Conclusiones

La evidencia electrónica se puede obtener de una variedad de fuentes, incluidas computadoras, dispositivos móviles, dispositivos de almacenamiento remoto, dispositivos de Internet de las cosas (IoT) y prácticamente cualquier otro sistema computarizado. Si bien los registros de *blockchain* tienen una integridad sólida, su admisibilidad en los tribunales aún puede estar sujeta al escrutinio judicial. Es fundamental establecer su confiabilidad y aceptación en los procedimientos legales. Es posible que las pruebas presentadas en el tribunal sean desestimadas si falta un eslabón en la cadena de custodia. Por lo tanto, es importante garantizar que se presente una cadena de custodia completa y significativa junto con las pruebas en el tribunal y que estas pruebas esten debidamente establecidas dentro del marco regulatorio ecuatoriano.

Para fortalecer la eficacia de las pruebas electrónicas en el sistema judicial ecuatoriano se definió un conjunto de seis criterios específicos de peritaje para que sean incluidos en la normativa procesal. En consecuencia, se realizó la propuesta de modificación al artículo 195 del Código Orgánico General de Procesos para que incluya los criterios específicos de peritaje definidos en la presente investigación. Adicionalmente se propuso un marco de preservación de pruebas electrónicas basado en *blockchain* para el IoT que implementa la cadena de custodia y utiliza la plataforma *Ethereum* para resforzar los principios de descentralización y transparencia que son fundamentales para la tecnología

blockchain. La propuesta fue validada mediante criterio de expertos, la cual fue valorada como muy pertinente de manera general.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas
2. Curación de datos: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
3. Análisis formal: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
4. Investigación: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
5. Metodología: Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas
6. Administración del proyecto: Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas
7. Software: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
8. Supervisión: Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas
9. Validación: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
10. Visualización: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde
11. Redacción – borrador original: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde, Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas
12. Redacción – revisión y edición: Lida Jimena Avila Contreras, José Vicente Serrano Campoverde, Johanna Irene Escobar Jara , Fátima Eugenia Campos Cardenas

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Acosta-León, C. A. (2023). La prueba documental de fuentes informáticas basadas en documentos digitales con firma electrónica certificada: Un análisis desde la perspectiva de las tecnologías de la información y el principio de libertad de prueba en el proceso penal venezolano. *Revista chilena de derecho y tecnología*, *12*. https://www.scielo.cl/scielo.php?pid=S0719-25842023000100203&script=sci_arttext

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. *Blockchain and Clinical Trial: Securing Patient Data*, 149-168. https://link.springer.com/chapter/10.1007/978-3-030-11289-9_7

Bueno de Mata, F. (2015). Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1. ª), de 19 de mayo de 2015 [ROJ: STS 2047/2015]. https://gredos.usal.es/bitstream/handle/10366/129115/Sentencia_del_Tribunal_Supremo_(Sala_de_.pdf?sequence=1

de Procesos, C. O. G. (2015). Código Orgánico General de Procesos. *Quito: Corpacion de Estudios y Publicaciones*. https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2018/03/codigo_organico_general_de_procesos.pdf

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, *52*, 70-89. https://www.sciencedirect.com/science/article/pii/S0167404815000449

Fernández, M. d. J. C., Salas, F. L., & Benjumea, M. P. P. (2022). Valor Probatorio del Documento Electrónico a la Luz de la Digitalización de la Justicia en Colombia. *Revista Jurídica Mario Alario D'Filippo*, *14*(28), 302-324. https://dialnet.unirioja.es/servlet/articulo?codigo=8982825

Galvis , Á. F., & Bustamante , M. (2019). La no equivalencia funcional entre la prueba electrónica y la prueba documental: Una lectura desde la regulación procesal colombiana. *Ius et praxis*, *25*(2), 189-222. https://www.scielo.cl/scielo.php?pid=S0718-00122019000200189&script=sci_arttext

Khan, A. A., Uddin, M., Shaikh, A. A., Laghari, A. A., & Rajput, A. E. (2021). MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access*, *9*, 103637-103650. https://ieeexplore.ieee.org/abstract/document/9492114/

Lema Morocho, G. E. (2018). *Análisis de la prueba electrónica en el proceso civil., y el derecho a la defensa* https://dspace.uniandes.edu.ec/handle/123456789/9213

León , D. A., León , R. B., & Durán , A. R. (2019). La prueba en el código orgánico general de procesos. Ecuador. *Revista Universidad y sociedad*, *11*(1), 359-368. http://scielo.sld.cu/scielo.php?pid=S2218-36202019000100359&script=sci_arttext

Li, S., Qin, T., & Min, G. (2019). Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, *6*(6), 1433-1441. https://ieeexplore.ieee.org/abstract/document/8777292/

Lone, A. H., & Mir, R. N. (2018). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Sci. Pract. Cyber Secur. J*, *1*, 21-27. https://journal.scsa.ge/wp-content/uploads/2018/12/4-auqib-hamid-lone-roohie-naaz-mir_forensic-chain-ethereum-blockchain-based-digital-forensics-chain-of-custody.pdf

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital investigation*, *28*, 44-55. https://www.sciencedirect.com/science/article/pii/S174228761830344X

Paredes, K. D. C., & Paredes, C. E. C. (2022). La prueba y su valoración dentro del Código Orgánico General de Procesos, Ecuador. *Sociedad & Tecnología*, *5*(S1), 17-29. https://institutojubones.edu.ec/ojs/index.php/societec/article/view/230

Puetate Paucar, J. M., Coka Flores, D. F., & Méndez Cabrita, C. M. (2021). La prueba digital en procesos judiciales aplicables al Código Orgánico General de Procesos (COGEP), a partir de la pandemia COVID-19. *Dilemas contemporáneos: educación, política y valores*, *8*(SPE3). https://www.scielo.org.mx/scielo.php?pid=S2007-78902021000500017&script=sci_arttext

Shurson, J. (2020). Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law. *International journal of law and information technology*, *28*(2), 167-184. https://academic.oup.com/ijlit/article-pdf/doi/10.1093/ijlit/eaaa011/33677448/eaaa011.pdf

Vadell, L. M. B., Rúa, M. M. B., & Garzón, L. O. T. (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://dialnet.unirioja.es/servlet/articulo?codigo=8084167

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1-8. http://repository.uwl.ac.uk/id/eprint/8012/