



Revista de Ciencias Sociales

Depósito legal ppi 201502ZU4662
Esta publicación científica en formato
digital es continuidad de la revista impresa
Depósito Legal: pp 197402ZU789
• ISSN: 1315-9518 • ISSN-E: 2477-9431

Universidad del Zulia. Revista de la Facultad de Ciencias Económicas y Sociales
Vol. XXXII, No. ESPECIAL 13 **Enero-Junio 2026**

Revista de Ciencias Sociales

Esta publicación científica en formato
digital es continuidad de la revista impresa
Depósito Legal: pp 197402ZU789
ISSN: 1315-9518

Desafíos de la era digital a los fundamentos dogmáticos de la prueba penal ecuatoriana

Astudillo Orellana, Washington Rene*

Resumen

El avance tecnológico ha redefinido las formas de interacción humana y los mecanismos de producción, transmisión y conservación de la información. Este cambio ha impactado directamente en el ámbito jurídico, especialmente en el proceso penal, donde la incorporación de evidencias digitales plantea nuevos retos frente a principios clásicos de la teoría de la prueba. En Ecuador, la irrupción tecnológica en los procedimientos judiciales ha generado tensiones entre la práctica procesal tradicional y las demandas de un entorno digital que exige respuestas más ágiles y garantistas. El objetivo de esta investigación es examinar los desafíos que la era digital impone a los fundamentos dogmáticos de la prueba penal ecuatoriana, con especial atención a los criterios de autenticidad, admisibilidad y valoración de evidencia tecnológica. La metodología aplicada responde a un enfoque cualitativo de tipo exploratorio-descriptivo, basado en la revisión documental de normas, doctrinas y jurisprudencias nacionales e internacionales. Los resultados evidencian la falta de armonización entre el marco jurídico vigente y exigencias digitales, así como ausencia de criterios uniformes sobre admisibilidad y fiabilidad de la prueba electrónica. En conclusión, la era digital obliga a replantear los fundamentos dogmáticos de la prueba penal, promoviendo reformas normativas y doctrinarias coherentes con derechos fundamentales.

Palabras clave: Prueba digital; fundamentos dogmáticos; ciberdelincuencia; era digital; valoración probatoria.

* Doctor en Derecho. Doctor en Gestión Pública y Gobernabilidad. Docente Titular Auxiliar 1 e Investigador de Pregrado y Posgrado en la Universidad de Guayaquil, Guayaquil, Ecuador. E-mail: washington.astudillo@ug.edu.ec ORCID: <https://orcid.org/0000-0002-5085-6099>

Challenges of the digital age to the dogmatic foundations of Ecuadorian criminal evidence

Abstract

Technological advancements have redefined human interaction and the mechanisms for producing, transmitting, and preserving information. This shift has directly impacted the legal field, particularly criminal proceedings, where the incorporation of digital evidence poses new challenges to classical principles of evidence theory. In Ecuador, the technological disruption of judicial procedures has generated tensions between traditional procedural practices and the demands of a digital environment that requires more agile and protective responses. The objective of this research is to examine the challenges that the digital age imposes on the dogmatic foundations of Ecuadorian criminal evidence, with particular attention to the criteria of authenticity, admissibility, and evaluation of technological evidence. The methodology employed is a qualitative, exploratory-descriptive approach, based on a review of national and international legal norms, doctrines, and jurisprudence. The results reveal a lack of harmonization between the current legal framework and digital requirements, as well as an absence of uniform criteria regarding the admissibility and reliability of electronic evidence. In conclusion, the digital age compels us to rethink the dogmatic foundations of criminal evidence, promoting normative and doctrinal reforms consistent with fundamental rights.

Keywords: Digital evidence; dogmatic foundations; cybercrime; digital age; evidentiary assessment.

Introducción

En las últimas décadas, el vertiginoso avance tecnológico ha transformado de manera profunda las formas de comunicación, almacenamiento y transmisión de información. Estos cambios han dado origen a nuevas dinámicas sociales y jurídicas (Mejía-Lobo et al., 2023), evidenciadas en fenómenos como los delitos informáticos, el uso masivo de datos personales y la participación digital en distintos ámbitos. Tales transformaciones obligan al Derecho penal a replantear sus estructuras conceptuales y adaptarse a un contexto en el que la tecnología permea todas las esferas de la vida social y judicial.

Como señalan Delso et al. (2024), que si bien el estudio de las transformaciones tecnológicas como el desarrollo del metaverso y otras infraestructuras digitales emergentes resulta fundamental para comprender cómo estas innovaciones pueden aprovecharse en distintos ámbitos del conocimiento, en el contexto jurídico su relevancia adquiere un matiz particular.

Tal como se plantea en los estudios sobre tecnología y sociedad, analizar estos

cambios permite identificar brechas y desafíos en la adaptación de los sistemas tradicionales, así como definir nuevas líneas de investigación orientadas a garantizar un uso sostenible y equitativo de las herramientas digitales. No obstante, en el ámbito del proceso penal, estos avances solo adquieren verdadera eficacia si van acompañados de mecanismos normativos y procedimentales que posibiliten la práctica, obtención y valoración adecuada de la prueba digital, preservando los principios dogmáticos que rigen el debido proceso.

Whalen (2022); y Centeno et al. (2022), sostienen que, aunque el futuro de los sistemas jurídicos aún presenta múltiples incertidumbres, la tecnología está llamada a desempeñar un papel cada vez más determinante en la práctica, el acceso, la aplicación y la creación del Derecho. Desde esta perspectiva, destacan la necesidad de abordar los procesos de digitalización jurídica con un enfoque crítico y equilibrado, que permita aprovechar los beneficios de eficiencia y transparencia que ofrecen las herramientas tecnológicas, sin descuidar los riesgos que estas pueden generar sobre los principios estructurales del ordenamiento jurídico.

Este planteamiento resulta especialmente relevante en el ámbito penal, donde la incorporación de medios tecnológicos en la obtención y valoración de la prueba exige una revisión profunda de los fundamentos dogmáticos que garantizan la validez y legitimidad del proceso.

En este contexto de constante innovación tecnológica y globalización de la información, resulta pertinente examinar las experiencias internacionales que enfrentan problemáticas similares. En el ámbito internacional, Abraha (2021) destaca que la omnipresencia de la computación en la nube ha generado un escenario en el que las investigaciones penales requieren cada vez más acceder a datos transfronterizos, lo que ha evidenciado la ineficacia del sistema tradicional de Asistencia Jurídica Mutua. Según el autor, esta limitación ha impulsado múltiples iniciativas para reformar o sustituir dicho sistema, aunque la falta de coordinación entre los distintos enfoques reformista, unilateralista, internacionalista y matizado, ha incrementado la incertidumbre jurídica y los conflictos jurisdiccionales.

Este análisis internacional ofrece un referente valioso para comprender cómo los desafíos tecnológicos actuales inciden en la obtención y valoración de las pruebas digitales, y cómo estas tensiones repercuten en la configuración dogmática del proceso penal, superando la asistencia penal internacional frente a la mente criminal que trasciende fronteras en este mundo digitalizado.

En el caso ecuatoriano, no ha sido la excepción enfrentarse a esta nueva realidad, que ha impactado los fundamentos dogmáticos de la prueba penal, al generar cuestionamientos sobre su naturaleza, las formas de obtención, los criterios de admisibilidad y valoración, así como las garantías constitucionales que deben preservarse en el proceso probatorio.

La globalización digital ha reconfigurado el modo en que se concibe, produce y presenta la prueba dentro del proceso penal. En Ecuador, la presencia constante de evidencia proveniente de medios tecnológicos como mensajes de *WhatsApp*, correos electrónicos,

metadatos, videos de cámaras de seguridad o publicaciones en redes sociales, exige una revisión crítica de los principios que sustentan la dogmática probatoria.

Los postulados clásicos, tales como la inmediación, la cadena de custodia, la valoración objetiva y la presunción de inocencia, enfrentan desafíos ante la fragilidad, la posibilidad de manipulación y la complejidad técnica que caracterizan a las evidencias digitales.

En ese sentido, Ward (2020) explica que, en el contexto penal de Inglaterra y Gales, la admisibilidad de la prueba pericial depende de que el tribunal verifique su fundamento científico y considere que este sea lo suficientemente confiable para ser valorado en juicio. Este enfoque evidencia la necesidad de que los sistemas jurídicos, frente a los retos que plantea la evidencia digital, adopten criterios rigurosos que aseguren el origen, la fiabilidad y legitimidad de los medios probatorios, que inexorablemente serán incorporados en el proceso penal.

El problema principal de esta investigación se centra en la limitada adecuación del marco dogmático y normativo ecuatoriano frente a las exigencias del entorno digital en materia probatoria. Aunque el Código Orgánico Integral Penal de 2023 que en adelante se identificará con los acrónimos (COIP), reconoce la existencia de la prueba electrónica, su tratamiento doctrinario y procesal aún no presenta una línea uniforme. Los operadores de justicia se enfrentan, por tanto, a la dificultad de comprobar la autenticidad y confiabilidad de estos elementos, lo que genera inseguridad jurídica y posibles vulneraciones al derecho a la defensa y al debido proceso.

En tal sentido, se vuelve necesario examinar los fundamentos teóricos de la prueba penal tradicional y su capacidad para responder a los nuevos escenarios tecnológicos, identificando los puntos de tensión entre la tecnología digital y los principios dogmáticos clásicos. De lo indicado, existe la necesidad de reformas normativas, doctrinarias y prácticas, que fortalezcan la admisibilidad, autenticidad

y valoración de la prueba digital, garantizando la protección de los derechos fundamentales y un tratamiento coherente con la jurisprudencia y el marco legal vigente.

En la actualidad, resulta inconcebible imaginar a una administración de justicia sin la intervención de herramientas tecnológicas, de hecho, los procesos penales contemporáneos dependen en gran medida de pruebas que contienen componentes electrónicos, informáticos o digitales. La legislación ecuatoriana, consciente de esta realidad, incorporó en 2020 diversas medidas de investigación tecnológica con el fin de adecuar los procedimientos penales a las nuevas formas de criminalidad.

En un Estado de Derechos, la respuesta penal no puede quedar rezagada frente a una delincuencia cada vez más sofisticada desde el punto de vista tecnológico. La prueba digital adquiere así un papel esencial, no solo para identificar y detener a los autores de los hechos punibles, sino también para acreditar la existencia del delito y sustentar una eventual condena. Este tipo de prueba se torna decisiva tanto en los delitos perpetrados mediante instrumentos tecnológicos cibercrimitos o delincuencia informática como en aquellos de carácter tradicional, donde la evidencia tecnológica resulta cada vez más relevante debido al proceso de digitalización general de la sociedad.

En esta línea, Martínez (2022), sostiene que el informe pericial constituye la materialización inteligible del análisis técnico de las evidencias informáticas, pero que el verdadero contenido probatorio reside en los anexos que acompañan dicho informe como discos, memorias USB o certificados digitales, los cuales contienen los archivos originales y los respectivos valores *hash* que garantizan su integridad y autenticidad.

De esta manera, el objetivo general de esta investigación consiste en identificar a través del análisis de los desafíos que la era digital plantea a los fundamentos dogmáticos de la prueba penal tradicional ecuatoriana, colocando énfasis en los aspectos relacionados con la autenticidad, valoración, admisibilidad

y respeto de los derechos fundamentales, para sustentar una acusación frente al auge delictivo con las exigencias derivadas de la sociedad digital contemporánea.

1. Fundamentación teórica

La era digital constituye un contexto socio-tecnológico caracterizado por la producción, procesamiento, transmisión y almacenamiento de información mediante dispositivos electrónicos, redes interconectadas e infraestructura virtual. Este entorno según Levin y Mamlok (2021), describen esta etapa como una revolución ontológica caracterizada por la abundancia informativa y la fusión entre lo real y lo virtual, lo humano y lo tecnológico, estas transformaciones inciden directamente en los modos de comunicación y de interacción social, generando nuevas formas de evidencia y de criminalidad, como los delitos informáticos, el uso ilícito de datos personales, la manipulación de contenidos digitales o la vulneración de la privacidad a través de medios tecnológicos.

En este escenario, la información adquiere un valor jurídico relevante, al convertirse en prueba dentro de los procesos penales, lo que exige la aplicación de criterios técnicos y dogmáticos capaces de salvaguardar desde una cadena de custodia lícita, para garantizar su autenticidad, integridad y fiabilidad, hasta la producción y/o tratamiento de la prueba.

Por su parte Santacruz (2013), menciona que la prueba penal, en el marco del sistema jurídico, constituye el conjunto de medios, actos y procedimientos orientados a demostrar la existencia de los hechos relevantes para la determinación de la responsabilidad penal. Su función probatoria se sustenta en principios constitucionales y procesales como la legalidad, presunción de inocencia, debido proceso, contradicción, inmediación y valoración racional o discrecionalidad del juzgador. Estos principios no sólo determinan la validez del medio probatorio, sino también la legitimidad del proceso judicial en su

conjunto, asegurando que toda decisión jurisdiccional repose sobre evidencias obtenidas y valoradas conforme a la ley y a las garantías fundamentales.

Por su parte, los fundamentos dogmáticos de la prueba penal representan el núcleo teórico que sostiene la estructura conceptual de la institución probatoria. Comprenden los principios de legalidad y legitimidad de la prueba, autenticidad e integridad del medio probatorio, valor probatorio, carga de la prueba (*onus probandi*), imparcialidad judicial, contradicción y debido proceso.

Cada uno de estos fundamentos cumple una función específica en la protección de los derechos procesales y en la construcción de una justicia penal transparente y confiable de acuerdo a la necesidad en este mundo globalizado tecnológico, tal como a continuación se detalla: a) la legalidad, asegura que sólo se admitan pruebas obtenidas conforme al ordenamiento jurídico; b) la autenticidad, garantiza que el elemento probatorio sea lo que efectivamente declara ser; c) la integridad, impide su alteración o manipulación; y, d) la valoración racional, exige al juez fundamentar su decisión conforme a criterios objetivos, razonables y verificables.

Arnold (2021), señala que las pruebas y las evidencias desempeñan un papel esencial dentro de las auditorías forenses, pues constituyen elementos determinantes en la toma de decisiones judiciales una vez que sean valoradas e introducidas en el proceso, además advierte, que con frecuencia se confunden los términos prueba y evidencia, lo que puede generar vacíos o desaciertos en la presentación y análisis de los hallazgos ante un tribunal. En consonancia con lo referido, la autora destaca que la distinción entre prueba y evidencia depende del contexto y de la pericia técnica del profesional que las analiza, puesto que solo adquieren valor probatorio cuando cumplen con los principios de conducencia, pertinencia y utilidad, criterios fundamentales ante los desafíos que plantea la era digital en la valoración de la prueba.

En relación con la categoría en estudio,

la prueba penal en la era digital, como un escenario de cambio estructural, aborda las implicaciones que tiene el uso de tecnologías de la información en la conformación y tratamiento de las evidencias dentro del proceso penal. Comprende el estudio de fenómenos como la generación de mensajes de datos, registros electrónicos, metadatos y contenidos digitales, así como los problemas asociados a su conservación, trazabilidad y autenticidad. También incluye el análisis de los desafíos técnicos y jurídicos vinculados con la cadena de custodia, la interoperabilidad de sistemas, la reserva de la información y la necesidad de peritajes especializados que garanticen la fiabilidad de las pruebas digitales.

Respecto a la categoría sobre los fundamentos dogmáticos de la prueba penal, como marco de contención jurídica se centra en la revisión teórica y doctrinaria de los principios que rigen la función probatoria. Desde su origen constitucional hasta su desarrollo en la legislación ecuatoriana y la jurisprudencia comparada, esta categoría examina cómo los postulados clásicos del Derecho penal legalidad, debido proceso, contradicción, imparcialidad y valoración judicial, se ven tensionados frente a las nuevas formas de evidencia digital. Su análisis permite identificar las transformaciones conceptuales necesarias para adecuar la dogmática probatoria a los retos del entorno tecnológico contemporáneo, sin menoscabar las garantías esenciales del derecho a la defensa en el proceso penal.

De acuerdo con el Boletín de Análisis de la Ciberdelincuencia (Ministerio del Interior de Ecuador [MIE], 2024): La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial, emitido por el Ministerio del Interior del Ecuador y otras autoridades competentes, la ciberdelincuencia puede entenderse como el conjunto de conductas ilícitas cometidas mediante el uso de sistemas informáticos, redes o tecnologías digitales, con el propósito de vulnerar la seguridad, la integridad o la confidencialidad de la información. Este concepto refleja cómo la criminalidad se ha adaptado al entorno

digital, aprovechando los avances tecnológicos para ejecutar nuevas formas de delito.

En este contexto, la inteligencia artificial se ha convertido en una herramienta que amplía las capacidades de los ciberdelincuentes, permitiéndoles realizar ataques más sofisticados y difíciles de detectar, como el *phishing* automatizado, el uso de *malware* inteligente o la aplicación de técnicas de manipulación basadas en algoritmos de aprendizaje automático, lo que dificulta detectar a estos cibercriminales ante una normativa arcaica y/o no a la medida frente a las necesidades de este mundo globalizado.

2. Metodología

En la presente investigación se empleó un enfoque metodológico de carácter cualitativo, de tipo descriptivo-explicativo, que, en términos de Molano et al. (2021), sirve para comprender y darle sentido desde la perspectiva científica a las experiencias humanas mediante la praxis, es decir, busca interpretar lo que expresan las personas y los contextos jurídicos, brindando una respuesta subjetiva y descriptiva sobre fenómenos vinculados al comportamiento social e institucional.

En concordancia con ello, este estudio se basó en la revisión documental y bibliográfica de diversas fuentes académicas, normativas y jurisprudenciales especializadas, obtenidas de repositorios y bases de datos científicas, con el propósito de analizar los diferentes enfoques doctrinarios y técnicos en torno a los desafíos que impone la era digital a los fundamentos dogmáticos clásicos respecto a la prueba penal en el sistema oral acusatorio ecuatoriano.

Posteriormente, se efectuó un análisis interpretativo de la información recopilada, a través del cual se identificaron los principales problemas y vacíos normativos relacionados con la incorporación, autenticidad y valoración de la evidencia digital en el sistema penal acusatorio. Dicho análisis permitió comprender cómo la transformación tecnológica incide en la validez probatoria y en

los principios dogmáticos clásicos del derecho penal ecuatoriano, recurriendo a la necesidad de replantear criterios jurídicos y procesales acordes con las exigencias de la era digital.

La población estuvo constituida por el conjunto total de documentos relacionados con la prueba digital, la dogmática penal, la valoración probatoria y los retos tecnológicos del proceso penal en Ecuador y en experiencias comparadas. La muestra se conformó mediante un muestreo intencional o criterial, integrado por normas vigentes, artículos científicos publicados en los últimos diez años, doctrina especializada y jurisprudencia relevante que abordara directamente la problemática objeto de estudio.

Para la inclusión de las fuentes se aplicaron los siguientes criterios: a) pertinencia temática, referida a contenidos específicos sobre evidencia digital, principios dogmáticos y valoración probatoria; b) actualidad, privilegiando publicaciones recientes de los últimos diez años, salvo textos clásicos indispensables; c) autoridad académica, priorizando revistas indexadas, editoriales reconocidas y repositorios institucionales; y, d) accesibilidad y completitud, asegurando la disponibilidad íntegra del documento para su análisis.

El tratamiento de la información se realizó mediante un análisis interpretativo, que permitió identificar convergencias y divergencias doctrinarias, vacíos normativos y tensiones entre la práctica judicial y los principios dogmáticos del proceso penal ecuatoriano. Este procedimiento posibilitó la elaboración de una comprensión crítica del estado actual de la prueba digital y su impacto en la estructura conceptual de la dogmática penal.

3. La prueba digital y su tratamiento en el sistema probatorio penal ecuatoriano

El proceso de digitalización de la justicia penal ecuatoriana ha transformado el modo en que se conciben, incorporan y

valoran las pruebas dentro del proceso judicial. La transición hacia un entorno tecnológico ha evidenciado importantes tensiones entre los postulados clásicos de la dogmática probatoria y las exigencias derivadas de la era digital.

En este contexto, Puetate et al. (2021) describen que las herramientas tecnológicas, especialmente tras la pandemia de la COVID-19, se han vuelto indispensables para la gestión procesal y la presentación de evidencias electrónicas, al ofrecer mecanismos destinados a asegurar el origen y la integridad de los documentos digitales presentados como prueba. No obstante, esta potencialidad tecnológica no siempre se traduce en una práctica judicial consolidada o coherente.

3.1. Autenticidad e integridad de la prueba digital

El Artículo 500 del Código Orgánico Integral Penal, COIP de 2023, define el contenido digital como toda representación informática de hechos o conceptos de la realidad, procesados o transmitidos por medios tecnológicos. Sin embargo, en la práctica judicial ecuatoriana persiste una brecha entre la definición normativa y su aplicación técnica.

En múltiples causas, la ausencia de informes periciales a través de *software* especializados en que se pueda realizar dicha pericia impide determinar si el contenido digital presentado mantiene su estado original o si ha sufrido alteraciones. Esta carencia afecta los principios de autenticidad e integridad, que constituyen pilares esenciales de la prueba penal. En este sentido, la fiabilidad de la evidencia digital depende no solo de su origen, sino también de la existencia de mecanismos técnicos que permitan constatar su conservación sin manipulación.

3.2. Cadena de custodia y preservación de evidencia

Las recientes reformas al COIP, en particular el artículo 17, establecen

la obligatoriedad del titular del órgano punitivo-fiscal de solicitar al juez la orden de preservación de evidencia digital, garantizando la cadena de custodia. Sin embargo, en el plano operativo se advierte una falta de estandarización en los procedimientos y protocolos técnicos de manejo de evidencia tecnológica. La insuficiente capacitación de los operadores judiciales y la carencia de infraestructura forense moderna debilitan la preservación y trazabilidad de la prueba digital. Estas deficiencias provocan incertidumbre sobre la integridad y fiabilidad de la evidencia, generando riesgos de nulidad procesal y afectando el valor dogmático de la prueba dentro del proceso penal.

3.3. Admisibilidad y valoración probatoria

El derecho a la prueba se encuentra sujeto a un control jurisdiccional basado en el principio de legalidad (Sentencia 2170-18- EP de 2020), cuando se trate de datos privados o comunicaciones protegidas, pero en la práctica, no siempre se cumple esta exigencia. Se han identificado casos en los que grabaciones o capturas digitales se incorporan al proceso penal de manera incorrecta puesto que se debe proporcionar el dispositivo electrónico para poder realizar el análisis técnico de la existencia de dicha evidencia digital, y en algunos casos sin autorización judicial, vulnerando el derecho a la intimidad y el debido proceso. El protocolo de reconocimiento de medios digitales emitido por la Fiscalía General del Estado (Resolución No. 073-FGE-2014), ha sido objeto de controversia precisamente por la falta de garantías de contradicción o control judicial.

En el ámbito de la valoración, los jueces enfrentan limitaciones técnicas que dificultan la apreciación objetiva de las pruebas digitales; como señala González (2021), la insuficiencia de formación en materia tecnológica y la ausencia de lineamientos uniformes, ocasionan decisiones inconsistentes o carentes de sustento probatorio sólido. Esta

situación exige la necesidad de fortalecer las capacidades técnicas y el desarrollo de criterios jurisprudenciales claros sobre la admisibilidad y la valoración de la evidencia electrónica.

3.4. Principios del debido proceso, presunción de inocencia y contradicción

De conformidad con el **Artículo 76** numeral 7 que se encuentra normado en la Constitución de la República del Ecuador de 2008, la cual en adelante se la denominará por los acrónimos CRE, estipula que el respeto al debido proceso se ve comprometido cuando la evidencia digital se obtiene sin autorización judicial o sin permitir la contradicción procesal. La falta de notificación al investigado es una omisión que representa vulneración directa a las garantías constitucionales y al principio de contradicción para impugnar la validez de la prueba tecnológica.

A su vez, el principio de presunción de inocencia se ve afectado cuando se pretende sustentar una acusación en pruebas cuya autenticidad o integridad es dudosa. Si el origen o la licitud de la evidencia no son comprobables, esta no debe alterar la carga de la prueba en perjuicio del procesado, pues ello atentaría contra los fundamentos dogmáticos de imparcialidad y equidad procesal.

A pesar de que el COIP de 2023 incorpora disposiciones específicas sobre la evidencia digital como los Artículos 17, 477.1 y 500, persisten vacíos significativos tanto a nivel normativo como procedimental. No existen protocolos técnicos uniformes ni estándares nacionales que regulen los peritajes digitales. De igual manera, las responsabilidades de los operadores judiciales y los límites de la admisibilidad de las pruebas tecnológicas no están claramente definidos. Entre los retos prácticos más relevantes se encuentran la escasez de peritos especializados, la falta de equipamiento forense adecuado y la limitada comprensión judicial sobre los procesos de extracción y verificación digital.

Desde un punto de vista interpretativo,

la disparidad de criterios entre jueces y fiscales sobre lo que constituye evidencia lícita en el ámbito digital, ha generado inseguridad jurídica. Mientras algunos operadores exigen un alto nivel de certeza técnica para admitir la prueba, otros valoran el elemento digital con criterios flexibles, generando una falta de coherencia en la aplicación de los principios de legalidad, autenticidad y valoración racional.

En síntesis, los hallazgos revelan que la adaptación del sistema probatorio penal ecuatoriano frente a la evidencia tecnológica, sigue siendo parcial e insuficiente. Si bien el marco normativo ha avanzado en reconocer la naturaleza y relevancia de la prueba digital, persisten tensiones estructurales entre la dogmática clásica y las nuevas exigencias tecnológicas. Ello impone la necesidad de desarrollar estándares técnicos, reforzar la formación de los operadores judiciales y consolidar un enfoque garantista que permita armonizar la eficacia de la justicia penal con la protección de los derechos fundamentales en la era digital.

Los tratadistas Naula-Beltrán y Quevedo-Quinteros (2022), sostienen que la falta de protocolos claros, la debilidad en la cadena de custodia y la insuficiente formación técnica de los operadores judiciales, constituyen barreras sustanciales que obstaculizan el uso efectivo de las pruebas digitales en el proceso penal ecuatoriano. Además, los autores enfatizan que, si no se garantiza el origen del indicio y la preservación adecuada de la cadena de custodia, no es posible referirse a un debido proceso y menos aún respecto al derecho a la defensa que asiste a toda persona.

Por su parte, Echeverría-Espinoza y Álvarez-Vera (2024) señalan que, aunque existen técnicas y herramientas forenses para delitos informáticos reconocidas en Ecuador, las normativas legales no siempre incluyen mecanismos que garanticen su aplicación práctica, especialmente respecto a la admisibilidad y autenticidad de la evidencia digital. Esta postura evidencia la brecha existente entre el desarrollo tecnológico y la normativa procesal dentro del sistema oral acusatorio ecuatoriano, donde se observan

las falencias o desventajas derivadas del desconocimiento sobre el uso de recursos técnicos para la identificación y análisis de evidencias digitales, lo que limita su explotación y eficacia de los resultados en el ámbito judicial.

En consonancia con lo indicado Imaicela y Alvarado (2024), comparan el marco ecuatoriano con los de Colombia y China, y concluyen que, aunque la normativa nacional reconoce a los documentos digitalizados la misma validez que a los físicos, persisten importantes desafíos relacionados con la seguridad jurídica, la autenticidad y los estándares técnicos aplicables. Los tratadistas sostienen que la modernización normativa en materia digital no ha sido suficiente para garantizar la fiabilidad de la evidencia tecnológica dentro del proceso penal. La equiparación formal de documentos físicos y electrónicos carece de eficacia práctica si no se acompaña de protocolos técnicos y jurídicos concisos que aseguren la integridad y trazabilidad de la información digital presentada como prueba.

De manera complementaria a las posturas anteriores, Grijalva y Loarte (2017) proponen que uno de los principales problemas radica en la carencia de un proceso normado que guíe a los peritos informáticos en el uso y aplicación de buenas prácticas, métodos y técnicas que aseguren que la evidencia digital obtenida se trate de forma íntegra y legítima conforme al derecho vigente.

Esta teoría, coincide en parte con los autores antes mencionados respecto a las limitaciones institucionales que afectan la eficacia del indicio y/o prueba digital; ergo, introduce un esquema relevante al enfocar la problemática en el ámbito pericial, la ausencia de lineamientos o protocolos técnicos para los peritos genera vacíos en la cadena de custodia y en la fiabilidad de los procedimientos de toma de muestras y análisis de evidencia digital, comprometiéndolo su autenticidad y valor probatorio de los elementos tecnológicos que a futuro serán producidos en la etapa de juicio.

Al margen de la discusión, AllahRakha (2024) destaca que la falta de estándares y

regulaciones específicas para la recopilación, preservación y análisis de pruebas digitales, obstaculiza su admisibilidad en juicios penales, pues sin estos estándares no hay certeza de integridad, autenticidad o cadena de custodia adecuada. De lo indicado en líneas precedentes por el autor, si se compara con la normativa penal ecuatoriana el legislador ha insertado reformas en el COIP, tal como lo establece el **Artículo 500**, pero la falta de protocolos técnicos específicos para la gestión de pruebas digitales, constituye una limitación significativa en el proceso penal generando una inseguridad jurídica y el riesgo de inadmisibilidad de la prueba digital en los tribunales.

Mousa (2021), sostiene que los delitos electrónicos se cometen en un entorno virtual, sin el uso de documentos físicos, donde la tecnología informática e *internet* permiten a los delincuentes alterar datos y programas poco después de cometer el ilícito, lo que puede anular la evidencia. Esta característica dificulta la recopilación y preservación de pruebas por parte de los investigadores. El autor destaca que, debido al rápido avance de la tecnología, han surgido nuevos tipos de delitos electrónicos con métodos diversos y dinámicos, en el que inclusive pueden eliminar las pruebas y complicar la obtención, identificación y clasificación de la evidencia, lo que a su vez dificulta demostrar hechos y posteriori ante un tribunal.

Mientras los autores precedentes analizan las limitaciones normativas e institucionales en la gestión de la prueba digital, Moussa (2021) profundiza en la naturaleza propia del delito informático y las dificultades inherentes a la obtención y preservación de evidencia electrónica.

Se considera correcta la apreciación de Peake (2024), quien argumenta que los tribunales internacionales enfrentan dificultades para garantizar la disponibilidad, fiabilidad y admisibilidad de la evidencia digital, debido a eliminación y deficiencias en la cadena de custodia digital. Esta postura, amplía la discusión al ámbito internacional y confirma que los desafíos en torno a la prueba

digital no son exclusivos de los sistemas judiciales nacionales.

La volatilidad de los datos electrónicos, sumada a la ausencia de protocolos globalmente estandarizados, obstaculiza la valoración y legitimidad de la evidencia tecnológica. El análisis de Peake (2024), resulta pertinente al evidenciar que la falta de mecanismos técnicos y normativos adecuados limita la eficacia y vulnerabilidad inherente a datos electrónicos, almacenamientos en la nube, copias de seguridad o *backups*, registros de transferencias bancarias digital, transacciones en dinero electrónico, incluido movimientos en criptomonedas, firmas digitales, obteniendo su fecha de creación y modificación, direcciones IP, geolocalización, entre otros.

Un crítico de la postura como lo es Shukla (2023) advierte que, en sistemas legales con poca experiencia en tecnología forense, los jueces a menudo carecen de formación para comprender el análisis técnico detrás de la evidencia digital, lo que puede llevar a decisiones inconsistentes o poco fundamentadas. Esta observación no solo pone de manifiesto la necesidad de fortalecer las capacidades técnicas del juzgador, sino también la de los abogados defensores, quienes deben contar con conocimientos especializados para objetar o autenticar la prueba digital.

Sin una preparación adecuada en materia de informática forense, cadena de custodia y estándares de integridad digital, el abogado carece de herramientas efectivas para contradecir la evidencia tecnológica presentada en juicio, afectando así el equilibrio procesal y el ejercicio pleno del derecho a la defensa, en lo denominado la triada del proceso penal (juez, fiscal y defensa).

Frente a esta problemática, Rosales (2023) advierte que el principio del debido proceso en los sistemas judiciales latinoamericanos, enfrenta serias tensiones derivadas de la falta de transparencia, la limitada imparcialidad y la deficiente intervención judicial efectiva al momento de admitir o valorar pruebas digitales. Estas deficiencias se acentúan cuando la evidencia tecnológica es incorporada al proceso sin la

debida autorización judicial o sin haberse garantizado el derecho a la contradicción, circunstancias que pueden comprometer derechos fundamentales y afectar la búsqueda de la verdad procesal. En consecuencia, resulta imperativo fortalecer los mecanismos institucionales y normativos que aseguren la licitud, integridad y autenticidad de la prueba digital.

De forma complementaria, Arias y Cedeño (2024), enfatizan que la incorporación de los distintos medios de prueba documentales, testimoniales o periciales, debe efectuarse bajo estricto respeto a los principios de inmediación y contradicción, puesto que son estos los que permiten al juez alcanzar una convicción razonada sobre los hechos y la responsabilidad penal. La omisión de tales principios compromete la legitimidad dogmática de la prueba y afecta el equilibrio del proceso penal.

En ese sentido, la observancia rigurosa de los principios de inmediación y contradicción no solo constituye una garantía procesal, sino también un requisito indispensable para la validez de la actividad probatoria. Por ello, resulta necesario que el sistema de administración de justicia implemente protocolos y lineamientos técnicos que orienten la incorporación, control y valoración de la prueba en especial la digital, a fin de evitar vulneraciones al debido proceso y fortalecer la legitimidad de las decisiones judiciales.

Por su parte, Chiluiza (2024) sostiene que, aunque los principios fundamentales del derecho penal ecuatoriano, legalidad, culpabilidad, proporcionalidad y presunción de inocencia, han sido reforzados con las reformas al Código Orgánico Integral Penal, COIP, su aplicación práctica continúa enfrentando debilidades, sobre todo en la valoración de la prueba. Si bien el marco normativo recoge los postulados esenciales de la dogmática penal, la práctica judicial no siempre garantiza la observancia de criterios de legitimidad, integridad y objetividad en el tratamiento de los medios probatorios. Esta brecha entre la norma y su aplicación coloca

de manifiesto la necesidad de consolidar una cultura jurídica coherente con los estándares dogmáticos, capaz de asegurar que la verdad procesal se construya sobre bases técnicas verificables y respetuosas del debido proceso.

En el análisis contemporáneo del proceso penal ecuatoriano, Torres (2022) sostiene que la prueba indiciaria solo adquiere verdadera fuerza probatoria cuando los indicios se sustentan en hechos comprobados y se articulan de manera lógica y coherente, permitiendo al juez construir una convicción racional sin apartarse del principio de presunción de inocencia.

El autor advierte que las conclusiones judiciales no deben derivarse de percepciones subjetivas o conjeturas, sino de un proceso de inferencia sustentado en la razón y en la evidencia empírica. Esta perspectiva refuerza la idea de que la prueba indiciaria, lejos de ser un instrumento de intuición o presunción, requiere un manejo técnico riguroso que garantice la objetividad del juicio. Desde una mirada dogmática, este planteamiento resalta la importancia de la racionalidad judicial como eje del sistema acusatorio, en tanto asegura que la valoración de los medios probatorios se mantenga dentro del marco del debido proceso y de la exigencia de duda razonable que orienta toda decisión legítima en materia penal en aplicación del *onus probandi*.

Se considera preciso comentar desde otra perspectiva lo expuesto por Navas-Abad y Vázquez-Martínez (2025), quien sostiene que la prueba digital se encuentra supeditada a criterios esenciales como la autenticidad, la integridad y la fiabilidad, condiciones que resultan imprescindibles para su admisibilidad en el proceso judicial. La autenticidad, permite demostrar que los datos no han sido alterados desde su recolección; mientras que la integridad, asegura que la información se mantiene completa y sin modificaciones.

Por su parte, la fiabilidad garantiza que la evidencia puede ser reproducida y verificada por peritos independientes, lo que resulta fundamental para respetar el principio de contradicción y permitir que las partes cuestionen la prueba presentada.

La observancia de estos criterios no solo condiciona la validez de la prueba digital, sino que protege el debido proceso, evitando que la evidencia pueda ser impugnada por su dudosa autenticidad o alteración.

Para finalizar este breve repaso, y sin pretender hacer un extenso y minucioso análisis de las criptomonedas, se refiere a Bryans y Jelske (2023), quienes señalan que las criptomonedas pueden ser utilizadas de manera indebida en actividades delictivas, como el lavado de activos, y destacan la importancia de que los reguladores trabajen de manera conjunta con la industria y las autoridades judiciales para desarrollar mecanismos que prevengan su uso ilícito.

Este fenómeno refleja un contexto en el que la digitalización y la innovación tecnológica transforman la forma en que se cometen y se investigan los delitos, planteando nuevos desafíos para la administración de justicia. En el derecho penal ecuatoriano, esta situación pone de relieve la necesidad de adaptar los fundamentos dogmáticos de la prueba a escenarios tecnológicos donde los medios tradicionales de evidencia resultan insuficientes. La valoración de evidencia digital, incluyendo transacciones con criptomonedas, requiere garantizar su autenticidad, integridad y fiabilidad, de manera que los principios de legalidad, culpabilidad y presunción de inocencia se mantengan plenamente reconocidos, asegurando así la legitimidad y eficacia del proceso penal en la era digital.

3.5. Estadísticas de los ciberdelitos cometidos en Ecuador

Efectuado el análisis de los datos estadísticos sobre las Noticias del Delito-NDD, proporcionados por la Dirección de Estadísticas y Sistemas de Información de la Fiscalía General del Estado, referentes a los delitos cometidos mediante el uso de herramientas tecnológicas, correspondientes al período del año 2024 del mes de enero a noviembre, se obtuvo el siguiente resultado en la Tabla 1.

Tabla 1
Denuncias de Delitos con el uso de las TIC durante el año 2024

DELITO	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Total
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	62	63	65	67	110	75	73	81	119	99	80	894
Acoso sexual (inciso 2 - Ciberacoso sexual)	10	5	5	6	8	12	9	6	8	12	5	86
Actos lesivos a los derechos de autor	0	0	0	0	1	1	0	0	0	0	0	2
Apropiación fraudulenta por medios electrónicos	277	286	312	359	326	332	312	305	326	280	270	3.385
Ataque a la integridad de sistemas informáticos	16	21	18	27	30	26	14	21	36	23	12	244
Comercialización de pornografía con utilización de niñas, niños o adolescentes	1	4	3	1	2	3	2	2	3	2	2	25
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	8	16	18	12	18	9	10	7	5	5	8	116
Delitos contra la información pública reservada legalmente	0	0	0	0	0	1	0	1	3	0	0	5
Distribución de material pornográfico a niñas, niños y adolescentes	0	2	3	4	1	0	1	0	0	2	0	13
Estafa (numerales 1 y 2 por medio electrónico)	90	103	102	82	94	81	98	127	77	92	84	1.030
Falsificación informática	6	13	16	8	9	6	12	11	7	11	6	105
Hostigamiento	60	92	74	70	65	61	95	59	66	62	72	776
Intercepción ilegal de datos	8	3	10	7	12	6	5	6	5	3	2	67
Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	1	1	0	3	0	1	1	2	0	0	0	9
Pornografía con utilización de niñas, niños o adolescentes	6	12	13	10	17	14	7	13	16	4	6	118
Reprogramación o modificación de información de equipos terminales móviles	0	0	0	2	0	0	0	2	0	0	0	4
Revelación ilegal de base de datos	5	3	3	5	4	4	6	4	1	3	5	43
Terrorismo (numeral 1)	11	0	2	0	0	1	0	0	0	0	0	14
Transferencia electrónica de activo patrimonial	11	18	23	9	21	13	13	10	10	16	7	151
Violación a la intimidad	138	179	131	153	167	152	170	145	145	138	119	1.637
TOTAL GENERAL	710	821	798	825	885	798	828	802	827	752	678	8.724

Fuente: Fiscalía General del Estado

Conclusiones

Basándose en el desarrollo de este artículo, se puede concluir que el análisis realizado evidencia que el tratamiento de la prueba digital en el sistema probatorio penal ecuatoriano, constituye uno de los mayores desafíos contemporáneos para la administración de justicia. La transición hacia entornos tecnológicos ha desbordado la capacidad normativa y técnica del sistema judicial, generando tensiones entre los principios dogmáticos clásicos como la legalidad, la autenticidad, la contradicción y la presunción de inocencia y las nuevas exigencias que plantea la evidencia electrónica.

El estudio aporta una comprensión crítica sobre la insuficiencia estructural

del marco procesal ecuatoriano frente a la gestión de pruebas digitales, identificando vacíos normativos, técnicos y formativos que obstaculizan la consolidación de un modelo garantista en materia probatoria. Se destaca la necesidad urgente de estandarizar los protocolos de cadena de custodia, preservar la integridad de los datos y fortalecer la capacitación de los operadores judiciales, de modo que la valoración de la evidencia tecnológica se realice con rigor metodológico y coherencia jurídica.

El aporte principal de esta investigación radica en visibilizar la brecha existente entre la teoría y la práctica judicial, proponiendo la articulación de un enfoque integral que combine la dogmática penal con la informática forense. Solo a través de esta sinergia es

posible consolidar un sistema probatorio capaz de responder con eficacia a los retos de la era digital sin vulnerar las garantías procesales.

Las líneas de investigación que se proyectan a partir de este estudio incluyen el desarrollo de estándares técnicos nacionales para la gestión de evidencia digital, la creación de una normativa especializada que regule la actuación de los peritos forenses informáticos, y el fortalecimiento de la formación tecnológica en la judicatura y la defensa. Asimismo, se plantea como eje futuro el análisis e implementación de buenas prácticas que permitan adaptar el proceso penal ecuatoriano a las exigencias de transparencia, trazabilidad y seguridad jurídica propias de la justicia digital.

En suma, el tratamiento de la prueba digital exige una transformación estructural del sistema penal ecuatoriano, sustentada en criterios científicos, tecnológicos y dogmáticos que garanticen la verdad procesal y la protección efectiva de los derechos fundamentales.

Asimismo, la capacidad de reproducir y verificar la información fortalece la transparencia y objetividad del juicio, por lo que tanto jueces como abogados requieren formación específica en materia de informática forense para evaluar adecuadamente la validez y confiabilidad de la evidencia digital, para garantizar que la prueba digital cumpla con los principios de legalidad, autenticidad e integridad dentro del proceso penal.

Referencias bibliográficas

- Abraha, H. H. (2021). Acceso de las fuerzas del orden a las pruebas electrónicas transfronterizas: análisis de enfoques políticos e iniciativas de reforma emergentes. *Revista Internacional de Derecho y Tecnologías de la Información*, 29(2), 118-153. <https://doi.org/10.1093/ijlit/eaab001>
- AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexicans Law Review*, XVI(2), 23-54. <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>
- Arias, V. H., y Cedeño, L. F. (2024). Análisis de la confiabilidad en la incorporación de los medios de prueba en materia penal en el Ecuador. *Revista Religación*, 9(41), e2401306. <https://doi.org/10.46652/rgn.v9i41.1306>
- Arnold, D. (2021). Las evidencias y pruebas como fundamento de validez científica en las auditorías forenses. *Revista Colón Ciencias Tecnologías y Negocios*, 8(2), 121-137. https://revistas.up.ac.pa/index.php/revista_colon_ctn/article/view/2243/2077
- Bryans, D., y Jelske, F. (2023). Bitcoin and money laundering: Mining for an effective solution. In K. J. McCarthy (Ed.), *The Money Laundering Market* (pp.139-170). Cambridge University Press. <https://doi.org/10.1017/9781911116448.006>
- Centeno, E., Mondragón, S. L., Ospina, E. F., y Franco, L. M. (2022). Resocialización de la pena: Retos desde las nuevas tecnologías de la información y la comunicación. *Revista de Ciencias Sociales (Ve)*, XXVIII(4), 303-314. <https://doi.org/10.31876/rcs.v28i4.39132>
- Chiluiza, E. E. (2024). Principios del Derecho Penal en el Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, 8(3), 143-154. https://doi.org/10.37811/cl_rcm.v8i3.11189
- Código Orgánico Integral Penal [COIP]. 3 de agosto de 2023.
- Constitución de la República del Ecuador. Registro Oficial 449 de 20 de octubre de 2008. Última modificación: 25 de enero de 2021.

- Corte Constitucional del Ecuador. Sala Penal. Sentencia juicio 2170-18- EP, 29 de julio de 2020.
- Delso, A. T., Almonacid, M., y García, M. (2024). La evolución del metaverso y su influencia en la realidad digital: Una revisión y líneas de investigación futura. *European Public & Social Innovation Review*, 9, 1-22. <https://doi.org/10.31637/epsir-2024-546>
- Echeverría-Espinoza, E. A., y Alvarez-Vera, M. S. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revisión sistemática. *593 Digital Publisher CEIT*, 9(6), 644-652. <https://doi.org/10.33386/593dp.2024.6.2775>
- Gonzalez, J. M. (2021). La prueba pericial digital y la cadena de custodia. *Anales de la Facultad de Derecho*, 38, 43-79. <https://doi.org/10.25145/j.anfade.2021.38.03>
- Grijalva, J. S., y Loarte, B.-R. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador. *CienciaAmérica*, 6(3). <https://cienciaamerica.edu.ec/index.php/uti/article/view/99>
- Imaicela, J. A., y Alvarado, L. A. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano. *Revista de Investigación en Ciencias Jurídicas, Lex*, 7(27), 1338-1350. <https://doi.org/10.33996/revistalex.v7i27.247>
- Levin, I., y Mamlok, D. (2021). Cultura y sociedad en la era digital. *Informacion*, 12(2), 68. <https://doi.org/10.3390/info12020068>
- Martínez, G. (2022). Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología*, 24, 23. <http://criminet.ugr.es/recpc/24/recpc24-23.pdf>
- Mejía-Lobo, M., Hurtado-Gil, S. V., y Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales (Ve)*, XXIX(2), 356-372. <https://doi.org/10.31876/rcs.v29i2.39981>
- Ministerio del Interior de Ecuador – MIE (2024). *Boletín de Análisis de la Ciberdelincuencia: La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial*. MIE. <https://www.ministeriodelinterior.gob.ec/wp-content/uploads/downloads/2025/07/Boletin-La-nueva-era-de-la-ciberdelincuencia-el-lado-oscuro-de-la-Inteligencia-Artificial.pdf>
- Molano, M., Valencia, A. M., y Apraez, M. (2021). Características e importancia de la metodología cualitativa en la investigación científica. *Semillas del Saber*, 1(1), 18-27. <https://revistas.unicatolica.edu.co/revista/index.php/semillas/article/view/314>
- Mousa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11, 20. <https://doi.org/10.1186/s41935-021-00234-6>
- Naula-Beltran, D. E., y Quevedo-Quintero, R. (2022). El protocolo de reconocimiento de medios digitales frente a la inobservancia del debido proceso penal. *Revista Arbitrada Interdisciplinaria KOINONIA*, 7(1), 209-229. <https://doi.org/10.35381/r.k.v7i1.1785>
- Navas-Abad, C. E., y Vázquez-Martínez, D. S. (2025). La importancia de la prueba digital en los procedimientos penales en Ecuador. *Polo del Conocimiento*, 10(1). <https://polodelconocimiento.com/ojs/index.php/es/article/view/8778>

- Peake, J. (2024). Challenges of Using Digital Evidence for War Crimes Prosecutions: Availability, Reliability, Admissibility. *AJIL Unbound*, 118. <https://doi.org/10.1017/aju.2024.5>
- Puetate, J. M., Coka, D. F., y Méndez, C. M. (2021). La prueba digital en procesos judiciales aplicables al Código Orgánico General de Procesos (COGEP), a partir de la pandemia COVID-19. *Revista Dilemas Contemporáneos: Educación, Política y Valores*, 8(17). <https://doi.org/10.46377/dilemas.v8i.2696>
- Resolucion No. 073-FGE-2014 [Fiscalía General del Estado]. 7 de agosto de 2014.
- Rosales, C. M. (2023). Forensic study of the principle of due process in Latin America. *Revista Quaestio Iuris*, 16(1), 99-122. <https://doi.org/10.12957/rqi.2023.71298>
- Santacruz, R. (2013). La prueba como elemento en un sistema penal. *Ciencia Jurídica*, 1(3), 163-172. <https://www.cienciajuridica.ugto.mx/index.php/CJ/>
- [es/article/view/57/56](https://article/view/57/56)
- Shukla, V. (2023). The admissibility of digital evidence: challenges and future implications. *Commonwealth Law Review Journal*, 9, 464-476. <https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf>
- Torres, Á. L. (2022). Aplicación de la prueba indiciaria en el proceso penal ecuatoriano y la duda razonable. *Revista Metropolitana de Ciencias Aplicadas*, 5(S-1), 128-137. <https://doi.org/10.62452/vzhkgk23>
- Ward, T. (2020). Explicación y confianza en la evidencia pericial: ¿Qué es una «base científica suficientemente fiable»? *The International Journal of Evidence & Proof*, 24(3), 233-254. <https://doi.org/10.1177/1365712720927622>
- Whalen, R. (2022). Defining legal technology and its implications. *International Journal of Law and Information Technology*, 30(1), 47-67. <https://doi.org/10.1093/ijlit/eaac005>