ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

Admisibilidad y valoración de la prueba digital en los procesos penales en Ecuador: desafíos y estándares jurídicos en la era de la ciberdelincuencia

Admissibility and evaluation of digital evidence in criminal proceedings in Ecuador: challenges and legal standards in the era of cybercrime

[1] Bebsi Alexandra Paredes Carcelén https://orcid.org/0009-0006-3105-6308
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador.
Maestría en Derecho Penal
baparedesc@ube.edu.ec

[2] Micaela Rashell Zapata Morejón https://orcid.org/0009-0001-6714-010X
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador.
mrzapatam@ube.edu.ec

[3] Sylka Noelia Zapata Morejón https://orcid.org/0009-0009-1907-3553
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador.
snzapatam@ube.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 10/06/2026
Revisado: 13/09/2026
Aceptado: 30/10/2026
Publicado: 13/11/2026
DOI: **https://doi.org/10.33262/visionariodigital.v10i4.3820**

Cítese: Paredes Carcelén, B. A., Zapata Morejón, M. R., & Zapata Morejón, S. N. (2026). Admisibilidad y valoración de la prueba digital en los procesos penales en Ecuador: desafíos y estándares jurídicos en la era de la ciberdelincuencia. Visionario Digital, 10(4), 332-354. https://doi.org/10.33262/visionariodigital.v10i4.3820

VISIONARIO DIGITAL, *es* una revista científica, **trimestral,** que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://visionariodigital.org
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Esta revista está protegida bajo una licencia Creative Commons Atribución-No Comercial-Compartir Igual 4.0 International. Copia de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

Palabras claves:
Admisibilidad; ciberdelincuencia; cadena de custodia; autenticidad; valoración probatoria; prueba digital.

Resumen

Introducción. La prueba digital en los procesos penales constituye un tema de especial relevancia en la era tecnológica, debido a que su adecuado tratamiento incide en la seguridad jurídica y en la efectividad de la persecución penal. **Objetivos.** El objetivo de este artículo es analizar los criterios de admisibilidad y valoración de la prueba digital en casos de ciberdelincuencia en Ecuador. **Metodología.** Se emplea una metodología cualitativa y dogmático-jurídica, basada en la revisión documental de normativa, jurisprudencia y doctrina, complementada con un enfoque comparado orientado a identificar vacíos y proponer lineamientos técnico-jurídicos. **Resultados.** La revisión realizada identifica ambigüedades normativas, deficiencias relacionadas con la cadena de custodia, limitaciones en la capacitación técnica de los operadores de justicia y ausencia de protocolos forenses suficientemente estandarizados, factores que pueden incidir en la admisibilidad y valoración de la evidencia digital. **Conclusiones.** Se concluye en la necesidad de fortalecer el sistema probatorio digital mediante criterios regulatorios más precisos, protocolos técnico-forenses y formación especializada de jueces, fiscales y peritos, con el propósito de favorecer un tratamiento de la prueba digital más sólido, previsible y garantista frente a la ciberdelincuencia. **Área de estudio general:** Derecho. **Área de estudio específica:** Derecho Penal, con énfasis en prueba digital y ciberdelincuencia.

Tipo de artículo: Revisión bibliográfica narrativa.

Keywords:
Admissibility; cybercrime; chain of custody; authenticity; evidentiary assessment; digital evidence.

Abstract

Introduction. Digital evidence in criminal proceedings is a topic of special relevance in the technological era because its proper treatment affects legal certainty and the effectiveness of criminal prosecution. **Objectives. The** objective of this article is to analyze the criteria for admissibility and assessment of digital evidence in cases of cybercrime in Ecuador. **Methodology.** A qualitative and dogmatic-legal methodology is used, based on the documentary review of regulations, jurisprudence, and doctrine, complemented by a comparative approach aimed at identifying gaps and proposing technical-legal guidelines. **Results.** The review identifies regulatory ambiguities, deficiencies related to the chain of custody, limitations in the

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

technical training of justice operators and the absence of sufficiently standardized forensic protocols, factors that may affect the admissibility and valuation of digital evidence. **Conclusions.** It is concluded that there is a need to strengthen the digital evidence system through more precise regulatory criteria, technical-forensic protocols and specialized training of judges, prosecutors, and experts, to favor a more solid, predictable, and guaranteeing treatment of digital evidence against cybercrime. **General area of study:** Law. **Specific area of study:** Criminal Law, with emphasis on digital evidence and cybercrime. **Type of article:** Narrative bibliographic review.

1. Introducción

La admisibilidad y valoración de la prueba digital en el proceso penal ecuatoriano deben analizarse a partir de las garantías constitucionales que rigen la actividad probatoria. El artículo 76 de la Constitución de la República del Ecuador reconoce el derecho al debido proceso y establece que las pruebas obtenidas o actuadas con violación de la Constitución o la ley carecen de validez y eficacia probatoria (Asamblea Nacional Constituyente del Ecuador, 2008). Asimismo, el artículo 66 reconoce, entre otros derechos, la intimidad personal y familiar y la protección de datos de carácter personal, garantías que adquieren particular relevancia cuando la información utilizada con fines probatorios procede de dispositivos electrónicos, comunicaciones digitales, redes sociales o sistemas informáticos (Asamblea Nacional Constituyente del Ecuador, 2008). En este contexto, la obtención e incorporación de evidencia digital exige observar los principios de legalidad, necesidad y proporcionalidad, así como el respeto de los derechos fundamentales.

La transformación digital de la sociedad ha modificado las dinámicas sociales y económicas y, paralelamente, las formas de comisión e investigación de determinadas conductas delictivas. La ciberdelincuencia plantea especiales dificultades para los sistemas de justicia penal debido, entre otros factores, a su dimensión transnacional, la constante evolución tecnológica y la volatilidad de determinados datos digitales. El Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), constituye uno de los principales instrumentos internacionales para afrontar este fenómeno y establece mecanismos dirigidos tanto a la persecución de determinadas conductas como a la obtención y conservación de evidencia electrónica. Estas particularidades exigen adaptar las herramientas procesales a las características propias de la investigación en entornos digitales.

En Ecuador, la incorporación de los delitos informáticos al Código Orgánico Integral Penal (COIP) representó un avance en la respuesta jurídica frente a las nuevas manifestaciones de criminalidad asociadas al uso de tecnologías (Asamblea Nacional del

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

Ecuador, 2014). Sin embargo, la tipificación de las conductas resulta insuficiente si no se encuentra acompañada de mecanismos probatorios capaces de garantizar la obtención, preservación, incorporación y valoración adecuada de la evidencia digital. Esta, entendida como información generada, almacenada, procesada o transmitida mediante medios electrónicos con aptitud para acreditar hechos relevantes dentro de un proceso, presenta características particulares derivadas de su intangibilidad, reproducibilidad, susceptibilidad de alteración y dependencia de procedimientos técnicos para verificar su origen e integridad.

La problemática objeto de esta investigación no se limita, por tanto, a una brecha genérica entre derecho y tecnología. En el proceso penal ecuatoriano pueden identificarse tres núcleos específicos de incertidumbre. El primero se relaciona con la suficiencia de los criterios jurídicos y técnicos utilizados para determinar cuándo una evidencia digital puede considerarse auténtica, íntegra y lícitamente obtenida. El segundo se refiere a la ausencia de parámetros suficientemente uniformes para documentar su adquisición, preservación, extracción, análisis y transferencia dentro de la cadena de custodia. El tercero concierne a la necesidad de diferenciar los defectos que pueden comprometer la admisibilidad de la evidencia de aquellas irregularidades que, sin justificar necesariamente su exclusión, pueden disminuir su fuerza probatoria. Esta distinción resulta fundamental para evitar tanto la exclusión automática de evidencia potencialmente fiable por deficiencias no sustanciales como la incorporación de material cuya autenticidad, integridad o licitud no haya sido suficientemente acreditada.

El problema presenta, en consecuencia, dimensiones normativas, interpretativas e institucionales. Desde la perspectiva normativa, las disposiciones generales del COIP en materia de cadena de custodia, contenido digital y valoración probatoria requieren ser interpretadas frente a fuentes de evidencia de diversa naturaleza, como teléfonos móviles, aplicaciones de mensajería instantánea, metadatos, registros de sistemas, información almacenada en la nube o datos cifrados. Desde la dimensión interpretativa, persisten interrogantes respecto de los mecanismos idóneos para acreditar autenticidad e integridad y sobre las consecuencias procesales derivadas de las irregularidades producidas durante la obtención o tratamiento de la evidencia. Finalmente, desde la perspectiva institucional, la adecuada aplicación de estos estándares se encuentra vinculada con las capacidades técnicas y forenses de los operadores que intervienen en la investigación y el proceso penal.

La literatura especializada ha advertido dificultades relacionadas con la aplicación de la normativa vigente, la preservación de la cadena de custodia y la ausencia de criterios técnicos suficientemente uniformes para el tratamiento de evidencia digital (Iglesias et al., 2025; Morante et al., 2025). Asimismo, se han identificado necesidades de capacitación especializada para el manejo y valoración de evidencias tecnológicas complejas (Coronel & Argüello, 2023). Estas circunstancias justifican examinar de manera conjunta las exigencias jurídicas y técnicas que condicionan la incorporación y

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

valoración de la prueba digital, evitando asumir que toda irregularidad produce idénticas consecuencias procesales.

La investigación se justifica académicamente por la necesidad de sistematizar los criterios jurídicos aplicables a la prueba digital en el proceso penal ecuatoriano y analizar su relación con las exigencias técnicas propias de esta clase de evidencia. Desde una perspectiva práctica, el estudio busca contribuir a la identificación de parámetros que permitan fortalecer la seguridad jurídica, la contradicción probatoria y la protección de los derechos fundamentales, sin desconocer las necesidades legítimas de investigación y persecución de la ciberdelincuencia.

En este marco, el objetivo del estudio consiste en analizar los criterios de admisibilidad y valoración de la prueba digital en los procesos penales ecuatorianos relacionados con casos de ciberdelincuencia, a fin de identificar los principales desafíos normativos, interpretativos y prácticos y proponer lineamientos técnico-jurídicos que contribuyan a un tratamiento probatorio más sólido, previsible y garantista.

2. Metodología

El estudio se desarrolló mediante un enfoque cualitativo y dogmático-jurídico, orientado al análisis crítico de los fundamentos normativos, doctrinales y jurisprudenciales aplicables a la prueba digital en Ecuador. Se adoptó un alcance descriptivo-analítico, dirigido a interpretar y sistematizar las disposiciones jurídicas y los criterios relevantes en materia de admisibilidad y valoración de la evidencia digital, con el propósito de identificar vacíos, problemas interpretativos y posibles lineamientos de mejora dentro del marco garantista del proceso penal.

La recolección de información se realizó mediante revisión documental de fuentes primarias y secundarias. Entre las fuentes primarias se consideraron normas del ordenamiento jurídico ecuatoriano relacionadas con el objeto de estudio, particularmente el Código Orgánico Integral Penal (COIP) (Asamblea Nacional del Ecuador, 2014), la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Congreso Nacional del Ecuador, 2002), y la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021), así como instrumentos internacionales relevantes, entre ellos el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001). Asimismo, se examinó jurisprudencia y criterios jurídicos nacionales relacionados con la prueba digital. Como parte del análisis comparado, se incorporaron pronunciamientos relevantes de órganos jurisdiccionales de España y Colombia. Las fuentes secundarias comprendieron doctrina especializada, artículos científicos, libros y trabajos académicos vinculados con la admisibilidad, autenticidad, integridad, cadena de custodia y valoración de la evidencia digital.

La búsqueda documental se efectuó mediante descriptores como «prueba digital», «ciberdelincuencia», «admisibilidad probatoria», «autenticidad de la evidencia digital» y «cadena de custodia digital», utilizando SciELO, Dialnet, Google Académico y

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

repositorios institucionales. Para la selección de las fuentes se consideraron su pertinencia temática, vinculación con el proceso penal y contribución al análisis jurídico de la evidencia digital. Se priorizaron publicaciones científicas correspondientes al período 2021-2025, sin excluir investigaciones anteriores que, por su relevancia doctrinal y técnica, resultaron necesarias para el desarrollo del estudio. Respecto de las fuentes normativas y jurisprudenciales, su selección respondió a la pertinencia jurídica y al valor interpretativo de sus disposiciones y pronunciamientos, independientemente de su fecha de expedición.

Para el tratamiento de la información se emplearon técnicas propias de la investigación jurídica. Mediante el análisis de contenido se examinaron las disposiciones normativas y los pronunciamientos jurisprudenciales seleccionados, así como los aportes doctrinales identificados, con el propósito de establecer criterios relacionados con la licitud, autenticidad, integridad, cadena de custodia y valoración probatoria. Asimismo, se aplicó el método comparado mediante el contraste de criterios desarrollados en España y Colombia con el marco jurídico ecuatoriano, a fin de identificar semejanzas, diferencias y referentes susceptibles de consideración en el contexto nacional. Finalmente, los resultados se sistematizaron mediante una síntesis interpretativa que permitió relacionar los fundamentos doctrinales con las disposiciones normativas y los criterios jurisprudenciales examinados.

La investigación presenta las limitaciones propias de su carácter documental. Al sustentarse en fuentes normativas, doctrinales y jurisprudenciales disponibles, no permite determinar empíricamente la frecuencia con la que las dificultades identificadas se presentan en la práctica ni incorporar de manera directa las experiencias de jueces, fiscales, defensores, investigadores o peritos. En consecuencia, las conclusiones se circunscriben al ámbito jurídico-documental analizado. Futuras investigaciones podrán complementar estos resultados mediante estudios empíricos, entrevistas a operadores de justicia y análisis de expedientes, con el propósito de contrastar la aplicación práctica de los estándares examinados.

3. Resultados

Los resultados de la investigación se presentan a partir del análisis doctrinal, normativo y jurisprudencial de la prueba digital en el sistema penal ecuatoriano, con especial atención a los criterios que determinan su admisibilidad y valoración en los casos de ciberdelincuencia. A través de la revisión documental se identifican los principales fundamentos jurídicos que regulan su tratamiento procesal, así como las dificultades técnicas y jurídicas relacionadas con la autenticidad, integridad, cadena de custodia y fiabilidad de la evidencia digital. Asimismo, se examinan los desafíos que enfrenta el sistema de justicia penal ecuatoriano en la aplicación de estos criterios, con el propósito de establecer los principales hallazgos de la investigación y su incidencia en la garantía del debido proceso y la seguridad jurídica.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

3.1.Fundamentos doctrinales y jurisprudenciales de la prueba digital en Ecuador

Desde una perspectiva doctrinal, la prueba digital puede entenderse como aquella información generada, almacenada, procesada o transmitida mediante sistemas informáticos o dispositivos electrónicos que posee aptitud para acreditar hechos relevantes dentro de un proceso judicial. Su naturaleza presenta particularidades frente a los medios probatorios tradicionales, entre ellas su intangibilidad, reproducibilidad, dependencia tecnológica y susceptibilidad de alteración, características que hacen especialmente relevante la utilización de mecanismos técnicos que permitan verificar su origen, integridad y trazabilidad.

En el ordenamiento jurídico ecuatoriano, el tratamiento de la evidencia digital encuentra sustento tanto en las garantías constitucionales relativas al debido proceso y la licitud probatoria como en las disposiciones del Código Orgánico Integral Penal (COIP) aplicables a su obtención, conservación, incorporación y valoración. En particular el artículo 456 establece la cadena de custodia respecto de los elementos físicos o contenidos digitales materia de prueba, con la finalidad de garantizar su autenticidad mediante la acreditación de su identidad y estado original (Asamblea Nacional del Ecuador, 2014). Por su parte, el artículo 457 dispone que la valoración de la prueba debe considerar su legalidad, autenticidad, sometimiento a cadena de custodia y los criterios técnicos y científicos aplicables a los informes periciales ((Asamblea Nacional del Ecuador, 2014).

Los mensajes de datos y las comunicaciones provenientes de aplicaciones de mensajería instantánea plantean dificultades particulares en materia de autenticación y valoración. Su aptitud probatoria no depende exclusivamente de su presentación material dentro del proceso, sino de la posibilidad de establecer suficientemente su origen, integridad y correspondencia con las personas o dispositivos a los que se atribuyen. En este sentido, la normativa sobre mensajes de datos, juntamente con las reglas procesales aplicables y los aportes doctrinales sobre evidencia digital, proporciona criterios para analizar su eficacia probatoria (Herrera, 2025).

La Corte Nacional de Justicia del Ecuador (2021) mediante la absolución de consulta No. 0120-AJ-P-CNJ-2021, abordó la utilización de documentos electrónicos y mensajes de datos como medios probatorios. Este pronunciamiento constituye un referente interpretativo para examinar la autenticidad e integridad de este tipo de información, aunque debe considerarse su naturaleza de criterio no vinculante. Desde esta perspectiva, las deficiencias relacionadas con la acreditación de autenticidad o integridad deben analizarse atendiendo a las circunstancias concretas y a su incidencia sobre la fiabilidad del elemento probatorio, evitando asumir que toda irregularidad produce necesariamente su exclusión automática.

Especial atención merecen las capturas de pantalla de conversaciones mantenidas mediante aplicaciones como WhatsApp. Su sola presentación puede resultar insuficiente cuando existe controversia respecto de la autoría, integridad, origen o posible manipulación del contenido. En tales casos, pueden resultar necesarios mecanismos

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

adicionales de corroboración, entre ellos el examen del dispositivo de origen, el análisis de metadatos, la identificación de cuentas o números asociados, la información proporcionada por los intervinientes o proveedores cuando legalmente corresponda y, particularmente, la pericia informática. La protocolización notarial puede contribuir a documentar la existencia o exhibición de determinado contenido, pero no sustituye por sí misma la verificación técnica de su autenticidad e integridad. Por ello, la suficiencia probatoria debe analizarse en función de las características del caso y de los mecanismos objetivos de corroboración disponibles (Borges, 2018; Torres, 2024).

La creciente utilización de tecnologías de información y comunicación también ha incrementado la relevancia de las fuentes digitales dentro de las investigaciones penales. Según los datos recogidos por Navas-Abad & Vázquez-Martínez (2025) entre enero y agosto de 2020 se registraron 5.048 denuncias vinculadas con delitos informáticos en Ecuador, entre las cuales figuraron la suplantación de identidad, la falsificación y uso de documentos falsos y la apropiación fraudulenta por medios electrónicos. Estos datos permiten advertir la importancia creciente de la información almacenada o transmitida mediante dispositivos, plataformas y sistemas informáticos para la investigación de determinadas conductas delictivas, aunque el número de denuncias no permite, por sí solo, determinar la frecuencia con la que la evidencia digital es incorporada o resulta decisiva en los procesos penales.

3.2. La experiencia comparada de España y Colombia

Desde una perspectiva comparada, la experiencia española ofrece elementos relevantes para analizar los estándares aplicables a la autenticidad y valoración de las comunicaciones electrónicas. La Sentencia 300/2015 del Tribunal Supremo de España (2015) advirtió sobre las posibilidades de manipulación de los mensajes provenientes de sistemas de mensajería instantánea y destacó la necesidad de extremar las cautelas cuando su autenticidad es controvertida. En estos supuestos, la prueba pericial puede constituir un mecanismo idóneo para verificar el origen, la integridad y la atribución de las comunicaciones. No obstante, la valoración de la evidencia digital no debe reducirse exclusivamente a la existencia o ausencia de una pericia, sino considerar el conjunto de elementos objetivos de corroboración disponibles en cada caso, siempre que permitan verificar razonablemente su autenticidad e integridad.

Desde la perspectiva constitucional, el ordenamiento español establece límites a la obtención de evidencia cuando las actuaciones investigativas afectan derechos fundamentales. La STC 114/1984 constituye un referente en materia de prueba obtenida con vulneración de derechos fundamentales y permite distinguir entre los problemas relacionados con la fiabilidad o autenticación de la evidencia y aquellos derivados de la ilicitud de su obtención (Tribunal Constitucional de España, 1984). Esta diferenciación resulta relevante para el análisis ecuatoriano, puesto que la Constitución y el COIP exigen que la actividad probatoria respete las garantías del debido proceso y los derechos fundamentales.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

En Colombia, la jurisprudencia constitucional también ha desarrollado límites relacionados con la afectación del derecho a la intimidad en el marco de actuaciones investigativas. La Sentencia C-301/12 de la Corte Constitucional de Colombia (2012) constituye un referente para examinar las exigencias constitucionales aplicables a determinadas medidas que implican injerencia en comunicaciones o información protegida. Este enfoque permite incorporar al análisis comparado la relación entre obtención de evidencia, autorización judicial, proporcionalidad y protección de derechos fundamentales (Solano et al., 2023).

El contraste entre ambas experiencias permite identificar dos dimensiones diferenciadas de análisis. Por una parte, el modelo español aporta criterios relevantes para examinar la autenticación y fiabilidad de las comunicaciones electrónicas; por otra, la experiencia colombiana permite reforzar el análisis de los límites constitucionales aplicables a su obtención. Estos referentes no deben trasladarse automáticamente al ordenamiento ecuatoriano, sino valorarse atendiendo a su compatibilidad con la Constitución y el COIP. Desde esta perspectiva, el derecho comparado cumple una función analítica y orientadora para identificar posibles criterios de fortalecimiento del tratamiento jurídico de la evidencia digital en Ecuador.

3.3. Desafíos estructurales en la admisibilidad de la prueba digital en Ecuador

La complejidad de estos desafíos se relaciona con las particularidades propias de la evidencia digital. A diferencia de otros medios probatorios, esta presenta características como su naturaleza intangible, susceptibilidad de alteración y dependencia de procedimientos técnicos para verificar su origen, contenido e integridad. Por esta razón, su incorporación y valoración en el proceso penal exige examinar no solo su pertinencia respecto de los hechos investigados, sino también la licitud de su obtención, su autenticidad, la preservación de su integridad y, cuando corresponda, el adecuado cumplimiento de la cadena de custodia. Estos elementos permiten determinar la fiabilidad de la evidencia y su compatibilidad con las garantías del debido proceso.

La literatura revisada identifica diversos problemas relacionados con el tratamiento jurídico y técnico de la prueba digital en el proceso penal ecuatoriano. Iglesias et al. (2025) e Imaicela & Alvarado (2024) advierten dificultades relacionadas con la precisión de los criterios aplicables a la obtención, incorporación y valoración de este tipo de evidencia, así como con la ausencia de procedimientos técnicos suficientemente uniformes. Estas circunstancias pueden favorecer interpretaciones divergentes respecto del tratamiento procesal de la evidencia digital. En este contexto, la absolución de consulta No. 0120-AJ-P-CNJ-2021 de la Corte Nacional de Justicia del Ecuador (2021) constituye un referente interpretativo respecto del tratamiento de los mensajes de datos y documentos electrónicos, particularmente en relación con la necesidad de acreditar su autenticidad e integridad, sin perjuicio de considerar la naturaleza no vinculante de dicho pronunciamiento.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa
www.visionariodigital.org

Otro desafío se relaciona con la preservación de la integridad y trazabilidad de la evidencia digital. Morante et al. (2025) advierten dificultades en las prácticas utilizadas para su obtención y conservación, las cuales pueden comprometer la fiabilidad del elemento probatorio cuando impiden reconstruir adecuadamente su origen o determinar si ha experimentado modificaciones. Desde una perspectiva comparada, Bujosa et al. (2021) destacan la relevancia de la obtención lícita de la evidencia y de mecanismos adecuados para preservar y documentar su integridad. Asimismo, Rodrigo (2021) resalta la incidencia que puede tener la vulneración de derechos fundamentales durante la obtención de evidencia, particularmente cuando las actuaciones investigativas afectan comunicaciones o información protegida.

A partir del contraste de las fuentes examinadas, esta investigación sostiene que el principal déficit del ordenamiento ecuatoriano no radica en la inexistencia absoluta de reglas aplicables a la prueba digital, sino en la insuficiente densidad técnica de su regulación. El COIP establece principios y reglas generales relacionados con la cadena de custodia y la valoración probatoria, pero persisten aspectos que requieren mayor precisión y uniformidad, entre ellos los procedimientos para realizar una adquisición forense reproducible, la información mínima que debe documentarse, los mecanismos técnicos para verificar la integridad de los archivos digitales y las consecuencias procesales derivadas de las distintas irregularidades (Asamblea Nacional del Ecuador, 2014).

La falta de una diferenciación suficientemente precisa puede conducir a dos respuestas problemáticas: considerar que cualquier defecto técnico determina automáticamente la exclusión de la evidencia o, en sentido contrario, restar relevancia a irregularidades que comprometen efectivamente su licitud, autenticidad o integridad. Por ello, resulta necesario distinguir entre los supuestos de obtención ilícita por vulneración de derechos fundamentales, las alteraciones o rupturas que comprometen sustancialmente la integridad de la evidencia y aquellas deficiencias de acreditación susceptibles de ser valoradas o subsanadas conforme a las circunstancias del caso. Esta distinción permite atribuir consecuencias jurídicas diferenciadas en función de la naturaleza y gravedad de la irregularidad identificada.

3.4. Dificultades en la valoración judicial y la pericia forense

Más allá de los problemas relacionados con la admisibilidad, la literatura revisada identifica dificultades en la valoración judicial de la prueba digital, particularmente por el nivel de conocimiento técnico que puede requerir la comprensión de determinados elementos tecnológicos. Coronel & Argüello (2023) advierten limitaciones en la preparación de los operadores de justicia para gestionar y valorar evidencias digitales complejas. En similar sentido, Fuentes-Tenorio (2025) destaca la necesidad de fortalecer la capacitación especializada de jueces y fiscales, considerando que la adecuada comprensión de los aspectos técnicos de la evidencia digital puede incidir en su correcta interpretación y valoración dentro del proceso penal.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

La pericia informática adquiere especial relevancia en aquellos casos en los que la determinación de la autenticidad, integridad, origen o posible alteración de la evidencia requiere conocimientos técnicos especializados. Merve et al. (2016) identifican dificultades relacionadas con la formación especializada en el ámbito forense digital, mientras que Borges (2018) analiza las particularidades que presenta la valoración de comunicaciones obtenidas mediante sistemas de mensajería instantánea, especialmente respecto de la autenticidad del contenido y la atribución de autoría.

A estas dificultades se añade la dimensión transnacional que pueden presentar determinadas formas de ciberdelincuencia. Jakubiec (2022) destaca que las características tecnológicas y transfronterizas de estas conductas plantean exigencias adicionales para la investigación y el tratamiento de la evidencia digital. En este contexto, el fortalecimiento de las capacidades técnicas de jueces, fiscales y peritos constituye un elemento relevante para una adecuada comprensión, contradicción y valoración de este tipo de evidencia, sin que ello implique sustituir la función jurisdiccional del juez por las conclusiones técnicas del perito.

3.5. Principios y criterios aplicables a la prueba digital

La prueba digital, por su naturaleza intangible, reproducible y susceptible de alteración, exige que su obtención, incorporación y valoración se encuentren sometidas a principios que permitan controlar su fiabilidad y compatibilidad con las garantías del proceso penal. En primer lugar, el principio de legalidad exige que la evidencia sea obtenida y practicada conforme a la Constitución y la ley, sin vulneración de derechos fundamentales, especialmente la intimidad, la protección de datos y el debido proceso. A ello se suma la pertinencia, entendida como la relación que debe existir entre el contenido digital incorporado y los hechos objeto de investigación o juzgamiento. La integridad, por su parte, supone que la información se conserve sin alteraciones sustanciales desde su obtención hasta su presentación, mientras que la autenticidad permite establecer que el elemento corresponde efectivamente a la fuente, dispositivo, cuenta o persona a la que se atribuye.

En este contexto, la trazabilidad constituye una exigencia especialmente relevante, pues permite reconstruir las actuaciones realizadas sobre la evidencia digital, identificar a quienes intervinieron y verificar las condiciones de recolección, transferencia, análisis y conservación. Estos principios no operan de manera aislada. El artículo 457 del COIP dispone que la valoración de la prueba debe considerar su legalidad, autenticidad, sometimiento a cadena de custodia y el grado de aceptación científica y técnica de los principios que sustentan los informes periciales (Asamblea Nacional del Ecuador, 2014). Por ello, en materia digital, la confiabilidad probatoria depende tanto de la licitud de la obtención como de la posibilidad de demostrar técnicamente que el contenido presentado conserva correspondencia con el dato originalmente obtenido.

3.6. Cadena de custodia y autenticidad de la evidencia digital

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa
www.visionariodigital.org

La cadena de custodia constituye un mecanismo destinado a preservar y acreditar la identidad, integridad y trazabilidad de los elementos probatorios. Conforme al artículo 456 del COIP, se aplica tanto a los elementos físicos como al contenido digital materia de prueba, con la finalidad de garantizar su autenticidad mediante la acreditación de su identidad y estado original (Asamblea Nacional del Ecuador, 2014). Para ello, deben documentarse las condiciones en las que el elemento fue obtenido, así como las personas que intervienen en su recolección, envío, manejo, análisis y conservación, incluidos los cambios efectuados por cada custodio. La cadena se inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y concluye por disposición de la autoridad competente.

En el ámbito digital, esta obligación no puede reducirse al registro formal de las sucesivas entregas o transferencias. La trazabilidad debe permitir reconstruir las actuaciones realizadas sobre los datos desde su obtención hasta su incorporación al proceso. En consecuencia, la documentación de la fuente, el dispositivo o sistema de origen, el método de extracción, las copias forenses, los metadatos y, cuando resulte técnicamente aplicable, los valores *hash*, contribuye a verificar la integridad del contenido y a identificar posibles alteraciones. Esta interpretación se complementa con el artículo 500 del COIP, que contempla la aplicación de técnicas digitales forenses para el análisis, recuperación y presentación del contenido digital y dispone la aplicación de la cadena de custodia en su recolección, tanto respecto de sistemas o memorias volátiles como de medios no volátiles (Asamblea Nacional del Ecuador, 2014).

Desde el punto de vista procesal, las deficiencias en la cadena de custodia deben analizarse atendiendo a su naturaleza y a su incidencia sobre la autenticidad, integridad y fiabilidad del elemento probatorio. El artículo 457 del COIP establece, además, que la autenticidad de los elementos probatorios no sometidos a cadena de custodia debe ser acreditada por la parte que los presenta (Asamblea Nacional del Ecuador, 2014). En consecuencia, la cadena de custodia constituye un mecanismo relevante de aseguramiento y trazabilidad de la evidencia, pero su cumplimiento no sustituye el análisis de la licitud de la obtención, la idoneidad de las técnicas empleadas ni las posibilidades de contradicción dentro del proceso.

3.7. Medios de obtención y fuentes de prueba digital

La evidencia digital puede provenir de múltiples fuentes y no se limita a los dispositivos físicos incautados. Puede encontrarse en redes sociales, correos electrónicos, aplicaciones de mensajería instantánea, archivos y documentos electrónicos, registros de sistemas, bases de datos, metadatos, discos duros, teléfonos móviles, memorias externas, servidores y servicios de almacenamiento en la nube. Cada fuente presenta riesgos particulares de alteración, pérdida, acceso no autorizado o dificultad de atribución, por lo que el método de obtención debe adecuarse a su naturaleza y respetar las garantías constitucionales y procesales aplicables.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

Los metadatos pueden aportar información sobre creación, modificación, ubicación, autoría técnica o transferencia de un archivo; los correos electrónicos y mensajes pueden requerir la verificación de cuentas, encabezados, dispositivos y registros asociados; y la información alojada en la nube puede encontrarse bajo control de proveedores ubicados dentro o fuera del territorio nacional. Por ello, la mera impresión o captura de pantalla no siempre permite demostrar por sí sola el origen, la integridad o la autoría. Cuando exista controversia fundada sobre manipulación, atribución o método de extracción, la pericia informática y otros mecanismos objetivos de corroboración adquieren especial relevancia, sin que ello signifique que toda evidencia digital requiera necesariamente una pericia para ser valorada.

3.8. Actuaciones especiales relativas al contenido digital

El COIP incorpora una sección específica de actuaciones especiales relativas al contenido digital, que desarrolla mecanismos orientados a preservar, obtener y asegurar información informática dentro de una investigación penal. El artículo 477.1 regula el aseguramiento de datos y permite al fiscal ordenar, sin autorización judicial, la conservación expedita de datos informáticos específicos incluidos datos de abonado y de tráfico, cuando exista riesgo de pérdida o modificación (Asamblea Nacional del Ecuador, 2014). La medida busca preservar y mantener la integridad de la información durante el tiempo legalmente previsto y obliga a quien la recibe a adoptar los medios necesarios para su conservación y confidencialidad.

El artículo 477.2 diferencia la entrega de datos de contenido de aquella relativa a datos de abonado y de tráfico (Asamblea Nacional del Ecuador, 2014). Para los datos de contenido, el juez, a pedido del fiscal, puede ordenar a una persona natural o jurídica que presente, remita o entregue la información vinculada con la investigación de un delito concreto; mientras que el fiscal puede requerir directamente datos de abonado y de tráfico en los términos establecidos por la norma. Esta diferenciación resulta relevante porque el nivel de intervención estatal y la intensidad de afectación a la privacidad no son idénticos en todas las categorías de información digital (Asamblea Nacional del Ecuador, 2014, art. 477.2).

A su vez, el artículo 477.3 del COIP faculta al juez, a requerimiento del fiscal, a ordenar la búsqueda, registro y acceso a un sistema informático, a los datos almacenados en él o a un medio de almacenamiento (Asamblea Nacional del Ecuador, 2014). La medida puede comprender la incautación de componentes físicos, la obtención de copias íntegras de los datos y las acciones necesarias para hacerlos inaccesibles o eliminarlos, conforme a los presupuestos legales. Los artículos siguientes del COIP regulan además mecanismos de cooperación internacional para la obtención, preservación y divulgación de contenido digital, aspecto especialmente importante frente al carácter transnacional de numerosos delitos informáticos (Asamblea Nacional del Ecuador, 2014, arts. 477.3-477.10).

Estas actuaciones especiales evidencian que la obtención de prueba digital no puede tratarse como una simple reproducción documental. El ordenamiento distingue entre

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

preservar datos para evitar su desaparición, requerir su presentación y acceder o registrar sistemas informáticos. Cada actuación posee presupuestos y niveles de autorización distintos, lo que obliga a verificar, en cada caso, la competencia de la autoridad, la finalidad investigativa, la proporcionalidad de la medida, la integridad de la información obtenida y su posterior sometimiento a las reglas de cadena de custodia y valoración probatoria.

3.9. Propuestas de estandarización y enfoques emergentes

A partir de la identificación de estos problemas multifactoriales, la literatura académica plantea diversas propuestas de estandarización orientadas a superar las brechas existentes. Morante et al. (2025) y Ochoa (2018) proponen el establecimiento de protocolos técnicos estandarizados que permitan preservar la integridad probatoria desde la fase de adquisición de la evidencia y destacan la necesidad de contar con guías específicas adaptadas a la recolección de distintos tipos de evidencia digital. Este enfoque técnico se complementa con las recomendaciones de Deslauriers-Varin & Fortin (2021) quienes promueven la utilización de métodos basados en evidencia científica para las investigaciones criminales, orientados a fortalecer la eficacia y fiabilidad de los procedimientos investigativos mediante procesos estandarizados y validados.

En el ámbito jurídico, Arias-Becerra & Monsalve-Robalino (2024) plantean la posibilidad de adaptar determinados criterios probatorios a las particularidades de los delitos de alta complejidad técnica. Esta propuesta busca conciliar las necesidades de la persecución penal con la protección de las garantías fundamentales del procesado y plantea el debate sobre la adecuación de las reglas probatorias a las particularidades que presenta la evidencia generada en entornos digitales.

La experiencia comparada analizada por Bujosa et al. (2021) en España y Colombia, junto con el marco forense digital colombiano examinado por Solano et al. (2023) aporta referentes para la identificación de criterios susceptibles de consideración en el contexto ecuatoriano. Desde esta perspectiva, las propuestas de estandarización requieren integrar aspectos técnicos, normativos y de formación profesional especializada. Asimismo, Fukami et al. (2021) desarrollan un modelo técnico para la extracción de datos almacenados en dispositivos móviles encriptados, lo que evidencia la necesidad de considerar los avances tecnológicos en el desarrollo de procedimientos de obtención y análisis de evidencia digital.

Finalmente, Bazurto et al. (2024) incorporan una perspectiva centrada en los derechos fundamentales al analizar la relación entre ciberdelincuencia y protección de datos personales, recordando que el desarrollo de estándares probatorios debe ser compatible con la protección de los derechos de las personas. A su vez, Zepeda (2024) destaca la relevancia de una adecuada gestión de la evidencia digital para garantizar su utilización dentro de procesos compatibles con las exigencias del Estado de Derecho.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

3.10. Lineamientos técnico-jurídicos propuestos para el sistema ecuatoriano

La contribución propositiva de este estudio se concreta en un modelo de actuación basado en cinco lineamientos articulados. Su finalidad no es sustituir la valoración judicial, sino reducir la incertidumbre sobre la incorporación de evidencia digital y ofrecer parámetros verificables para fiscales, investigadores, peritos, defensores y jueces.

a) *Regla de diferenciación de efectos procesales.* Debe distinguirse expresamente entre: 1) evidencia obtenida con vulneración de derechos fundamentales, cuya consecuencia debe analizarse desde la ilicitud y exclusión; 2) fallas que comprometen materialmente la autenticidad o integridad, que pueden impedir su fiabilidad; y 3) irregularidades documentales o técnicas subsanables, que deben incidir en el peso probatorio cuando existan otros mecanismos objetivos de corroboración. Esta diferenciación evitaría respuestas automáticas y fortalecería la motivación judicial.

b) *Protocolo nacional mínimo de evidencia digital.* La Fiscalía General del Estado, la Policía Nacional y el Consejo de la Judicatura, dentro de sus competencias, deberían articular un protocolo uniforme que contemple identificación de la fuente, aislamiento del dispositivo, método de adquisición, generación y registro de valores *hash* cuando sea técnicamente aplicable, preservación del original, trabajo sobre copias forenses, registro cronológico de transferencias y documentación de las herramientas utilizadas. El protocolo debe ser tecnológicamente neutral para poder adaptarse a nuevas plataformas.

c) *Estándar mínimo de autenticación.* La autenticidad no debería descansar exclusivamente en una formalidad, como una captura de pantalla o una protocolización notarial. Debe acreditarse mediante un conjunto de indicadores según la naturaleza de la fuente: metadatos, extracción forense, identificación de cuentas o dispositivos, información del proveedor cuando sea legalmente accesible, reconocimiento de intervinientes y otros elementos de corroboración. La pericia debe ser especialmente relevante cuando exista impugnación fundada sobre manipulación, autoría o integridad.

d) *Formación y certificación especializada.* La capacitación debe diferenciar funciones. Los investigadores requieren competencias de preservación y adquisición; los peritos, actualización técnica y metodologías reproducibles; fiscales y defensores, capacidad para formular y controvertir hipótesis técnicas; y jueces, herramientas para controlar la fiabilidad del procedimiento y motivar el valor otorgado a la evidencia. La formación continua debe acompañarse de criterios institucionales de acreditación y actualización.

e) *Motivación judicial reforzada y construcción de precedentes.* Las decisiones que admitan excluyan o asignen valor decisivo a prueba digital deberían explicar de forma expresa la licitud de la obtención, los elementos de autenticación, la integridad, la cadena de custodia, la metodología pericial y la existencia de corroboración. Una

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

motivación estructurada permitiría identificar criterios repetibles y favorecería progresivamente una jurisprudencia más coherente.

Estos lineamientos responden a la causa central identificada en la investigación: la asimetría entre exigencias jurídicas relativamente altas y capacidades técnicas e institucionales desiguales. Su implementación conjunta permitiría trasladar el debate desde fórmulas abstractas sobre "autenticidad" e "integridad" hacia verificaciones concretas, controlables por las partes y motivables por el juzgador.

4. Discusión

Los hallazgos permiten sostener que el problema ecuatoriano no debe formularse como una oposición simple entre eficacia investigativa y garantismo. La cuestión decisiva radica en la necesidad de contar con criterios capaces de traducir principios jurídicos: licitud, autenticidad, integridad y contradicción, en operaciones técnicas verificables. Mientras esta articulación permanezca incompleta, el tratamiento de la prueba digital puede depender en gran medida de la capacidad técnica del perito y de los criterios aplicados por el juzgador, situación que se relaciona con las dificultades advertidas por Iglesias et al. (2025) y Morante et al. (2025).

La absolución de consulta No. 0120-AJ-P-CNJ-2021, aun cuando constituye un criterio no vinculante emitido en materia civil, ofrece un referente interpretativo sobre el tratamiento probatorio de los mensajes de datos (Corte Nacional de Justicia del Ecuador, 2021). La consulta reconoce que los mensajes enviados mediante WhatsApp pueden constituir documentos electrónicos siempre que cumplan los requisitos legales relativos, entre otros aspectos, a la autenticidad de su origen y a la identificación del titular de la cuenta. Sin embargo, trasladar estas consideraciones al ámbito penal requiere atender a las particularidades y garantías propias del proceso penal. En este contexto, la ausencia de un estándar técnico suficientemente detallado mantiene abierta la cuestión sobre los mecanismos concretos mediante los cuales debe acreditarse la autenticidad e integridad de este tipo de evidencia. A juicio de esta investigación, esta cuestión no debe resolverse imponiendo una pericia obligatoria en todos los casos, sino atendiendo a la existencia de una controversia fundada sobre autoría, manipulación, integridad o método de extracción y a la disponibilidad de otros elementos objetivos de corroboración.

El contraste con España y Colombia refuerza esta conclusión. Del modelo colombiano resulta relevante la centralidad otorgada a los derechos fundamentales en la obtención de evidencia; mientras que la experiencia española aporta criterios relacionados con la autenticación de las comunicaciones electrónicas y la posibilidad de considerar mecanismos objetivos de corroboración. La recepción ecuatoriana de estas experiencias debe evitar trasplantes jurídicos acríticos: tanto un formalismo técnico que conduzca a excluir evidencia fiable por defectos no sustanciales como una flexibilidad que permita otorgar eficacia probatoria a material cuyo origen, integridad o licitud no puedan ser suficientemente acreditados.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

La literatura revisada también evidencia una tensión institucional: se atribuye a la pericia forense una función relevante para resolver controversias relacionadas con la autenticidad e integridad de la evidencia digital, mientras que determinadas fuentes advierten dificultades relacionadas con la formación especializada y la ausencia de protocolos uniformes. En consecuencia, la sola existencia de un informe pericial no garantiza por sí misma la fiabilidad de sus conclusiones. El control judicial debe considerar la transparencia y solidez del método empleado, incluyendo, cuando corresponda, la posibilidad de reproducción del análisis, la documentación de las herramientas utilizadas, la preservación del original, la trazabilidad de las copias y la explicación de las limitaciones del procedimiento técnico.

Desde esta perspectiva, la cadena de custodia digital tampoco debe entenderse como una secuencia meramente administrativa de firmas y entregas. Su función probatoria se relaciona con la posibilidad de acreditar la identidad, continuidad e integridad del elemento desde su obtención hasta su presentación en juicio. Por ello, la documentación técnica incluidos, cuando proceda, valores *hash*, imágenes forenses, metadatos y registros de intervención, debe integrarse a la lógica jurídica de la cadena de custodia. Esta interpretación permite explicar por qué una omisión formal no necesariamente equivale a una alteración de la evidencia y, al mismo tiempo, por qué una cadena documental aparentemente completa puede resultar insuficiente si no permite determinar qué ocurrió técnicamente con los datos.

La propuesta propia que deriva del estudio consiste, por tanto, en sustituir un enfoque binario de “admisible/no admisible” por un modelo escalonado de control. En un primer nivel debe examinarse la licitud constitucional de la obtención; posteriormente, la autenticidad e integridad mediante indicadores técnicos y elementos de corroboración; finalmente, las deficiencias restantes deben analizarse atendiendo a su incidencia concreta sobre la fiabilidad del elemento probatorio. Este esquema permite preservar las garantías fundamentales, evitar respuestas automáticas y proporcionar parámetros más claros para la motivación judicial.

La principal limitación de esta propuesta deriva del carácter documental de la investigación. No se ha determinado empíricamente la frecuencia con la que las deficiencias identificadas se presentan en fiscalías, unidades investigativas o tribunales. Por ello, los lineamientos formulados deberán ser contrastados en futuras investigaciones mediante entrevistas, análisis de expedientes y procesos de validación con peritos y operadores de justicia. No obstante, dentro del alcance dogmático-jurídico planteado, el contraste normativo, doctrinal y comparado permite identificar los aspectos en los que la regulación general requiere un mayor desarrollo técnico e interpretativo.

5. Conclusión

- La investigación concluye que la principal dificultad de la prueba digital en el proceso penal ecuatoriano no radica en su falta de reconocimiento jurídico, sino

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

en la ausencia de un desarrollo suficientemente preciso que conecte las reglas procesales generales con las exigencias técnicas propias de la evidencia digital. Los principales desafíos se concentran en la autenticación, la documentación de la cadena de custodia digital, la determinación de las consecuencias jurídicas derivadas de las distintas irregularidades y la falta de criterios suficientemente uniformes para su valoración judicial.

- La revisión normativa, doctrinal y jurisprudencial permite identificar que la licitud, autenticidad e integridad constituyen categorías relevantes para el tratamiento de la evidencia digital, aunque su aplicación todavía requiere una mayor concreción técnica e interpretativa. Por ello, esta investigación propone diferenciar entre la evidencia obtenida ilícitamente, los defectos que comprometen materialmente su autenticidad o integridad y las irregularidades subsanables cuya incidencia debe analizarse principalmente en el ámbito de la valoración probatoria. Esta distinción permite proteger las garantías del debido proceso sin convertir las exigencias técnicas de la evidencia digital en un formalismo que produzca automáticamente su exclusión.
- Como aporte concreto, se plantean cinco lineamientos: diferenciación de efectos procesales, protocolo nacional mínimo de evidencia digital, estándar plural de autenticación, formación y certificación especializada, y motivación judicial reforzada. Su aplicación articulada puede contribuir a una mayor uniformidad en el tratamiento de la evidencia digital, fortalecer las posibilidades de contradicción y favorecer progresivamente la construcción de criterios jurisprudenciales más previsibles.
- El fortalecimiento del sistema ecuatoriano exige, en consecuencia, coordinación entre la Fiscalía General del Estado, la Policía Nacional, el Consejo de la Judicatura y los órganos jurisdiccionales, dentro de sus respectivas competencias. Una eventual reforma normativa resultaría insuficiente si no se acompaña de protocolos técnicamente actualizables, fortalecimiento de las capacidades forenses y formación continua de los operadores involucrados. Las experiencias de España y Colombia ofrecen referentes útiles para este propósito, pero su consideración debe realizarse atendiendo a su compatibilidad con las garantías constitucionales, la normativa procesal y las particularidades institucionales del sistema ecuatoriano.
- Finalmente, por tratarse de un estudio cualitativo, dogmático-jurídico y documental, los lineamientos propuestos requieren una posterior contrastación empírica. Una siguiente fase de investigación podría examinar expedientes judiciales y recoger la experiencia de jueces, fiscales, defensores y peritos informáticos, con el propósito de determinar la frecuencia y características de las dificultades identificadas y evaluar la aplicabilidad práctica del modelo escalonado de control propuesto.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

6. Conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con el artículo presentado.

7. Derechos de autor (copyright)

Los autores son los titulares de los derechos de autor (patrimoniales y/o de explotación) de los contenidos de la revista.

8. Declaración de contribución de los autores

Los autores declaran haber participado de manera equitativa y sustancial en la realización de esta investigación, bajo las responsabilidades según la Taxonomía CRediT para describir las contribuciones individuales de cada autor al trabajo.
Bebsi Alexandra Paredes Carcelén, realizó la conceptualización de la investigación, organización y ejecución del ensayo, recopilación y curación de los datos, revisión del análisis estadístico, interpretación de los resultados, elaboración del borrador original, preparación de tablas y figuras, revisión crítica del contenido y aprobación de la versión final del manuscrito.
Micaela Rashell Zapata Morejón & Sylka Noelia Zapata Morejón, realizaron la supervisión académica y metodológica de la investigación, brindó orientación durante el desarrollo del ensayo, revisó el análisis y la interpretación de los resultados, efectuó la revisión crítica del manuscrito, realizó la corrección científica y académica y aprobó la versión final para su publicación.
Divulgación de la delegación a la IA generativa
Los autores declaran que emplearon ChatGPT (OpenAI, GPT-5.5) como herramienta de apoyo para reorganizar y reformular editorialmente el manuscrito original, corregir el estilo, traducir el resumen al inglés y comprobar el cumplimiento formal del formato de la revista. Los datos experimentales, el diseño, los resultados estadísticos y las decisiones científicas proceden de la investigación de los autores y no fueron generados ni modificados por la herramienta. Los autores revisaron, contrastaron y aprobaron cada sección y asumen la responsabilidad íntegra del contenido final. La herramienta no figura como autor ni asume responsabilidad por los resultados.
Declaración presentada por: Bebsi Alexandra Paredes Carcelén.

9. Costos de financiamiento

La presente investigación fue financiada en su totalidad con fondos propios de los autores.

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

10. Referencias bibliográficas

Arias-Becerra, C. A., & Monsalve-Robalino, B. X. (2024). El estándar probatorio en delitos en la delincuencia organizada. *MQRInvestigar, 8*(3), 4555–4574. https://doi.org/10.56048/MQR20225.8.3.2024.4555-4574

Asamblea Nacional Constituyente del Ecuador. (2008). *Constitución de la República del Ecuador*. Registro Oficial No. 449, 20 de octubre de 2008. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento No. 180, 10 de febrero de 2014. www.defensa.gob.ec/wp-content/uploads/downloads/2021/07/COIP_act_jun-2021.pdf

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Quinto Suplemento No. 459, 26 de mayo de 2021. https://www.sot.gob.ec/wp-content/uploads/2024/11/21.-Ley-Organica-de-Proteccion-de-datos.pdf

Bazurto Mecias, C. J., Jurado Cabello, Y. K., Sifa Mueses, L. M., & Reinoso Paredes, A. G. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica, 7*(5), 594–612. https://sinergiaacademica.com/index.php/sa/article/view/289

Borges Blásquez, R. (2018). La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. *Iuris Tantum*, (25), 536–549. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100018

Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal, 7*(2), 1347–1384. https://doi.org/10.22197/rbdpp.v7i2.482

Congreso Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Registro Oficial Suplemento No. 557, 17 de abril de 2002. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Coronel Maji, J. R., & Argüello Arellano, E. E. (2025). Análisis forense digital: La eficacia de la legislación ecuatoriana ante el cibercrimen. *Polo del Conocimiento, 10(11), 2012–2037.* https://doi.org/10.23857/pc.v10i11.10748

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia: http://creativecommons.org/licenses/by-nc-sa/4.0/

Corte Constitucional de Colombia. (2012). *Sentencia C-301/12*. Sala Plena de la Corte Constitucional. https://www.corteconstitucional.gov.co/relatoria/2012/c-301-12.htm

Corte Nacional de Justicia del Ecuador. (2021). *Prueba por medio de documentos electrónicos (WhatsApp) [Criterio no vinculante, absolución de consulta No. 0120-AJ-P-CNJ-2021]*. https://www.cortenacional.gob.ec/resources/consultas_absueltas/No_Penales/Civil/127.pdf

Deslauriers-Varin, N., & Fortin, F. (2021). Improving efficiency and understanding of criminal investigations: Toward an evidence-based approach. *Journal of Police and Criminal Psychology*, *36*(4), 635–638. https://doi.org/10.1007/s11896-021-09491-6

Fuentes-Tenorio, E. G. (2025). Criminalidad en el ciberespacio: tipificación de delitos informáticos y desafíos probatorios en Ecuador. *Polo del Conocimiento*, *10*(6), 2342–2350. https://polodelconocimiento.com/ojs/index.php/es/article/view/9817/html

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Investigación Digital*, *38*, 301169. https://doi.org/10.1016/j.fsidi.2021.301169

Herrera Zapata, S. M. (2025). *El papel de la prueba digital en los procedimientos penales en Ecuador* [Tesis de maestría, Universidad Andina Simón Bolívar, Sede Ecuador]. http://hdl.handle.net/10644/10524

Iglesias Chonillo, S. C., Orbea Vaca, L. P., & Campos Cárdenas, F. E. (2025). Admisibilidad de la prueba digital en los procedimientos judiciales según la normativa ecuatoriana. *Revista Lex, 8(30), 1716–1739.* https://doi.org/10.33996/revistalex.v9i30.374

Imaicela Revilla, J. A., & Alvarado Ajila, L. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano. *Revista Lex, 7*(27), 1338–1350. https://doi.org/10.33996/revistalex.v7i27.247

Jakubiec, W. (2022). Cybercriminals and criminal structures in the world of organized crime. *Scientific Journal of Bielsko-Biala School of Finance and Law, 26*(4), 36–39. https://doi.org/10.19192/wsfip.sj4.2022.6

Merve, O., İbrahim, K., & Hüseyin, Ç. (2016). Evaluación general y requisitos de la formación en informática forense. *Bilişim teknolojileri dergisi, 9*(2), 137–145. https://dergipark.org.tr/en/download/article-file/262271

Morante Mendoza, L. E., Safadi Mendoza, J. A., & Gómez Rivera, G. P. (2025). Delitos informáticos y prueba digital en el COIP: Validez, cadena de custodia y pericia forense en el Ecuador. *Tesla Revista Científica, 5*(2), e542. https://doi.org/10.55204/trc.v5i2.e542

Navas-Abad, C. E., & Vázquez-Martínez, D. S. (2025). La importancia de la prueba digital en los procedimientos penales en Ecuador. *Polo del Conocimiento, 10(1),*

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia: http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

1742–1775. https://polodelconocimiento.com/ojs/index.php/es/article/view/8778/pdf

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía y Política*, (28), 35–46. https://doi.org/10.25097/rep.n28.2018.03

Rodrigo, M. F. (2021). La evidencia digital en el proceso penal y la preservación de los derechos fundamentales. *Revista Acadêmica Escola Superior do Ministério Público do Ceará, 13*(1), 135–161. https://doi.org/10.54275/raesmpce.v13i1.154

Solano Oviedo, D. S., Roldán Álvarez, M. A., & Vargas Montoya, H. F. (2023). Investigación forense digital en entidades del Estado colombiano: Acercamiento a la Ley 1952 de 2019. *Revista Logos Ciencia & Tecnología, 15(1), 122–140*. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2422-42002023000100122

Torres Loján, C. G. (2024). WhatsApp como herramienta de prueba en litigios por obligaciones financieras: una mirada al sistema judicial ecuatoriano. *Revista Lex, 7*(25), 496–511. https://doi.org/10.33996/revistalex.v7i25.196

Tribunal Constitucional de España. (1984). *Sentencia 114/1984, de 29 de noviembre (Recurso de amparo núm. 167/1984). Boletín Oficial del Estado*. https://hj.tribunalconstitucional.es/es/Resolucion/Show/367

Tribunal Supremo de España. (2015). *Sentencia 300/2015, de 19 de mayo (Sala de lo Penal)*. https://vlex.es/vid/571257698

Zepeda Castro, H. J. (2024). Manejo de evidencia digital: Un pilar en la lucha contra el cibercrimen. *Revista Iberoamericana de Derecho, Cultura y Ambiente*, (6). https://aidca.org/ridca6-penal-zepeda-castro-manejo-de-evidencia-digital-un-pilar-en-la-lucha-contra-el-cibercrimen/

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/

ISSN: **2602-8506**
Vol. 10 No. 4, pp. 332 – 354, octubre – diciembre 2026
Revista en Ciencias sociales y humanidades
Artículo de revisión bibliográfica narrativa

www.visionariodigital.org

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Visionario Digital.**

El artículo queda en propiedad de la revista y, por tanto, su publicación parcial y/o total en otro medio tiene que ser autorizado por el director de la **Revista Visionario Digital.**

Esta revista está protegida bajo una licencia Creative Commons en la 4.0 International. Copia de la licencia:
http://creativecommons.org/licenses/by-nc-sa/4.0/