ISSN:
3091-1796
Vol. 4 No. 10 PP. 216-228

DOI:
https://doi.org/10.56519/47yw7870
Agosto 2026

ANÁLISIS JURÍDICO DEL USO DE LA EVIDENCIA DIGITAL EN LOS PROCESOS PENALES Y SU IMPACTO EN LA GARANTÍA DEL DEBIDO PROCESO

LEGAL ANALYSIS OF THE USE OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS AND ITS IMPACT ON THE GUARANTEE OF DUE PROCESS

María Fernanda Echeverría[1], Juan Carlos Baquero Salazar[2], Orlando Lenin Carrión[3], Melany Lisseth Escobar Garzon[4]

{maferecheverria@hotmail.com[1], juan.baquero.tse@gmail.com[2], mgs.orlando_carrion@hotmail.com[3], melany.lgc.23@gmail.com[4]}

Fecha de recepción: 08/07/2026 / Fecha de aceptación: 20/08/2026 / Fecha de publicación: 25/08/2026

RESUMEN: El uso de la evidencia digital en los procesos penales constituye uno de los fenómenos jurídicos más relevantes derivados de la transformación tecnológica de las últimas dos décadas, en la medida en que los sistemas de justicia penal de América Latina, y particularmente de Ecuador, enfrentan el reto de incorporar mensajes de datos, metadatos, imágenes, videos, registros de geolocalización y demás elementos electrónicos como medios de prueba válidos, sin comprometer las garantías del debido proceso. Este trabajo examinó, mediante una revisión sistemática de la literatura especializada siguiendo los parámetros PRISMA, el abordaje procesal de la evidencia digital en las causas penales y cómo esta repercute en las garantías del debido proceso. Se empleó una metodología documental de carácter cualitativo y con un alcance descriptivo-analítico; para lograrlo, se llevó a cabo una búsqueda estructurada en bases de datos indexadas aplicando criterios definidos de inclusión y exclusión, lo que permitió seleccionar un grupo final de artículos académicos publicados entre 2021 y 2026. Los hallazgos revelan que, aunque la normativa ecuatoriana y de la región admite el valor probatorio de los componentes informáticos, aún existen vacíos legales y operativos al resguardar la cadena de custodia, sumado a la ausencia de protocolos forenses uniformes, la limitada formación de los servidores judiciales y la falta de criterio único al momento de evaluar su autenticidad e integridad. Estas falencias perjudican de forma directa el derecho a la defensa, la contradicción de las pruebas y la imparcialidad en las resoluciones de los jueces. En consecuencia, asegurar una verdadera protección judicial frente a las pruebas tecnológicas exige adecuar las leyes locales a los parámetros internacionales, formalizar guías para las pericias y capacitar de forma permanente a los profesionales del sistema de justicia. Únicamente de esta manera se

[1]Investigador Independiente, https://orcid.org/0000-0002-7266-2906
[2]BS Legal Tech, https://orcid.org/0009-0004-1762-2778
[3]Consultoría Jurídica Criminalística "Carrión", https://orcid.org/0009-0005-1335-905X
[4]Provincial, Consejo de la Judicatura de Tungurahua, https://orcid.org/0009-0001-1124-1585

ISSN:
3091-1796

podrá consolidar un juzgamiento penal transparente, riguroso y en apego estricto a los derechos constitucionales en el entorno digital.

Palabras clave: prueba electrónica, cadena de custodia, informática forense, garantías judiciales, ciberdelincuencia

ABSTRACT: The use of digital evidence in criminal proceedings is one of the most significant legal developments resulting from the technological transformation of the past two decades, as criminal justice systems in Latin America—and particularly in Ecuador—face the challenge of incorporating data messages, metadata, images, videos, geolocation records, and other electronic elements as valid forms of evidence without compromising due process guarantees. This study examined, through a systematic review of the specialized literature following the PRISMA guidelines, the procedural approach to digital evidence in criminal cases and how it impacts due process guarantees. A qualitative, descriptive-analytical documentary methodology was employed; to achieve this, a structured search was conducted in indexed databases using defined inclusion and exclusion criteria, which allowed for the selection of a final set of academic articles published between 2021 and 2026. The findings reveal that, although Ecuadorian and regional regulations recognize the evidentiary value of digital evidence, there are still legal and operational gaps in safeguarding the chain of custody, compounded by the absence of uniform forensic protocols, limited training for judicial officials, and the lack of a single standard for evaluating the authenticity and integrity of such evidence. These shortcomings directly undermine the right to a defense, the right to challenge evidence, and the impartiality of judicial rulings. Consequently, ensuring genuine judicial protection against digital evidence requires aligning local laws with international standards, formalizing guidelines for forensic analysis, and providing ongoing training to professionals in the justice system. Only in this way can a transparent and rigorous criminal justice process be established, one that strictly adheres to constitutional rights in the digital environment.

Keywords: electronic evidence, chain of custody, computer forensics, judicial safeguards, cybercrime

INTRODUCTION

Contemporary society is going through a process of digital transformation that has substantially modified the way in which criminal acts are committed, investigated and prosecuted. The massive use of mobile devices, social networks, messaging systems, cloud storage platforms and Internet of Things devices has generated a growing volume of information that can become a source of evidence in criminal proceedings (1). This phenomenon has given rise to the legal category of digital evidence, understood as any data or information stored or transmitted in binary format that can be used as an element of conviction within a judicial process (15). Unlike traditional evidence, digital evidence is characterized by its volatility, its easy alterability and the need for specialized technical knowledge for its identification, collection, preservation and analysis, as

evidenced by recent studies on the forensic analysis of volatile memory applied to common crimes with a technological component in the Ecuadorian context (3), which requires the development of rigorous forensic protocols that guarantee its authenticity and integrity throughout the entire chain of custody (4).

On an international level, organizations such as the Council of Europe have promoted the Convention on Cybercrime since 2001, known as the Budapest Convention, as the first binding instrument aimed at harmonizing the criminal prosecution of computer crimes and establishing common criteria for obtaining electronic evidence between States (17). In parallel, the International Organization for Standardization developed the family of standards ISO/IEC 27037 and ISO/IEC 27042, which establish technical guidelines for the identification, collection, acquisition, preservation, analysis and interpretation of digital evidence, becoming references for good forensic practices adopted by police laboratories and computer experts from different countries (15,16).

In Latin America, the exponential growth of computer crimes has, in many cases, exceeded the regulatory and institutional response capacity of criminal justice systems. According to the regional diagnosis prepared by the Organization of American States, the countries of the region face significant gaps in forensic infrastructure, training of justice operators and international cooperation to obtain cross-border digital evidence, which has a direct impact on the effectiveness of criminal prosecution and the protection of the rights of those prosecuted (2). Comparative studies carried out in countries such as Spain, Colombia, Chile and Peru also show tensions between the need to incorporate technology into criminal investigation and respect for guarantees such as privacy, the inviolability of communications and the right to defense (5).

In the particular case of Ecuador, the Comprehensive Organic Criminal Code expressly recognizes data messages, computer records, emails and other digital documents as valid means of proof within the criminal process, and regulates, although in a general way, the chain of custody and the actions of accredited experts (8). Without prejudice to this regulatory recognition, various investigations carried out in the country have identified relevant deficiencies in its practical application: absence of unified technical protocols, insufficient specialized forensic infrastructure, shortage of accredited computer experts and disparity in judicial criteria to assess the authenticity and integrity of digital evidence (5,6,7). These deficiencies acquire special constitutional relevance, to the extent that article 76 of the Constitution of the Republic of Ecuador enshrines due process as a set of basic guarantees applicable to any procedure in which rights and obligations are determined, among them the presumption of innocence, the right to defense, the contradiction of evidence and the motivation of judicial resolutions (9).

Due process, in addition to its internal constitutional consecration, finds foundation in Article 8 of the American Convention on Human Rights, which recognizes the right of every person to be heard with due guarantees by a competent, independent and impartial judge or tribunal (10). The Inter-American Court of Human Rights has developed consolidated jurisprudence on the components of criminal due process, including the right of defense, access to criminal evidence and the effective possibility of challenging it, standards that are fully applicable to the treatment of digital evidence (11). When the chain of custody of a digital element is broken, when there are no

verifiable collection protocols or when the computer expert lacks technical accreditation, the possibility opens up that the evidence is questioned due to manipulation, affecting guarantees such as contradiction and equality of procedural arms.

From a criminological perspective, the growth of crimes that leave a digital trace, computer fraud, identity theft, extortion through social networks, online child pornography and digital gender violence, among others, has made digital evidence the central evidentiary element of a growing number of criminal cases, even in crimes traditionally investigated through physical evidence, such as homicide or robbery, in which geolocation records, video surveillance cameras and Metadata from mobile devices have been incorporated as key pieces of research (1,2). This marked relevance of computer evidence intensifies the legal impact of any failure in its expert handling: a modification in the chain of custody or obtaining it outside the law not only invalidates an isolated piece of information, but also annuls the entire trial. This opens the door both for various crimes to go unpunished and for innocent people to be unfairly punished based on altered or defective information (3,4).

Faced with this panorama, it is necessary to systematize the scientific knowledge available on the legal treatment of digital evidence in criminal proceedings and its relationship with the guarantees of due process, identifying the main regulatory, technical and jurisprudential gaps documented in the specialized literature of recent years. In this sense, the general objective of the present study was to analyze, through a systematic review of the scientific literature, the legal treatment of digital evidence in criminal proceedings and its impact on the guarantee of due process, with emphasis on the Ecuadorian and Latin American context.

The research problem addressed in this study is located at the intersection between criminal procedural law, constitutional law and computer forensics, three disciplinary fields that, according to the literature reviewed, do not always dialogue in an articulate manner in judicial practice. While the legislator has made progress in the formal recognition of digital evidence as a means of proof, the development of expert technical capabilities and institutional action protocols has not followed the same pace, generating an asymmetry that transfers to judges the burden of resolving, case by case and without uniform criteria, eminently technical issues related to the authenticity, integrity and traceability of electronic evidence (6,7).

Despite the regulatory recognition of digital evidence as a valid means of proof in the Ecuadorian criminal process and in most Latin American legal systems, a gap remains between said formal recognition and the technical and institutional conditions necessary to guarantee its authenticity, integrity and evidentiary reliability (5,6). This gap translates into heterogeneous evidence collection and preservation practices, absence of standardized national protocols, insufficient accreditation of forensic computer experts, and disparate judicial criteria for admitting or excluding digital evidence, which generates legal uncertainty for both the Prosecutor's Office and the technical defense (12,13). The problem becomes especially serious when it is noted that the violation of the digital chain of custody not only compromises the effectiveness of criminal prosecution, but can lead to the violation of the fundamental rights of the

accused, by admitting as evidence of prosecution elements whose traceability cannot be fully verified (14). Consequently, the following research question is posed: What is the legal treatment that scientific literature has documented regarding the use of digital evidence in criminal proceedings in Ecuador and Latin America, and in what way does said treatment affect the guarantee of due process?

This research analyzed, through a systematic review of academic literature applying the PRISMA approach, the legal regulation of digital evidence within the criminal system and its impact on the guarantees of due process. The study examined with special emphasis the panorama of Ecuador and Latin America, compiling the scientific production disseminated between 2021 and 2026.

MATERIALS AND METHODS

This study uses a documentary design, prepared from a qualitative perspective and with a descriptive-analytical level. Its development was carried out through a systematic examination of specialized literature, aligned with the guidelines of the PRISMA 2020 declaration. This methodological scheme ensures a clear and rigorous process in the stages of location, selection, evaluation of evidentiary quality and incorporation of the texts that constitute the final analysis sample, significantly reducing the bias inherent in usual theoretical reviews.

Information collection was carried out between June and August 2026 in specialized databases such as Scopus, Dialnet, Redalyc, SciELO, Latindex and Google Academic, reinforced with access to university digital libraries in the region and legal repositories oriented to technology and procedural law. The search formulas combined descriptors such as "digital evidence", "digital evidence", "criminal process", "due process", "chain of custody" and "cybercrime" using Boolean operators AND and OR, also adding their equivalents in English ("digital evidence", "criminal proceedings", "due process") to extend the bibliographic coverage.

The selection process gave priority to indexed articles with peer evaluation, postgraduate theses, institutional reports and book chapters published between 2021 and 2026, written in Spanish or English, with access to full text and focused on the use of computer evidence in criminal justice. Non-refereed publications, duplicate records, non-scientific content and technical works lacking normative-procedural analysis were discarded.

The initial crawl identified 138 records. After eliminating 22 duplicates, 116 were analyzed by title and abstract, discarding 61 for not adjusting to the object of study. Of the 55 full-text works reviewed, 24 were purged for failing to meet the rigor criteria (12 purely computer science, 7 without formal arbitration and 5 redundant), consolidating a final sample of 31 academic publications processed using synthetic analysis matrices.

Table 1. Phases of the selection process according to the PRISMA method.

Phase	No. of records	Observation

Identification	138	Search in indexed databases and repositories
Duplicates eliminated	22	Bibliographic manager and manual review
Screening (title/abstract)	116	61 excluded due to lack of thematic relevance
Eligibility (full text)	55	24 excluded due to quality/relevance criteria
Included in the synthesis	31	Final sample analyzed

The 31 selected documents were cataloged in a bibliographic template that recorded authorship, year of publication, country, type of study, methodology and main findings. On this basis, a qualitative content analysis was carried out aimed at identifying recurring patterns, structured in four thematic axes: (a) regulatory framework of digital evidence; (b) procedural guarantees and technical requirements; (c) evidentiary assessment of the computer material; and (d) protection of due process. Given the qualitative-documentary approach of the work, no inferential statistical models were used, restricting the data treatment to the basic descriptive calculation (frequencies and percentages) to characterize the body of literature examined.

RESULTS

The results of this systematic review are organized following the four thematic axes derived from the content analysis of the documentary sample, preceded by a general characterization of the included studies. This organization allows us to offer a comprehensive reading of the state of the art on digital evidence in criminal proceedings, from its regulatory recognition to its specific impact on the guarantees of due process, passing through the technical-forensic and judicial assessment aspects that constitute the core of the debate identified in the specialized literature.

Of a total of 31 inquiries analyzed in this research, 58% (n=18) derive from publications distributed in Ecuadorian scientific journals indexed in Latindex, Dialnet and various regional repertoires. Likewise, 23% (n=7) finds its origin in comparative studies from other Ibero-American nations, while the remaining 19% (n=6) is made up of regulatory frameworks, technical opinions and inter-American jurisprudence. Regarding the date of issue, 74% of the bibliographic inputs are between 2023 and 2026, which reflects increasing academic attention to the convergence between digital evidence and due process guarantees.

Table 2. Distribution of the documentary sample according to thematic axis.

Thematic axis	n	%	Main source
Regulatory framework for digital evidence	9	29 %	COIP, COGEP, LOPD
Chain of custody and technical standards	11	35 %	ISO/IEC 27037, ISO/IEC 27042
Judicial assessment of digital evidence	6	20 %	Jurisprudence and procedural doctrine
Due process guarantees	5	16 %	Constitution, ACHR, Inter-American Court

Regulatory framework for digital evidence

The documentary analysis shows that the Comprehensive Organic Criminal Code expressly recognizes electronic documents, data messages and computer records as means of proof, referring in a complementary manner to the Law on Electronic Commerce, Electronic Signatures and Data Messages for the purposes of their evidentiary assessment (8). However, the studies agree that said regulation is insufficient in the face of the technical complexity of contemporary digital evidence, as it does not establish specific and unified collection protocols for mobile devices, cloud systems or institutional servers, leaving said standardization to be left to specific technical proposals rather than to a consolidated public policy (1,6). In the comparative field, the laws of Spain, Colombia, Chile and Peru present an uneven regulatory development: while Spain has specific regulation on technological research proceedings, Ecuador and other countries in the region still lack an autonomous legal framework for electronic evidence, relying on general provisions of the criminal procedure code (5,20).

Chain of custody and technical standards

The thematic axis with the highest frequency of documentation was that related to the digital chain of custody, present in 35% of the sample. The studies reviewed repeatedly identify the absence of unified technical protocols at the national level in Ecuador for the identification, collection, packaging, transportation and storage of electronic devices, which increases the risk of contamination or alteration of the evidence before its expert analysis (12,22). The limited formal adoption of international standards such as the ISO/IEC 27037 standard is also documented, which establishes the principles of auditability, repeatability, reproducibility and justifiability as minimum conditions to guarantee the reliability of digital evidence (15,16). Judicial cases analyzed in the literature illustrate how the lack of coincidence between the hash values recorded at the time of seizure and those verified in the expert phase has led to the declaration of nullity or exclusion of the evidence due to breaking the chain of custody (14).

Likewise, a significant lack of accredited computer forensic experts and specialized laboratories equipped with bit-by-bit forensic duplication tools is identified in the region, which forces in many cases to resort to external experts or international cooperation organizations, generating procedural delays and making access to justice more expensive (6,24). The Organization of American States has indicated that this limitation of technical capabilities constitutes one of the main obstacles to the effective prosecution of cybercrime in the region (2).

Judicial assessment of digital evidence

Regarding judicial assessment, the studies reviewed show disparate criteria among justice operators regarding the admissibility of screenshots, instant messaging conversations and publications on social networks as evidence of prosecution, in the absence of technical expertise that certifies their authenticity (13.25). A growing jurisprudential trend is documented to require technical verification of metadata and complete traceability of the chain of custody as a condition of admissibility, although this requirement is not applied uniformly in all judiciaries in the country (28,29). On the

other hand, some studies warn about the risk of an excessively formal judicial assessment, which could discard substantially relevant digital evidence due to minor procedural defects, to the detriment of the search for material truth (21,23).

Due process guarantees

Documents that directly address the relationship between digital evidence and due process highlight three main tensions. Firstly, the possible impact on the right to privacy and the inviolability of communications during the obtaining of digital evidence without proper judicial authorizations, as well as the risk that said evidence will be used selectively or at convenience by the procedural parties (30). Secondly, the limitations on the right of defense when the prosecuted party does not have timely access or the technical capacity to dispute the digital evidence of the charge, which compromises the principle of equality of arms (11,31). Thirdly, the requirement of judicial motivation is reinforced when the conviction is based predominantly on digital evidence, by virtue of the standards set by the Inter-American Court of Human Rights in matters of judicial guarantees (10,11). These findings converge in pointing out that the technical validity of digital evidence constitutes a necessary, although not sufficient, condition to guarantee comprehensive respect for due process, which also requires conditions of contradiction, procedural equality and sufficient judicial motivation.

Comparative jurisprudence and illustrative cases

The documentary analysis identified several illustrative cases cited repeatedly in the reviewed literature, which allow us to observe the practical application of the principles described above. In one case analyzed within the sample, the acquittal of the defendants was based, among other elements, on the finding that the hash values of the seized computer material did not coincide with those recorded in the police report at the time of the intervention, which led the court to declare the evidence contaminated, invalid and unreliable, due to the lack of certainty about its preservation and authenticity (14). This type of precedent reinforces the practical and not merely theoretical importance of the technical standards for the preservation of digital evidence, to the extent that non-compliance can directly determine the meaning of the ruling. In the Ecuadorian sphere, the National Court of Justice has had the opportunity to rule on the assessment of electronic evidence in processes for computer crimes, reiterating that the mere existence of digital data is not enough to prove its authenticity if the technical process of obtaining it is not documented (22).

On a comparative level, the studies reviewed on Colombia document a jurisprudential development aimed at requiring the intervention of accredited experts and the application of standardized forensic protocols as a condition for the admissibility of digital evidence in judicial processes, in line with the principles of the ISO/IEC 27037 standard (15,23). In Chile, the Public Ministry has developed specific institutional guidelines on the integrity and authenticity of technological evidence, aimed at unifying the action criteria of prosecutors at the national level, an institutional development that, according to the documents analyzed, is still in an incipient stage in the Ecuadorian case (5). These comparative findings suggest that institutional strengthening rather than

exclusively normative constitutes a determining factor for the effective guarantee of due process in the face of digital evidence.

DISCUSSION

The results obtained confirm, in general terms, the findings reported by Avemañay Lema et al. (5), who identified a gap between the regulatory recognition of digital evidence in Ecuador and its practical application, marked by the absence of technical protocols and limitations in the chain of custody. This coincidence suggests that this gap does not constitute an isolated finding, but rather a sustained trend in recent Ecuadorian literature, also documented by Navas-Abad and Vázquez-Martínez (6) and by Morante Mendoza et al. (12), who attribute the problem to the absence of specific regulation on electronic evidence, in contrast to the Model Law on Electronic Evidence promoted for the Latin American region by international cooperation organizations.

In relation to the chain of custody, the findings of this study reinforce what was pointed out by Ordoñez Ordoñez et al. (14), who documented specific cases of impunity derived from the breaking of the chain of custody by security agencies, as well as what was exposed by Quichimbo Román et al. (13) regarding the insufficient regulation of digital evidence in the General Organic Code of Processes. These results are consistent with the international literature: Casey (3) and Kerr (4) have maintained for more than a decade that the volatility of digital evidence requires more rigorous forensic protocols than those applicable to traditional physical evidence, while the ISO/IEC 27037 and ISO/IEC 27042 standards constitute, at a comparative level, the most accepted technical reference for its collection and analysis (15,16), a coincidence that supports the recommendation, supported by multiple studies of the sample, to adopt formally said standards in the Ecuadorian expert protocols.

However, the results of this study partially qualify the conclusions of López (20) and López Morales (21), who, in the comparative Latin American context, maintain that the legal validity of digital evidence has been consolidated more clearly in those countries that have developed specific jurisprudence on its admissibility. Unlike this scenario, the evidence collected in the present study indicates that Ecuador continues to rely on general procedural provisions, without an equivalent autonomous regulatory development, which could explain the greater disparity in judicial criteria identified in the evaluation of Ecuadorian digital evidence compared to that observed in the compared systems (28).

Regarding the guarantees of due process, the findings coincide with the jurisprudence of the Inter-American Court of Human Rights in the case of Suárez Rosero vs. Ecuador, in that they reaffirm that the right of defense requires timely and effective access to the evidence that supports the accusation (11). This convergence reinforces the thesis, also supported by Mendoza (25) and by San Martín Andrade et al. (26), that the technical validity of digital evidence is insufficient if procedural conditions of contradiction and equality of arms are not guaranteed. However, unlike more deterministic positions that attribute the violation of due process exclusively to technological factors, the results of this study suggest that the main causes identified in the literature are institutional and

organizational in nature, lack of protocols, insufficient training, shortage of accredited experts rather than strictly technological, which reorients public policy recommendations towards institutional strengthening rather than solely updating regulations.

An additional aspect that deserves discussion is the practical effectiveness of international cooperation instruments regarding cross-border digital evidence. Although the Budapest Convention constitutes the most cited framework in the literature for obtaining electronic evidence hosted on servers located outside national jurisdiction (17), Ecuador is not part of said instrument as a full subscriber State, which, according to the studies reviewed, hinders the processes of mutual judicial assistance and expeditious conservation of computer data before providers of international messaging and social networking services (2,7). This limitation coincides with what was indicated by the Organization of American States in its regional diagnosis, which identifies international cooperation as one of the most lagging components of the state response to cybercrime in Latin America (2), and suggests that internal regulatory reforms, by themselves, are insufficient if they are not accompanied by an active foreign policy on digital judicial cooperation.

Finally, it is worth noting as a limitation of the present study the eminently documentary nature of the review, which did not incorporate a primary empirical component through interviews or surveys with justice operators, unlike mixed studies such as that of Avemañay Lema et al. (5). It is recommended that future research complement this systematic review with field studies that allow the documentary findings to be contrasted with daily judicial practice in the different judiciaries of the country.

CONCLUSIONS

The systematic review of the literature shows that, although the Ecuadorian legal system and the majority of Latin American criminal systems normatively recognize the validity of digital evidence as a means of proof, said formal recognition is not accompanied by sufficient technical-procedural development, which generates a structural gap between the norm and its practical application in the criminal process.

Strengthening the digital chain of custody, through the adoption of internationally recognized technical standards such as the ISO/IEC 27037 standard and the formal accreditation of computer forensic experts, constitutes an essential condition to guarantee the authenticity and integrity of digital evidence and, therefore, to prevent its exclusion or nullity due to procedural defects.

The impact of digital evidence on the guarantee of due process does not depend exclusively on technological factors, but mainly on institutional conditions related to the specialized training of judges, prosecutors, defenders and experts, as well as the existence of clear protocols that ensure the right of defense, contradiction and reinforced judicial motivation in those criminal processes supported predominantly by electronic evidence, thus responding to the general objective set out in the present study.

REFERENCES

1. De la Torre Muñoz FM, Puertas Realpe AX, Burbano Peña CE. Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador. ISUPOL Rev Investig Segur Ciudadana Orden Público. 2024;(9):43-57.
2. Organización de los Estados Americanos. Ciberdelito en América Latina y el Caribe: diagnóstico regional 2022. Washington DC: Secretaría de Seguridad Multidimensional, OEA; 2022.
3. Vaca H. El análisis forense de memoria RAM como evidencia digital en delitos comunes: simulación de peculado en Ecuador. Rev Dig Cienc Forense. 2026;5(1).
4. Kerr OS. Computer Crime Law. 5th ed. St. Paul: West Academic Publishing; 2022.
5. Avemañay Lema SA, Avemañay Lema AJ, Duarte Correa MA. La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica. Cienc Lat Rev Cient Multidiscip. 2025;9(5):17880-900. doi:10.37811/cl_rcm.v9i6.21212
6. Navas-Abad CE, Vázquez-Martínez DS. La importancia de la prueba digital en los procedimientos penales en Ecuador. Polo Conoc. 2025;10(1):1742-75. doi:10.23857/pc.v10i1.8778
7. Herrera Zapata SM. El papel de la prueba digital en los procedimientos penales en Ecuador: marco legal, desafíos y necesidad de modernización [tesis de maestría]. Quito: Universidad Andina Simón Bolívar; 2025.
8. Asamblea Nacional del Ecuador. Código Orgánico Integral Penal. Registro Oficial Suplemento 180, 10 de febrero de 2014 (actualización 2023).
9. Constitución de la República del Ecuador. Registro Oficial 449, 20 de octubre de 2008.
10. Convención Americana sobre Derechos Humanos. Art. 8, Garantías Judiciales. San José: Organización de los Estados Americanos; 1969.
11. Corte Interamericana de Derechos Humanos. Caso Suárez Rosero Vs. Ecuador. Sentencia de fondo, 12 de noviembre de 1997.
12. Morante Mendoza LE, Safadi Mendoza JA, Gómez Rivera GP. Delitos informáticos y prueba digital en el COIP: validez, cadena de custodia y pericia forense en el Ecuador. Tesla Rev Cient. 2025;5(2):e542. doi:10.55204/trc.v5i2.e542
13. Quichimbo Román MA, Mereci Balcázar LS, Ramón Merchán ME. La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos. Domin Cienc. 2024;10(3):1126-42. doi:10.23857/dc.v10i3.3972
14. Ordoñez Ordoñez LA, Vásquez Olaya AY, Campoverde Nivicela LJ. La impunidad por violentarse la cadena de custodia por parte de la Policía Nacional. Cienc Lat Rev Cient Multidiscip. 2024;8(2):1742-75. doi:10.37811/cl_rcm.v8i2.11208
15. International Organization for Standardization. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO; 2012.
16. International Organization for Standardization. ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO; 2015.

17. Consejo de Europa. Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Budapest: Consejo de Europa; 2001.
18. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Rev Esp Cardiol. 2021;74(9):790-9.
19. González Reyes M. Naturaleza y valoración de la evidencia digital. Salamanca: Universidad de Salamanca; 2021.
20. López JA. Evidencia digital y su admisibilidad en los procesos penales latinoamericanos. Rev Iberoam Derecho Penal Proces. 2023;10(2):55-74.
21. López Morales ZA. Validez jurídica de la prueba digital en Guatemala. Rev Cienc Multidiscip CUNORI. 2023;7(2).
22. Porras MA. La cadena de custodia digital en el proceso penal ecuatoriano. Rev Ecuat Cienc Juríd. 2023;12(3):87-105.
23. Yepes J, Cárdenas S, Gómez D. La evidencia digital en los procesos judiciales colombianos: un análisis forense comparado. Rev Derecho Proces Comp. 2022;8(1):33-49.
24. Espinoza EE. Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos en Ecuador. Rev Cient. 2024;8(2):101-15.
25. Mendoza M. Interpretación y desafíos de la evidencia digital en la investigación criminal. Código Cient Rev Investig. 2024;5(3):480-98. doi:10.55813/gaea/ccri/v5/nE3/328
26. San Martín Andrade MA, Bravo Moreno SR, Garza Lomas CD. Desafíos de la evidencia digital en la protección de datos personales: la cadena de custodia. Rev Lechuzas. 2026;2(4):1-14.
27. Espinales J. Análisis del derecho procesal y los entornos jurídicos. Rev Cient Arbit Investig Comun Mark Empresa REICOMUNICAR. 2023;6(12):89-97.
28. Riofrío García IA, Ruiz K, Lema P. La prueba electrónica en los procesos penales en Ecuador en concordancia con celeridad y economía procesal. Serie Cient UCI. 2025;18(2):49-62.
29. Imaicela Revilla JA, Alvarado Ajila LA. La incorporación de la prueba digital en el derecho procesal ecuatoriano. Rev Lex. 2024;7(27):1338-50. doi:10.33996/revistalex.v7i27.247
30. Valdés R. La excepcional limitación al derecho fundamental a la intimidad: una reflexión sobre la prueba ilícita y su uso a conveniencia. Rev Derecho Debates Pers. 2023.
31. Jiménez Guartán FA. La prueba digital y su valoración en el proceso penal ecuatoriano frente a las garantías constitucionales. Polo Conoc. 2026;11(1):1-18.