Polo del Conocimiento

Pol. Con. (Edición núm. 112) Vol. 10, No 11
Noviembre 2025, pp. 2012-2037
ISSN: 2550 - 682X
DOI: 10.23857/pc.v10i11.10748

Análisis forense digital: La eficacia de la legislación ecuatoriana ante el cibercrimen

Digital forensics: The effectiveness of Ecuadorian legislation against cybercrime

Perícia digital: a eficácia da legislação equatoriana contra o cibercrime

José Ramiro Coronel Maji [I]
ramirocoroneldaan@gmail.com
https://orcid.org/0009-0003-7080-3845

Enrique Efraín Argüello Arellano [II]
efra_argu@hotmail.com
https://orcid.org/0000-0003-2798-2895

Correspondencia: ramirocoroneldaan@gmail.com

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 18 de septiembre de 2025 ***Aceptado:** 24 de octubre de 2025 *** Publicado:** 20 de noviembre de 2025

I. Maestrante de Criminalística y Ciencias Forenses de la Universidad Nacional de Chimborazo, Abogado de los Tribunales y Juzgados de la República; Riobamba – Ecuador.
II. Magíster en Criminalística y Ciencias Forenses Docente de la Maestría en Criminalística y Ciencias Forenses de la Universidad Nacional de Chimborazo; Riobamba – Ecuador.

Resumen

La investigación analiza la eficacia de la evidencia digital dentro del sistema de justicia penal ecuatoriano, considerando la articulación entre el Código Orgánico Integral Penal (COIP), la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General, el Manual de Actuación para la Recolección, Preservación, Tratamiento y Análisis del Contenido Digital, y los principios establecidos en el Convenio de Budapest. A partir de la percepción de 35 operadores judiciales peritos informáticos, fiscales, defensores y jueces, el estudio revela que, aunque el marco normativo es sustancialmente sólido, su aplicación presenta debilidades estructurales derivadas de la escasez de recursos técnicos, la falta de capacitación especializada y la limitada adaptación a nuevas modalidades del cibercrimen. Se concluye que la eficacia de la evidencia digital en Ecuador depende no solo de la normativa, sino también del fortalecimiento institucional y técnico de los actores encargados de su gestión, conforme a los estándares internacionales de investigación y de protección de datos personales.

Palabras Clave: evidencia digital; cibercrimen; cadena de custodia; COIP; LOPDP.

Abstract

This research analyzes the effectiveness of digital evidence within the Ecuadorian criminal justice system, considering the interplay between the Comprehensive Organic Criminal Code (COIP), the Organic Law on the Protection of Personal Data (LOPDP) and its General Regulations, the Manual of Procedures for the Collection, Preservation, Processing, and Analysis of Digital Content, and the principles established in the Budapest Convention. Based on the perceptions of 35 judicial officers, including computer forensics experts, prosecutors, defense attorneys, and judges, the study reveals that, although the legal framework is substantially robust, its application presents structural weaknesses stemming from a scarcity of technical resources, a lack of specialized training, and limited adaptation to new forms of cybercrime. The study concludes that the effectiveness of digital evidence in Ecuador depends not only on the regulations themselves but also on strengthening the institutional and technical capacity of the actors responsible for its management, in accordance with international standards for investigation and personal data protection.

Keywords: digital evidence; cybercrime; chain of custody; COIP; LOPDP.

Resumo

Esta pesquisa analisa a eficácia das provas digitais no sistema de justiça criminal equatoriano, considerando a interação entre o Código Orgânico Integral do Crime (COIP), a Lei Orgânica de Proteção de Dados Pessoais (LOPDP) e o seu Regulamento Geral, o Manual de Procedimentos para a Recolha, Preservação, Processamento e Análise de Conteúdos Digitais e os princípios estabelecidos na Convenção de Budapeste. Com base na perceção de 35 magistrados, incluindo peritos forenses digitais, procuradores, advogados de defesa e juízes, o estudo revela que, embora o quadro legal seja substancialmente robusto, a sua aplicação apresenta fragilidades estruturais decorrentes da escassez de recursos técnicos, da falta de formação especializada e da limitada adaptação às novas formas de cibercrime. O estudo conclui que a eficácia das provas digitais no Equador depende não só da própria legislação, mas também do reforço da capacidade institucional e técnica dos atores responsáveis pela sua gestão, em conformidade com as normas internacionais de investigação e proteção de dados pessoais.

Palavras-chave: provas digitais; cibercrime; cadeia de custódia; COIP; LOPDP.

Introducción

El aumento del cibercrimen en América Latina y el Caribe (LAC) ha evidenciado la necesidad de contar con marcos regulatorios, tanto legales como técnicos, que garanticen la persecución penal efectiva, así como la admisibilidad de la evidencia digital en juicio (Casino et al., 2022).

El Reporte de Ciberseguridad 2020 de la OEA y el BID evalúa la madurez de los países de LAC mediante cinco dimensiones, revelando avances respecto de 2016, como la adopción de estrategias nacionales de ciberseguridad por parte de varios países; sin embargo, persisten brechas significativas, entre ellas la consolidación de marcos legales robustos frente a los desafíos convergentes de la ciberseguridad y el cibercrimen.

En el mismo orden de ideas, el informe del Banco Mundial, *Economics of Cybersecurity for Latin America and the Caribbean*, indica que la región registró la mayor tasa de crecimiento de incidentes divulgados entre 2014 y 2023 (25%), lo que refuerza la necesidad de consolidar capacidades técnico-legales y de cooperación internacional (Diao et al., 2024).

En el ámbito ecuatoriano, la respuesta normativa frente al cibercrimen se articula principalmente con el Código Orgánico Integral Penal (COIP), que constituye la base para la tipificación de conductas como el acceso ilícito, la interceptación de datos, el fraude informático, entre otras.

Complementariamente, la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General introducen principios de licitud, consentimiento y proporcionalidad en el tratamiento de la información sensible, que condicionan la forma de obtener y utilizar la evidencia digital (Rosas-Lanas & Pila-Cárdenas, 2023).

De manera complementaria, la ratificación del Convenio de Budapest en 2024 fortalece la cooperación internacional y establece directrices técnicas para la preservación de datos. Así, esta triple dimensión —represiva en el ámbito penal, garantista en la protección de datos y cooperativa en el plano internacional— revela la existencia de un marco formal robusto, aunque con limitaciones prácticas en su implementación (Ponce Tubay, 2024).

En este sentido, el debate no se reduce a la mera existencia de normas penales y de protección de datos, sino a su eficacia práctica en la investigación y la judicialización del cibercrimen. Como advierte Reedy (2023), la validez de la evidencia digital depende tanto de la rigurosidad técnica en su recolección y preservación como de la capacidad de los marcos legales para garantizar su admisibilidad.

Marco Teórico

El desarrollo acelerado de las tecnologías de la información y la comunicación ha transformado vertiginosamente las dinámicas en todos los campos, incluido el delictivo, al potenciarlas y generar nuevas formas de criminalidad que desbordan la categorización jurídica tradicional. En este contexto, el análisis forense digital adquiere un papel central, dado que el ecosistema digital plantea desafíos inéditos para la obtención, preservación y valoración de la evidencia en el proceso penal (Malik et al., 2024).

Por lo tanto, comprender la eficacia del marco normativo nacional e internacional frente al cibercrimen requiere examinar los fundamentos conceptuales, jurídicos y técnicos que sustentan la gestión de la evidencia digital y su validez procesal.

Definición y alcance del cibercrimen

Si bien no existe una aceptación universal sobre la definición de cibercrimen, para fines de este articulo mencionaremos que es una categoría que engloba los delitos cometidos a través del uso de una computadora, sistema informático o redes electrónicas (Lee, Kang & Kim, 2023), mientras que

ciberdelito suele utilizarse para referirse a la tipificación penal especifica de determinadas conductas dentro de cada legislación nacional.

Esta distinción, con una semántica relativamente sutil, es clave desde la perspectiva jurídica, pues permite comprender la delimitación de los marcos normativos y de las políticas de persecución penal, así como la especialización pericial que estas conductas requieren (Zhang & Gong, 2024). Así, el cibercrimen se concibe como un fenómeno global y transnacional, mientras que el ciberdelito representa su concreción normativa local, como ocurre en el COIP.

La evidencia digital como elemento probatorio

Frente a esta realidad, la evidencia digital se configura como el elemento con carácter probatorio que permitirá establecer el nexo causal entre la acción y su autor (Díaz-Pérez et al., 2022; Abdullah et al., 2025). Su naturaleza volátil, reproducible y sensible a la manipulación exige procedimientos técnicos estandarizados para garantizar su autenticidad e integridad.

En este sentido, la norma ISO/IEC 27037:2012 constituye un referente internacional que orienta la identificación, recolección y preservación de la evidencia digital, mientras que las normas ISO/IEC 27041 y 27042 establecen lineamientos para el análisis y la presentación (International Organization for Standardization [ISO], 2012, 2015, 2015).

La cadena de custodia digital y su legitimidad jurídica

La cadena de custodia digital constituye un principio *sine qua non* de la legitimación jurídica en un proceso penal, pues asegura que el elemento considerado como evidencia digital potencial no haya sufrido alteración desde su adquisición hasta su presentación en la etapa de juicio (D'Anna et al., 2023; Ludeña et al., 2025).

Su cumplimiento se ajusta a los criterios de validez científica establecidos en el estándar Daubert, al exigir la reproducibilidad, la transparencia metodológica y la trazabilidad técnica en los informes periciales (Alcoceba Gil, 2018).

Este principio guarda estrecha relación con el artículo 457 del COIP, que dispone que la valoración de la prueba se base en su legalidad, autenticidad, cadena de custodia y aceptación científica y técnica. Dicho precepto coincide con los criterios del estándar Daubert, que exige que las pericias sean reproducibles, verificables y sustentadas en métodos científicamente aceptados. En conjunto, ambos marcos consolidan la exigencia de rigor técnico y de transparencia metodológica como

condiciones indispensables para la admisibilidad judicial de la evidencia digital (Asamblea Nacional del Ecuador, 2014; Brunty, 2023).

Etapas del proceso forense digital

Diversos estudios recientes coinciden en que el proceso asociado a la obtención del contenido digital se desarrolla en varias etapas sucesivas que otorgan fiabilidad a lo actuado por parte del experto, debido a que aseguran la integridad y trazabilidad de la potencial evidencia digital: identificación, adquisición, preservación, análisis y presentación del informe (Thakar et al., 2021; Malik et al., 2024).

En ese sentido, autores como AlKhanafseh & Surakhi (2024) y Lim et al. (2025) destacan que la adecuada aplicación de estas etapas constituye la base metodológica de toda investigación forense digital.

Comprendidos los fundamentos conceptuales y técnicos del análisis forense digital, resulta indispensable examinar el entramado jurídico que regula su aplicación en los niveles internacional y nacional.

Marco normativo internacional y nacional

El Convenio de Budapest y la cooperación internacional

El Convenio sobre Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, fue abierto a la firma en 2001; sin embargo, entró en vigor en 2004. Este instrumento constituye el principal referente jurídico internacional en materia de cibercrimen. Su objetivo es armonizar la tipificación de los delitos informáticos, establecer medidas procesales e investigativas homogéneas, así como fortalecer la cooperación judicial y técnica entre Estados (Consejo de Europa, 2001).

En el caso de Ecuador, desde diciembre de 2024 se convirtió oficialmente en el Estado Parte número 77 (Council of Europe, 2024). Esta adhesión consolida la armonización entre las normas internacionales de cooperación penal y el marco jurídico nacional establecido en el COIP, ambos orientados a fortalecer la persecución de los delitos informáticos y la obtención de evidencia digital (Jinad et al., 2024). Mientras el Convenio establece los lineamientos globales en materia de tipificación y cooperación, el COIP los incorpora y adecua a la estructura institucional y procesal ecuatoriana.

La protección de datos personales como eje transversal

En relación con lo anterior, la Ley Orgánica de Protección de Datos Personales y su Reglamento General constituyen un eje transversal que condiciona la aplicación de dichas normas. Ambos instrumentos introducen principios de licitud, consentimiento y proporcionalidad en el tratamiento de la información digital, estableciendo obligaciones para responsables y encargados del tratamiento de datos (Cabezas et al., 2024).

Este marco garantista delimita la forma en que la información con potencial valor probatorio puede obtenerse y utilizarse, equilibrando la eficacia investigativa con la protección de los derechos fundamentales de los titulares, conforme a los artículos 5 y 7 del Reglamento de la LOPDP (2023).

El Manual de Actuación del SEIIMLCF y la eficacia operativa del sistema

A pesar de estos avances significativos en el abordaje investigativo y procesal penal, la eficacia del marco normativo ecuatoriano frente a los desafíos del cibercrimen depende de la implementación de mecanismos técnicos, institucionales y de coordinación interagencial que garanticen una respuesta oportuna (Paspuel Hernández et al., 2024).

En este contexto, el Manual de Actuación para la Recolección, Preservación, Tratamiento y Análisis del Contenido Digital del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses (SEIIMLCF, 2025) representa un avance sustantivo en la estandarización de la práctica forense digital, al integrar principios de trazabilidad, integridad y debido proceso. No obstante, su implementación práctica aún enfrenta limitaciones relacionadas con la desigualdad de capacitación del personal, la falta de interoperabilidad tecnológica entre instituciones y la ausencia de mecanismos de supervisión homogéneos que garanticen su cumplimiento efectivo.

En consecuencia, la efectividad normativa no se evalúa únicamente por la existencia de disposiciones legales o de manuales técnicos, sino también por su capacidad para aplicarse de manera uniforme y verificable en todas las etapas de la investigación penal. Lograr esa coherencia operativa entre el marco jurídico, la praxis forense y la cooperación interinstitucional constituye el principal desafío del Ecuador frente al cibercrimen (Casino et al., 2021).

Metodología

Enfoque y diseño de investigación

El presente estudio se fundamenta en un diseño mixto de carácter descriptivo y exploratorio, que articula el análisis documental con la recolección de percepciones operativas de los actores del sistema de justicia penal vinculados al abordaje del cibercrimen. Los enfoques mixtos permiten integrar la objetividad del análisis cuantitativo con la profundidad interpretativa del cualitativo, lo cual resulta adecuado para abordar fenómenos complejos, como la aplicación judicial de la normativa penal en entornos tecnológicos (Forni & De Grande, 2020).

En cuanto a su estructura metodológica, esta investigación se desarrolla en dos fases complementarias. Primero se realizó un análisis normativo de los instrumentos nacionales e internacionales que regulan la gestión de la evidencia digital —Código Orgánico Integral Penal (COIP), Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y el Convenio de Budapest sobre Ciberdelincuencia—, y posteriormente se recopiló información empírica mediante una encuesta estructurada dirigida a jueces, fiscales, defensores y peritos informáticos, con el fin de identificar percepciones sobre la validez probatoria, la cadena de custodia y la coordinación interinstitucional.

Fuentes de información

El presente trabajo se sustenta en fuentes verificables y pertinentes al contexto ecuatoriano. En el caso de las fuentes normativas, se seleccionaron por su vigencia, aplicabilidad y alcance operativo, priorizando instrumentos legales y tratados internacionales directamente relacionados con la gestión de la evidencia digital y la persecución penal del cibercrimen. En este sentido, la investigación jurídica exige procedimientos sistemáticos, rigurosos y verificables, pues genera nuevos constructos de conocimiento jurisprudencial (Obando-Peralta, 2024, p. 59), integrando la dimensión teórica con su aplicación práctica.

De manera complementaria, las fuentes empíricas provinieron de los cuestionarios aplicados a operadores judiciales y peritos informáticos, cuyas respuestas reflejan la práctica institucional en torno a la obtención y valoración de la evidencia digital.

Esta combinación de insumos legales, técnicos y testimoniales fortaleció la validez del estudio al permitir contrastar el marco jurídico con la realidad operativa de las instituciones encargadas de investigar y procesar delitos informáticos.

Recolección de percepciones operativas

Con el objetivo de contrastar la normativa con su aplicación práctica, se aplicó una encuesta estructurada a un total de 41 profesionales que aceptaron participar; 35 completaron el cuestionario hasta el final (tasa de respuesta: 85.37%), distribuidos en cuatro grupos: 2 jueces (5.88%), 3 fiscales (8.82%), 10 defensores públicos y privados (26.47%) y 20 peritos informáticos (58.82%). La mayoría de los participantes labora en las provincias de Pichincha (71.43%, n=25) y Guayas (17.14%, n=6), lo que refleja la concentración de instituciones judiciales en estas regiones.

El cuestionario estuvo conformado por 13 preguntas, estructuradas en tres bloques temáticos:

a) ***Perfil profesional (4 preguntas):*** rol, provincia de trabajo, años de experiencia y frecuencia de trabajo con evidencia digital,

b) ***Evaluación del marco legal y procedimientos (8 preguntas)*****:** una pregunta de selección múltiple sobre tipos de casos que requieren evidencia digital, y siete preguntas bajo escala tipo Likert de cinco puntos (1 = totalmente en desacuerdo; 5 = totalmente de acuerdo) que evaluaron dimensiones relacionadas con la adecuación del COIP en la tipificación del cibercrimen, la claridad de la Ley Orgánica de Protección de Datos Personales, los protocolos de cadena de custodia, la admisibilidad judicial, los recursos técnicos disponibles, el conocimiento del Convenio de Budapest y la preparación del marco legal para nuevas tipologías delictivas.

c) ***Obstáculos percibidos (1 pregunta abierta):*** identificación del principal obstáculo para la eficacia de la evidencia digital en los procesos judiciales.

El tamaño muestral, aunque reducido, se justifica por el carácter especializado de la población y por las limitaciones de acceso propias de las funciones judiciales y periciales. En este tipo de investigaciones, la suficiencia muestral se evalúa por la pertinencia y la profundidad de la información obtenida, más que por su volumen (Parra, 2019; Vasileiou et al., 2018; Boddy, 2016).

Análisis de datos

Para el tratamiento de la información se emplearon técnicas de estadística descriptiva —frecuencias absolutas y relativas, porcentajes, medidas aritméticas (M), desviación estándar (DE) e intervalos de confianza al 95% (IC 95%)— que permitieron identificar patrones de percepción entre los grupos profesionales encuestados. Los datos fueron procesados en Microsoft Excel.

Dada la naturaleza ordinal de las escalas Likert y el tamaño limitado de la muestra, se reportan medidas de tendencia central y de dispersión sin asumir normalidad de la distribución de las

respuestas. Para cada ítem de evaluación del marco legal, se calculó el porcentaje de respuestas agrupadas en tres categorías: desacuerdo (totalmente en desacuerdo + en desacuerdo), neutral (ni de acuerdo ni en desacuerdo) y acuerdo (de acuerdo + totalmente de acuerdo), lo cual facilita la interpretación de las tendencias generales (Sosa González et al., 2020).

Las respuestas a la pregunta abierta sobre obstáculos se analizaron mediante el enfoque de análisis temático reflexivo propuesto por Braun & Clarke (2019). Este método permitió identificar patrones temáticos recurrentes mediante un proceso sistemático de familiarización con los datos, generación de códigos iniciales, búsqueda y revisión de temas, definición de categorías y su posterior presentación.

Del total de 35 participantes, 33 proporcionaron respuestas sustantivas a la pregunta abierta, las cuales se codificaron inductivamente hasta alcanzar saturación temática, identificándose seis categorías principales: falta de capacitación, desconocimiento de operadores judiciales, marco legal desactualizado, falta de recursos y de equipos, problemas en la cadena de custodia y corrupción.

La integración de los resultados cuantitativos y cualitativos fortaleció la validez interpretativa de los hallazgos, en consonancia con lo señalado por Wilkes et al. (2022), quienes sostienen que los métodos mixtos incrementan la solidez analítica y explicativa al combinar evidencias de distinta naturaleza en una misma estrategia de investigación.

Consideraciones éticas

El estudio se desarrolló conforme a los principios éticos de la investigación social y jurídica, resguardando la confidencialidad y el anonimato de los participantes (Santi, 2016). La encuesta fue autoaplicada y voluntaria, previa aceptación de un consentimiento informado digital, con una tasa de aceptación del 100% entre quienes iniciaron el cuestionario.

El tratamiento de la información se ajustó a lo dispuesto en la Ley Orgánica de Protección de Datos Personales y su Reglamento General, garantizando la minimización de datos, el almacenamiento seguro y la eliminación controlada tras el análisis. No se utilizó información sensible ni se accedió a procesos judiciales activos, lo que asegura la validez ética y la replicabilidad del estudio.

Resultados

Perfil de los participantes

Del total de 41 profesionales que aceptaron participar en el estudio, 35 completaron el cuestionario completo, representando una tasa de respuesta del 85,37 %. La distribución por rol profesional mostró una composición heterogénea, con predominio de peritos informáticos (58.82%, n=20), seguidos por defensores públicos y privados (26.47%, n=10), fiscales (8.82%, n=3) y jueces (5.88%, n=2). Esta configuración refleja la naturaleza técnico-probatoria de la evidencia digital y la necesidad de integrar criterios interdisciplinarios en la valoración judicial, en consonancia con el artículo 456 del COIP, que establece la cadena de custodia como responsabilidad compartida entre peritos, fiscales y servidores judiciales.

Tabla 1

Características demográficas de los participantes

Rol	Frecuencia	Porcentaje	Porcentaje acumulado
Juez	2	5,88	5,88
Fiscal	3	8,82	14,7
Defensor	10	26,47	41,17
Perito Informático	20	58,82	100
Total	**35**	**100**	—

Nota: Elaboración propia de los autores a partir de una encuesta aplicada a operadores judiciales.

En cuanto a la distribución geográfica, la mayoría de los participantes laboran en la provincia de Pichincha (71.43%, n=25), seguida por Guayas (17.14%, n=6), Chimborazo (5.71%, n=2), El Oro (2.86%, n=1) y Manabí (2.86%, n=1). La concentración en las dos principales provincias coincide con la ubicación de las instancias judiciales superiores y de los laboratorios forenses nacionales, lo cual es coherente con la estructura institucional descrita en el artículo 448 del COIP.

Respecto a la experiencia profesional en el área, el 40% (n=14) de los participantes reportó tener entre 3 y 5 años de trayectoria, el 25.71% (n=9) más de 11 años, el 20% (n=7) menos de 2 años, y el 14.29% (n=5) entre 6 y 10 años (M=2.46, DE=1.094). Esta distribución indica que, si bien existe un segmento considerable con amplia experiencia, la mayoría se encuentra en etapas intermedias

del desarrollo profesional, lo que podría influir en la percepción de las capacidades institucionales y de la aplicación de la normativa.

La frecuencia de trabajo con evidencia digital mostró niveles elevados de exposición práctica a la problemática investigada. El 45.71% (n=16) de los participantes indicó trabajar con evidencia digital muy frecuentemente, el 22.86% (n=8) frecuentemente, el 22.86% (n=8) ocasionalmente y solo el 8.57% (n=3) declaró no haber trabajado nunca con este tipo de evidencia (M=3.06, DE=1.027). Estos datos evidencian que la muestra cuenta con experiencia directa y sistemática en los desafíos operativos asociados a la recolección, preservación y valoración de la evidencia digital en procesos judiciales.

Tipos de casos que requieren evidencia digital

La pregunta sobre los tipos de casos que, en la experiencia de los participantes, requieren el uso de evidencia digital generó múltiples respuestas, totalizando 118 menciones entre los 35 encuestados. Los resultados revelaron siete categorías principales, con frecuencias y distribuciones que reflejan las modalidades delictivas más prevalentes en el contexto ecuatoriano.

El tipo de caso más frecuentemente identificado fue el material de abuso sexual infantil (68.57%, n=24), seguido por la extorsión digital y ransomware (57.14%, n=20) y el fraude electrónico o phishing (51.43%, n=18). Estas tres categorías concentran las menciones más elevadas y reflejan delitos de alto impacto social que requieren capacidades técnicas especializadas tanto para la investigación como para la preservación de la evidencia.

Tabla 2

Tipos de casos que requieren evidencia digital

Tipo de caso	n	%
Material de abuso sexual infantil	24	68,57
Extorsión digital y ransomware	20	57,14
Fraude electrónico o phishing	18	51,43
Acceso ilícito a sistemas	16	45,71
Violación de datos personales o doxing	16	45,71
Otros	13	37,14
Interceptación ilícita o espionaje	11	31,43

Nota. Pregunta de respuestas múltiples. Total de menciones = 118. Base: N = 35.

En un nivel intermedio de prevalencia se identificaron el acceso ilícito a sistemas (45.71%, n=16) y la violación de datos personales o doxing (45.71%, n=16), ambos con igual proporción de menciones, delitos directamente vinculados con la Ley Orgánica de Protección de Datos Personales y su Reglamento General, los cuales exigen la obtención de consentimiento expreso y medidas de seguridad adecuadas en el tratamiento de información (arts. 5–7 del Reglamento General).

Finalmente, la categoría "Otros" fue señalada por el 37,14 % (n = 13) de los participantes, lo que sugiere la existencia de modalidades delictivas emergentes o de casos mixtos que no se ajustan plenamente a las tipificaciones tradicionales. La interceptación ilícita o espionaje fue la categoría menos mencionada (31,43%, n=11), aunque su presencia evidencia la persistencia de delitos vinculados a la vulneración de comunicaciones privadas.

La diversidad de respuestas y el hecho de que varios participantes señalaran múltiples tipos de casos indican que la evidencia digital es transversal a un amplio espectro de conductas delictivas, lo que plantea exigencias diferenciadas en términos de formación técnica, coordinación institucional y actualización normativa.

Evaluación del marco legal y procedimientos institucionales

La evaluación del marco legal ecuatoriano en materia de cibercrimen y de la gestión de la evidencia digital arrojó resultados heterogéneos, con áreas de relativa solidez normativa y procedimientos claramente deficitarios. Los participantes valoraron seis dimensiones clave mediante escalas tipo Likert de cinco puntos, cuyos resultados se presentan a continuación en orden descendente según su media aritmética.

Tabla 3

Evaluación del marco legal y procedimientos institucionales

Dimensión evaluada	**M**	**DE**	**IC 95%**
Protocolos de cadena de custodia	3,31	1,16	[2.93, 3.70]
Ley Orgánica de Protección de Datos Personales	3,21	1,01	[2.87, 3.55]
Admisibilidad y valoración judicial	2,94	1,21	[2.54, 3.34]
Tipificación del cibercrimen en el COIP	2,82	0,97	[2.50, 3.15]
Preparación para nuevas tipologías delictivas	2,71	1,19	[2.30, 3.11]
Recursos técnicos y talento humano especializado	2,37	1	[2.04, 2.70]

Nota. Escala Likert de 5 puntos (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo).

M = media; DE = desviación estándar; IC = intervalo de confianza. N = 35.

Protocolos de cadena de custodia

Los protocolos institucionales sobre la cadena de custodia de la evidencia digital obtuvieron la valoración más alta entre todas las dimensiones evaluadas (M=3.31, DE=1.157, IC 95% [2.931-3.698]). El 48.57% (n=17) de los participantes manifestó estar de acuerdo con que los protocolos son claros, actualizados y aplicables en la práctica, mientras que el 8.57% (n=3) expresó estar totalmente de acuerdo, lo que suma un 57.14% de respuestas favorables. Por otra parte, el 20% (n=7) adoptó una posición neutral y el 22.86% manifestó desacuerdo (11.43% en desacuerdo, n=4; 11.43% totalmente en desacuerdo, n=4).

Estos resultados sugieren que, en términos generales, los procedimientos de preservación y trazabilidad de la evidencia digital cuentan con una aceptación mayoritaria entre los operadores, aunque persisten desafíos en su aplicación uniforme, particularmente entre quienes expresaron desacuerdo o neutralidad.

Ley Orgánica de Protección de Datos Personales

La claridad y utilidad de la LOPDP y de su Reglamento General para el tratamiento de la evidencia que involucra datos personales obtuvieron una valoración favorable (M=3.21, DE=1.008, IC 95% [2.867-3.545]). El 44.12% (n=15) estuvo de acuerdo con su claridad y utilidad, y el 2.94% (n=2) totalmente de acuerdo, sumando un 47.06% de percepciones positivas. Un tercio de los participantes (32.35%, n=11) se mantuvo en una posición neutral, mientras que el 20.58% expresó desacuerdo (11.76% en desacuerdo, n=4; 8.82% totalmente en desacuerdo, n=3).

Estos datos indican que, aunque la normativa sobre protección de datos personales es valorada positivamente por cerca de la mitad de los encuestados, existe una proporción considerable que aún no percibe su aplicabilidad práctica o considera que su implementación requiere mayor claridad operativa.

Admisibilidad y valoración judicial de la evidencia digital

La consistencia y uniformidad en la admisibilidad y valoración judicial de la evidencia digital entre los distintos tribunales ecuatorianos obtuvieron una valoración intermedia-baja (M=2.94, DE=1.211, IC 95% [2.542-3.344]). El 37.14% (n=13) estuvo de acuerdo en que existe consistencia

y el 5.71% (n=2) estuvo totalmente de acuerdo, lo que suma un 42.85% de respuestas favorables. Sin embargo, el 40% de los participantes manifestó desacuerdo (25.71% en desacuerdo, n=9; 14.29% totalmente en desacuerdo, n=5), y el 17.14% (n=6) adoptó una posición neutral.

Esta polarización en las respuestas evidencia percepciones divididas sobre la aplicación judicial de los estándares probatorios relativos a la evidencia digital, lo que sugiere disparidades en los criterios interpretativos entre los tribunales o insuficiencias en la formación judicial en estos temas.

Tipificación del cibercrimen en el COIP

La suficiencia de la tipificación de los ciberdelitos más comunes en el Código Orgánico Integral Penal incluyendo fraude electrónico, acceso ilícito, sabotaje y material de abuso sexual infantil recibió una valoración ambivalente (M=2.82, DE=0.968, IC 95% [2.498-3.149]). Solo el 26.47% expresó acuerdo (23.53% de acuerdo, n=8; 2.94% totalmente de acuerdo, n=2), mientras que el 41.17% manifestó desacuerdo (35.29% en desacuerdo, n=12; 5.88% totalmente en desacuerdo, n=2). Un tercio de los participantes (32.35%, n=11) se mantuvo neutral.

Estos resultados revelan que una proporción significativa de los operadores del sistema de justicia considera que la tipificación actual del COIP no abarca de manera suficiente las modalidades y características del cibercrimen contemporáneo, lo que podría generar vacíos de punibilidad o dificultades para la subsunción de conductas delictivas emergentes.

Preparación del marco legal para nuevas tipologías delictivas

La preparación del marco legal ecuatoriano para enfrentar nuevas tipologías de ciberdelito —como phishing, doxing y delitos asistidos por inteligencia artificial— obtuvo una de las valoraciones más bajas (M=2.71, DE=1.194, IC 95% [2.304-3.107]). El 50% de los participantes expresó desacuerdo (35.29% en desacuerdo, n=13; 14.71% totalmente en desacuerdo, n=5), mientras que solo el 26.47% manifestó acuerdo (17.65% de acuerdo, n=6; 8.82% totalmente de acuerdo, n=3). El 23.53% (n=8) adoptó una posición neutral.

Estos datos evidencian una percepción mayoritaria de desactualización normativa ante la evolución tecnológica y las nuevas formas de criminalidad digital, lo que plantea desafíos tanto legislativos como operativos para la persecución efectiva de estos delitos.

Recursos técnicos y talento humano especializado

La disponibilidad de recursos técnicos y de talento humano especializado suficientes para atender la demanda de pericias que involucran evidencia digital recibió la valoración más crítica en todas las dimensiones evaluadas (M=2.37, DE=1.003, IC 95% [2.039-2.704]). El 60% de los participantes expresó desacuerdo (40% en desacuerdo, n=14; 20% totalmente en desacuerdo, n=7), lo que constituye el déficit más pronunciado identificado en el estudio. Solo el 17.14% (n=6) manifestó estar de acuerdo; ninguno expresó total acuerdo y el 22.86% (n=8) se mantuvo neutral. Esta percepción de insuficiencia estructural de recursos técnicos y humanos constituye un obstáculo fundamental para la eficacia del sistema de justicia penal en el procesamiento de casos de cibercrimen, independientemente de las fortalezas normativas o procedimentales que puedan existir en otros ámbitos.

Conocimiento y uso del Convenio de Budapest

La mayoría de los participantes (57.14%, n=20) declaró no conocer los mecanismos del Convenio de Budapest. El 40% (n=14) indicó conocerlos, pero no haberlos utilizado en su práctica profesional. Solo un participante (2.86%) manifestó conocer y haber utilizado efectivamente estos mecanismos de cooperación internacional.

Tabla 4

Conocimiento y uso del Convenio de Budapest

Nivel de conocimiento y uso	**n**	**%**
No conoce los mecanismos	20	57,14
Conoce, pero no ha utilizado	14	40
Conoce y ha utilizado	1	2,86
Total	**35**	**100**

Nota. Solo 1 participante (2.86%) ha utilizado efectivamente los mecanismos de cooperación internacional del Convenio de Budapest. N = 35.

Estos datos evidencian una desconexión significativa entre los instrumentos internacionales disponibles y su aplicación práctica en el contexto ecuatoriano, lo que limita la capacidad del sistema de justicia para investigar ciberdelitos con componentes transnacionales o que requieren asistencia internacional para obtener evidencia almacenada en servidores extranjeros.

Obstáculos para la eficacia de la evidencia digital: análisis cualitativo

La pregunta abierta sobre el principal obstáculo para la eficacia de la evidencia digital en los procesos judiciales ecuatorianos generó 33 respuestas sustantivas, cuyo análisis temático y reflexivo permitió identificar seis categorías principales. La Tabla 5 presenta la frecuencia y la distribución porcentual de estas categorías, junto con ejemplos representativos extraídos de las respuestas textuales.

Tabla 5

Principal obstáculo para la eficacia de la evidencia digital

Categoría	n	%
Falta de capacitación	12	36,4
Desconocimiento de los operadores de justicia	10	30,3
Marco legal desactualizado o ambiguo	6	18,2
Falta de recursos técnicos y equipamiento	5	15,2
Problemas en la cadena de custodia	4	12,1
Corrupción	1	3

Nota. Análisis temático reflexivo de respuestas abiertas.

Base: n = 33 respuestas sustantivas de 35 participantes.

Falta de capacitación

La categoría más prevalente, mencionada por el 36.4% (n=12) de los participantes, fue la falta de capacitación de los operadores del sistema de justicia. Las respuestas enfatizaron deficiencias formativas tanto en aspectos técnicos de la informática forense como en el manejo procedimental de la evidencia digital. Un participante señaló:

"La falta de capacitación técnica en operadores judiciales ya que muchos jueces, fiscales y defensores públicos no tienen formación especializada en informática forense o manejo de evidencia digital, lo que puede generar dudas sobre su validez o interpretación."

Desconocimiento de los operadores de justicia

Estrechamente relacionada con la anterior, esta categoría fue identificada por el 30.3% (n=10) de los participantes y enfatiza no solo la falta de formación estructurada, sino también el

Pol. Con. (Edición núm. 112) Vol. 10, No 11, Noviembre 2025, pp. 2012-2037, ISSN: 2550 - 682X

desconocimiento generalizado de la evidencia digital entre jueces, fiscales y defensores. Las menciones incluyeron: *"Desconocimiento por parte de fiscales y jueces"; "El desconocimiento del marco legal respectivo"; "Conocimiento técnico por parte de los entes de justicia, abogados defensores."*

Un participante precisó: *"La falta de conocimiento al respecto en los ámbitos investigativos, judiciales, etc."*, subrayando que el problema trasciende el ámbito judicial y también alcanza a las instituciones de investigación criminal.

Marco legal desactualizado o ambiguo

El 18.2% (n=6) de los participantes identificó limitaciones en la normativa vigente, señalando que esta no se adapta a la velocidad de evolución de las modalidades delictivas en el ciberespacio. Un participante expresó:

"La redacción genérica de la normativa legal, pues no se adapta a la velocidad con la que evolucionan las modalidades delictivas en el ciberespacio. Se requiere una actualización normativa para tipificar de forma clara extorsión digital, ransomware, ataques a infraestructuras críticas, ciberacoso, grooming online y nuevas modalidades de fraude electrónico."

Falta de recursos técnicos y equipamiento

El 15.2% (n=5) de los participantes señaló la insuficiencia de recursos materiales y tecnológicos omo el principal obstáculo. Las menciones incluyeron: "*Falta de equipos forenses para la alta demanda que existe"; "Falta de equipamiento para la extracción de la información".*

Un participante especificó: *"Falta mayor infraestructura, especialistas en la materia, leyes más específicas y procedimientos legales más eficientes y avanzados"*, integrando el déficit de recursos con otras dimensiones del problema.

Problemas en la cadena de custodia

El 12.1% (n=4) de los participantes identificó vulnerabilidades en la preservación, el manejo y la trazabilidad de la evidencia digital. Las respuestas incluyeron: *"Vulnerabilidad en la cadena de custodia"; "Tratamiento de la evidencia"; "El mal manejo de la evidencia digital por parte del personal del eje investigativo".*

Un participante señaló: *"Debe tener un tratamiento digital adecuado desde el primer interviniente"*, subrayando la importancia de la actuación inicial en el lugar de los hechos para garantizar la integridad posterior de la evidencia.

Corrupción

Un único participante (3.0%) mencionó *"La corrupción y el soborno" como el principal obstáculo*, lo que, si bien constituye una frecuencia marginal, introduce una dimensión ética y de integridad institucional que no puede ser desestimada en el análisis global de la eficacia del sistema de justicia penal.

El análisis cualitativo evidencia que los principales obstáculos son multidimensionales y se articulan entre sí. La falta de capacitación y el limitado conocimiento técnico-jurídico de los operadores identificados por el 66,7% de los participantes conforman el eje central del problema, amplificado por carencias estructurales de recursos, vacíos normativos y debilidades procedimentales.

Uno de los participantes resumió esta situación al afirmar: *"El obstáculo no es la falta de evidencia, sino la ausencia de estandarización de la evidencia digital entre fiscales, jueces y peritos."* Esta percepción refleja que el desafío no radica únicamente en las capacidades individuales, sino en la inexistencia de criterios y protocolos unificados que garanticen coherencia en el manejo de la evidencia digital a lo largo del proceso judicial.

En síntesis, la falta de capacitación especializada (36,4%) y el desconocimiento técnico-jurídico (30,3%) se perfilan como los obstáculos más recurrentes, en correspondencia con la escasez de personal experto y la limitada apropiación de marcos internacionales como el Convenio de Budapest.

Discusión

Los resultados evidencian una paradoja estructural en la respuesta ecuatoriana frente al cibercrimen: aunque el país cuenta con un marco normativo sólido — Manual de Actuación para la Recolección, Preservación, Tratamiento y Análisis del Contenido Digital (SEIIMLCF, 2025) y Convenio de Budapest—, su aplicación se ve limitada por la falta de recursos técnicos, infraestructura forense y capacitación especializada (Klasén, Fock & Forchheimer, 2024). Las mayores valoraciones en cadena de custodia (M=3.31) y protección de datos (M=3.21) contrastan

con las bajas en equipamiento y personal capacitado (M=2.37), confirmando que la eficacia normativa depende de la capacidad institucional para aplicarla (Reedy, 2023; Lim et al., 2025).

El 66,7 % de los participantes señaló la falta de formación especializada como el principal obstáculo, afectando tanto la aplicación de protocolos como la valoración judicial de la evidencia. Aunque el Manual de Actuación proporciona directrices técnicas claras para la gestión de evidencia digital, su implementación sigue siendo desigual por la limitada formación en informática forense entre jueces y fiscales. Esta carencia restringe la aplicación de los criterios de autenticidad y validez establecidos en el COIP y en el estándar Daubert (Brunty, 2023), generando riesgos de inadmisión o valoración inconsistente de la prueba digital (Ismail & Ariffin, 2025). Además, el 57,1 % reconoció desconocer los mecanismos operativos del Convenio de Budapest, lo que evidencia la brecha entre la adhesión formal y la cooperación judicial efectiva (Jinad et al., 2024; Diao et al., 2024).

Estos hallazgos demandan políticas públicas orientadas a fortalecer las capacidades institucionales. Es prioritario establecer programas permanentes de formación en informática forense para jueces, fiscales y defensores; invertir sostenidamente en infraestructura tecnológica y talento humano; y actualizar el COIP para incorporar nuevas tipologías delictivas ransomware, doxing, grooming online y delitos asistidos por IA en armonía con el Convenio de Budapest. En suma, el caso ecuatoriano refleja un desafío regional: cerrar la brecha entre el diseño normativo y su aplicación práctica mediante cooperación internacional y justicia digital técnicamente competente (Casino et al., 2022).

Conclusiones

- La investigación evidencia una dualidad en la respuesta ecuatoriana frente al cibercrimen: un marco normativo robusto COIP, LOPDP, el Manual de Actuación para la Recolección, Preservación, Tratamiento y Análisis del Contenido Digital (SEIIMLCF, 2025) y Convenio de Budapest convive con limitaciones estructurales que reducen su eficacia. El análisis de 35 operadores judiciales reveló fortalezas en la cadena de custodia (M=3.31) y la protección de datos personales (M=3.21), pero también deficiencias en recursos técnicos (M=2.37), actualización normativa (M=2.71) y uniformidad en la admisibilidad judicial (M=2.94). Solo el 42,86% de los participantes conoce el Convenio de Budapest y apenas el 2,86% lo ha aplicado, lo que refleja una desconexión entre la adhesión formal y la práctica judicial.

- El problema, más que normativo, es operativo y formativo. Dos tercios de los encuestados atribuyen las limitaciones a la falta de capacitación y de conocimiento técnico-jurídico, agravadas por la concentración geográfica de especialistas en Pichincha y Guayas y por la escasa experiencia en manejo de evidencia digital. La frecuencia de casos de abuso sexual infantil (68,57%), ransomware (57,14%) y fraude electrónico (51,43%) demuestra la transversalidad del cibercrimen y la necesidad de que todos los operadores comprendan los principios básicos de recolección, preservación y valoración de evidencia digital.
- Si bien los procedimientos de cadena de custodia muestran consolidación, el COIP aún no tipifica con claridad conductas emergentes como doxing, ciberacoso o delitos asistidos por IA, lo que limita la capacidad del sistema penal para adaptarse al cambio tecnológico. La falta de criterios judiciales uniformes en la valoración probatoria genera disparidades entre tribunales y afecta la seguridad jurídica. Además, el uso limitado de los mecanismos de cooperación internacional restringe la capacidad del país para investigar delitos transnacionales, especialmente cuando la evidencia reside en servidores extranjeros.
- El déficit de infraestructura forense y de talento especializado constituye el obstáculo más crítico: sin laboratorios equipados, herramientas verificadas ni programas de formación continua, ningún marco legal puede garantizar la validez de la prueba digital. Superar estas limitaciones exige una estrategia integral que combine actualización legislativa, inversión tecnológica, cooperación internacional y profesionalización sostenida de todos los actores del sistema judicial.

En síntesis, aunque la legislación ecuatoriana está alineada con los estándares internacionales, su efectividad depende de la capacidad institucional para aplicarla. Solo mediante la estandarización interinstitucional, la formación especializada y el fortalecimiento técnico será posible traducir la solidez legal en resultados tangibles en la investigación y persecución penal del cibercrimen.

Referencias

1. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. Research Journal for Social Affairs, 3(5), 795–805. https://doi.org/10.71317/RJSA.003.05.0375

2. Alcoceba Gil, J. M. (2018). Los estándares de cientificidad como criterio de admisibilidad de la prueba científica. Revista Brasileira de Direito Processual Penal, 4(1), 215. https://doi.org/10.22197/rbdpp.v4i1.120

3. Alfosail, M., & Norris, P. (2021). Tor forensics: Proposed workflow for client memory artefacts. Computers & Security, 106, 102311. https://doi.org/10.1016/j.cose.2021.102311

4. AlKhanafseh, M., & Surakhi, O. (2024). Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. Electronics, 13(18), 3729. https://doi.org/10.3390/electronics13183729

5. Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal [Registro Oficial Suplemento No. 180].

6. Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales (No. Registro Oficial Suplemento No. 459). https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

7. Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (2020). Reporte de Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://doi.org/10.18235/0002513

8. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

9. Brunty, J. (2023). Validation of forensic tools and methods: A primer for the digital forensics examiner. WIREs Forensic Science, 5(2), e1474. https://doi.org/10.1002/wfs2.1474

10. Cabezas, D., Lucas, G., Arcos-Argudo, M., Bojorque, R., Plaza-Cordero, A., & Morquecho-Yunga, P. (2024). Comparative Analysis of Data Protection Laws in Ecuador and Spain: Similarities, Differences, and Implications. En X.-S. Yang, S. Sherratt, N. Dey, & A. Joshi (Eds.), Proceedings of Ninth International Congress on Information and Communication Technology (pp. 385–393). Springer Nature Singapore.

11. Casino, F., Dasaklis, T., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2021). Research trends, challenges, and emerging topics of digital forensics: A review of reviews. arXiv. https://doi.org/10.48550/ARXIV.2108.04634

12. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

13. Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (No. ETS núm. 185). https://rm.coe.int/16802fa403

14. Council of Europe. (2024, diciembre 12). Convention on Cybercrime: Ecuador becomes the 77th Party and Peru signs the Second Protocol on electronic evidence [T-CY News]. Cybercrime. https://www.coe.int/en/web/cybercrime/-/convention-on-cybercrime-ecuador-becomes-the-77th-party-and-peru-signs-the-second-protocol-on-electronic-evidence

15. D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. Healthcare, 11(5), 634. https://doi.org/10.3390/healthcare11050634

16. Diao, H., Vergara Cobos, E. B., & Andrés, L. A. (2024). Cybersecurity Economics for Latin America and the Caribbean. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P179481-5515e6c4-1d69-444d-a057-741edce07402.pdf

17. Díaz-Pérez, L. C., Quintanar-Reséndiz, A. L., Vázquez-Álvarez, G., & Vázquez-Medina, R. (2022). A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology. Applied Computing and Informatics. https://doi.org/10.1108/ACI-01-2022-0010

18. Douglas, D. M. (2016). Doxing: A conceptual analysis. Ethics and Information Technology, 18(3), 199–210. https://doi.org/10.1007/s10676-016-9406-0

19. Forni, P., & De Grande, P. (2020). Triangulación y métodos mixtos en las ciencias sociales contemporáneas. Revista Mexicana de Sociología, 82(1). https://doi.org/10.22201/iis.01882503p.2020.1.58064

20. International Organization for Standardization & International Electrotechnical Commission. (2012). ISO/IEC 27037:2012 Information technology—Security techniques—

Guidelines for identification, collection, acquisition, and preservation of digital evidence (Norma Estandar No. ISO/IEC 27037:2012(E)).

21. International Organization for Standardization & International Electrotechnical Commission. (2015a). ISO/IEC 27041:2015 Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigative method (Norma Estandar No. ISO/IEC 27041:2015(E)).

22. International Organization for Standardization, & International Electrotechnical Commission. (2015b). ISO/IEC 27042:2015 Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence (Norma Estandar No. ISO/IEC 27042:2015(E)).

23. Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLOS ONE, 20(9), 1–26. https://doi.org/10.1371/journal.pone.0331683

24. Jinad, R., Gupta, K., Simsek, E., & Zhou, B. (2024). Bias and fairness in software and automation tools in digital forensics. Journal of Surveillance, Security and Safety, 5(1). https://doi.org/10.20517/jsss.2023.41

25. Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Science International, 362, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

26. Lee, S.-H., Kang, I., & Kim, H.-W. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? Technology in Society, 75, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

27. Lim, M. C. E., Chen, B. H. C., Lim, L. Y., Shanbagamaran, T., Lim, D. Y. J., Hlaing, N. W., & Rafsanjani, A. S. (2025). Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation. Journal of Informatics and Web Engineering, 4(2), 158–181. https://doi.org/10.33093/jiwe.2025.4.2.11

28. Ludeña, L., Díaz Silva, H. A., & Calixto Velásquez, D. F. (2025). Manejo de la evidencia digital en la investigación del delito de pornografía infantil. Revista Escpogra PNP, 4(2), 205–220. https://doi.org/10.59956/escpograpnpv4n2.14

29. Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors, 24(2), 433. https://doi.org/10.3390/s24020433

30. Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample Size in Qualitative Interview Studies: Guided by Information Power. Qualitative Health Research, 26(13), 1753–1760. https://doi.org/10.1177/1049732315617444

31. Obando-Peralta, E. C. (2025). Métodos de investigación jurídica: Análisis de su diversidad y fundamentos epistemológicos. https://doi.org/10.5281/ZENODO.14927514

32. Parra, J. D. (2019). El arte del muestreo cualitativo y su importancia para la evaluación y la investigación de políticas públicas: Una aproximación realista. OPERA, 25, 119–136. https://doi.org/10.18601/16578651.n25.07

33. Paspuel Hernández, J. E. P., Panchi Criollo, C. A. P., Paredes Mera, J. S., & Suquitana Segura, M. W. (2024). Organized Crime And Cybercrime In Ecuador: A New Reality Of Complex Criminality. Migration Letters, 21(S10), 734–747. https://doi.org/10.59670/ml.v21iS11.10561

34. Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

35. Presidencia de la República del Ecuador. (2023). Reglamento General de la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904). https://spdp.gob.ec/wp-content/uploads/2024/12/04.pdf.pdf

36. Reedy, P. (2023). Interpol review of digital evidence for 2019-2022. Forensic Science International. Synergy, 6, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

37. Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). The protection of personal data in Ecuador: A historical-normative review of this fundamental right in the South American country. VISUAL REVIEW. International Visual Culture Review / Revista Internacional de Cultura Visual, 13(2), 1–16. https://doi.org/10.37467/revvisual.v10.4568

38. Santi, M. F. (2016). Controversias éticas en torno a la privacidad, la confidencialidad y el anonimato en investigación social. Revista de Bioética y Derecho, 0(37), 5–21. https://doi.org/10.1344/rbd2016.37.16147

39. Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses. (2025). Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital (Manual No. CSEIIMLCF-MLCF-MAN-2025-002).

40. Sosa González, W. E., Santillán Fernández, A., Canto de Gante, G., Bautista-Ortega, J., & Escobar Castillo, J. (2020). Escala de Likert: Una alternativa para elaborar e interpretar un instrumento de percepción social. Revista de Alta Tecnología y Sociedad, 12.

41. Thakar, A. A., Kumar, K., & Patel, B. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM)—Enhanced, Time Reducing and Comprehensive Framework. Journal of Physics: Conference Series, 1767(1), 012054. https://doi.org/10.1088/1742-6596/1767/1/012054

42. Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. BMC Medical Research Methodology, 18(1), 148. https://doi.org/10.1186/s12874-018-0594-7

43. Wilkes, N., Anderson, V. R., Johnson, C. L., & Bedell, L. M. (2022). Mixed Methods Research in Criminology and Criminal Justice: A Systematic Review. American Journal of Criminal Justice, 47(3), 526–546. https://doi.org/10.1007/s12103-020-09593-7

44. Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. The International Journal of Evidence & Proof, 28(1), 21–44. https://doi.org/10.1177/13657127231187059