Verdad y Derecho
Revista Arbitrada de Ciencias Jurídicas y Sociales
Vol. 5(especial6), 494-508, 2026
https://doi.org/10.62574/6q1rjcss

La evolución del ciberdelito en el ciberespacio: análisis jurídico y tecnológico del fenómeno delictivo digital en Ecuador

The evolution of cybercrime in cyberspace: A legal and technological analysis of the digital criminal phenomenon in Ecuador

Ariana Belen Mora-Troya
arianabmt16@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ecuador
https://orcid.org/0000-0002-3051-290X

Ignacio Fernando Barcos-Arias
ub.ignaciobarcos@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ecuador
https://orcid.org/0000-0002-9493-7931

Josselyn Briggitte Vilela-Verdezoto
ub.josselynvv41@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ecuador
https://orcid.org/0009-0005-2557-7150

RESUMEN

La expansión del ciberespacio ha transformado la criminalidad: conductas tradicionales como el fraude, la extorsión o el abuso sexual se cometen ahora por medios digitales, y han surgido delitos que solo pueden existir en entornos informáticos. El estudio analizó la evolución del ciberdelito y la respuesta del ordenamiento jurídico ecuatoriano desde una perspectiva jurídica y tecnológica. Se empleó un enfoque cualitativo, de alcance descriptivo-analítico, mediante análisis documental jurídico de la Constitución, el Código Orgánico Integral Penal, la Ley Orgánica de Protección de Datos Personales, la Ley de Comercio Electrónico, el Convenio de Budapest y doctrina indexada. Los resultados muestran que el Código Orgánico Integral Penal tipifica las principales categorías de ciberdelitos, pero que persisten problemas en la obtención y valoración de la prueba digital, en la cooperación internacional y en la adaptación a nuevas modalidades. Se concluye que la respuesta exige actualización normativa, capacidades forenses y coordinación internacional.

Descriptores: delito informático; ciberespacio; seguridad informática; derecho penal; protección de datos. (Fuente: Tesauro UNESCO).

ABSTRACT

The expansion of cyberspace has transformed crime: traditional conducts such as fraud, extortion or sexual abuse are now committed through digital means, and offences have emerged that can only exist in computer environments. The study analysed the evolution of cybercrime and the response of the Ecuadorian legal system from a legal and technological perspective. A qualitative, descriptive-analytical approach was used, through legal documentary analysis of the Constitution, the Comprehensive Organic Criminal Code, the Organic Law on Personal Data Protection, the Electronic Commerce Law, the Budapest Convention and indexed doctrine. The results show that the Comprehensive Organic Criminal Code typifies the main categories of cybercrime, but problems persist in obtaining and assessing digital evidence, in international cooperation and in adapting to new modalities. It is concluded that the response requires regulatory updating, forensic capabilities and international coordination.

Descriptors: computer crime; cyberspace; computer security; criminal law; data protection. (Source: UNESCO Thesaurus).

Recibido: 15/09/2026. Revisado: 05/10/2026. Aprobado: 30/10/2026. Publicado: 20/11/2026.
Sección artículos de investigación

INTRODUCCIÓN

El ciberespacio se ha convertido en un ámbito central de la vida social, económica y política. En él se realizan transacciones financieras, se almacenan datos personales, se prestan servicios públicos y se establecen relaciones personales. Esa expansión ha traído consigo una transformación de la criminalidad: muchas conductas delictivas tradicionales se cometen ahora a través de medios digitales y, al mismo tiempo, han aparecido formas de delincuencia que solo pueden existir en entornos informáticos. Gamón (2017) describe internet como la nueva era del delito y vincula en un mismo campo el ciberdelito, el ciberterrorismo, la legislación y la ciberseguridad.

Las modalidades de ciberdelincuencia son diversas y cambian con rapidez. Domínguez Arteaga y Vázquez (2022) estudian el ciberfraude al comercio electrónico, Macías-Lara et al. (2024) y Moreno-Arvelo et al. (2022) se ocupan de la suplantación de identidad en redes sociales y en entornos digitales, y Cevallos-Pachacama (2024) analiza el lavado de activos a través de monedas virtuales. A ello se suman los riesgos que enfrentan los niños y adolescentes en internet, como el contacto con fines sexuales, que Sani et al. (2021) examinan a partir de la percepción de los padres sobre el grooming.

En Ecuador, el Código Orgánico Integral Penal incorporó en 2014 un conjunto de tipos penales referidos a sistemas informáticos, datos y medios electrónicos (Asamblea Nacional, 2014), y la Ley Orgánica de Protección de Datos Personales reforzó en 2021 el marco de protección de la información (Asamblea Nacional, 2021). Sin embargo, la doctrina nacional ha advertido problemas en la persecución de estos delitos, especialmente en la prueba digital. Saca-Condo et al. (2023) sostienen, desde su propio título, que la

prueba digital resulta inviable por falta de regulación en los delitos informáticos, y Echeverría-Espinoza y Álvarez-Vera (2024) revisan las técnicas y herramientas forenses para su investigación en el país.

Frente a ese panorama, resulta pertinente un análisis que relacione la evolución tecnológica del ciberdelito con la respuesta normativa ecuatoriana. El objetivo de este estudio fue analizar la evolución del ciberdelito en el contexto del ciberespacio desde una perspectiva jurídica y tecnológica, identificando las categorías de conductas tipificadas en Ecuador, los instrumentos normativos aplicables y los principales desafíos para su persecución.

MARCO REFERENCIAL TEÓRICO

Ciberespacio y transformación del delito

El ciberespacio presenta rasgos que alteran las categorías clásicas del derecho penal. La conducta puede realizarse a distancia, sin contacto físico entre autor y víctima; sus efectos pueden producirse simultáneamente en varios países; la identidad del autor puede ocultarse mediante herramientas de anonimización; y la evidencia es volátil, porque los datos pueden modificarse o eliminarse con facilidad. Gamón (2017) sitúa estas características en la base de la expansión del ciberdelito y de la necesidad de políticas de ciberseguridad.

La doctrina suele distinguir entre los delitos informáticos en sentido estricto, cuyo objeto es el propio sistema o los datos, como el acceso no autorizado o el daño informático, y los delitos cometidos por medios informáticos, en los que la tecnología es el instrumento de una conducta tradicional, como el fraude, la extorsión o el abuso sexual. La suplantación de identidad digital

(Moreno-Arvelo et al., 2022; Macías-Lara et al., 2024) y el ciberfraude (Domínguez Arteaga y Vázquez, 2022) pertenecen a esta segunda categoría y muestran cómo una misma conducta adquiere nuevas dimensiones al trasladarse al entorno digital.

La evolución tecnológica introduce, además, nuevas herramientas tanto para la comisión como para la prevención de delitos. Becerril-Gil (2021) analiza los retos de la regulación jurídica de la inteligencia artificial en el ámbito de la ciberseguridad, y Cevallos-Pachacama (2024) muestra que las monedas virtuales ofrecen nuevos canales para el lavado de activos. Lobo (2023), por su parte, examina la protección de los menores en internet y en las redes sociales, ámbito en el que la vulnerabilidad de la víctima agrava el impacto de la conducta.

La prueba digital

La persecución del ciberdelito depende de la capacidad de obtener, preservar y valorar la evidencia digital. González Reyes (2021) estudia la relación entre la prueba digital y la cadena de custodia, que garantiza la integridad y autenticidad de la evidencia desde su obtención hasta su presentación en juicio. Imaicela Revilla y Alvarado Ajila (2024) analizan la incorporación de la prueba digital en el derecho procesal ecuatoriano, y Echeverría-Espinoza y Álvarez-Vera (2024) revisan las técnicas y herramientas forenses disponibles para investigar estos delitos.

Marco normativo nacional e internacional

La Constitución reconoce el derecho de acceso universal a las tecnologías de información y comunicación (Asamblea Nacional Constituyente, 2008, art. 16, num. 2), el derecho a la protección de datos de carácter personal (art. 66, num. 19), a la intimidad personal y familiar (art. 66, num. 20) y a la

inviolabilidad y al secreto de la correspondencia física y virtual (art. 66, num. 21), así como la garantía de hábeas data (art. 92). La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce a los mensajes de datos igual valor jurídico que los documentos escritos (Congreso Nacional, 2002, art. 2), y la Ley Orgánica de Protección de Datos Personales regula el tratamiento de datos y las obligaciones de seguridad de quienes los tratan (Asamblea Nacional, 2021).

En el plano penal, el Código Orgánico Integral Penal tipifica, entre otras conductas, la violación a la intimidad (Asamblea Nacional, 2014, art. 178), la apropiación fraudulenta por medios electrónicos (art. 190), la revelación ilegal de bases de datos (art. 229), la interceptación ilegal de datos (art. 230), la transferencia electrónica de activo patrimonial (art. 231), el ataque a la integridad de sistemas informáticos (art. 232), los delitos contra la información pública reservada (art. 233) y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234). Tipifica también el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos (art. 173) y la oferta de servicios sexuales con menores por medios electrónicos (art. 174). En el ámbito internacional, el Convenio sobre la Ciberdelincuencia del Consejo de Europa (2001) constituye el principal instrumento de armonización en materia de tipificación, de medidas procesales y de cooperación internacional.

MÉTODO

La investigación tuvo un enfoque cualitativo y un alcance descriptivo-analítico, y se desarrolló mediante análisis documental jurídico complementado con una lectura de la dimensión tecnológica del fenómeno a partir de la doctrina especializada. No se realizaron entrevistas, encuestas

ni análisis de expedientes judiciales, ni se emplearon estadísticas de denuncias.

El corpus se integró por la Constitución de la República (Asamblea Nacional Constituyente, 2008), el Código Orgánico Integral Penal (Asamblea Nacional, 2014), la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021), la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Congreso Nacional, 2002) y el Convenio sobre la Ciberdelincuencia (Consejo de Europa, 2001), junto con artículos de revistas académicas y libros sobre ciberdelito, ciberseguridad, suplantación de identidad, fraude electrónico, prueba digital y protección de menores en internet.

Se seleccionaron las normas vigentes que regulan directamente las conductas delictivas cometidas en o contra sistemas informáticos y la doctrina publicada en fuentes académicas identificables, preferentemente entre 2015 y 2025. Se excluyeron tesis, blogs, páginas web y literatura gris.

Se aplicó el análisis exegético a los tipos penales y a las normas de protección de datos; el análisis sistemático, para relacionar esas disposiciones con los derechos constitucionales y con las reglas sobre prueba digital; y el análisis comparado, para contrastar la tipificación ecuatoriana con las categorías del Convenio de Budapest. Entre las limitaciones se cuentan la rápida evolución tecnológica, que puede dejar desactualizado cualquier análisis, y el hecho de que la doctrina se utilizó en la medida en que su objeto declarado respalda las afirmaciones realizadas.

RESULTADOS

Evolución del fenómeno: de la intrusión a la afectación directa de las personas

El primer resultado es que el ciberdelito ha evolucionado desde conductas centradas en el sistema informático hacia conductas centradas en las personas y en el patrimonio. En una primera etapa, la preocupación principal era el acceso no autorizado y el daño a sistemas; posteriormente, el fraude electrónico y la apropiación de datos financieros adquirieron protagonismo; y, en la etapa actual, la masificación de las redes sociales y de los pagos digitales ha desplazado el foco hacia la suplantación de identidad, la extorsión y los delitos sexuales contra menores. Gamón (2017) ya advertía la articulación entre ciberdelito y ciberterrorismo, y la literatura posterior sobre suplantación de identidad (Moreno-Arvelo et al., 2022; Macías-Lara et al., 2024) y ciberfraude (Domínguez Arteaga y Vázquez, 2022) confirma el desplazamiento hacia conductas que afectan directamente a los usuarios.

Un segundo rasgo de esa evolución es la incorporación de tecnologías emergentes. Las monedas virtuales facilitan el movimiento de fondos ilícitos (Cevallos-Pachacama, 2024), y la inteligencia artificial plantea retos regulatorios en materia de ciberseguridad (Becerril-Gil, 2021). Estos desarrollos muestran que la criminalidad digital no es estática, sino que se adapta a cada innovación tecnológica, lo que obliga al derecho a revisar periódicamente sus categorías.

La respuesta del Código Orgánico Integral Penal

El segundo resultado es que el Código Orgánico Integral Penal cubre las principales categorías de ciberdelitos que identifica el Convenio de

Budapest. Los delitos contra la confidencialidad, integridad y disponibilidad de los sistemas y datos se corresponden con el acceso no consentido, la interceptación ilegal y el ataque a la integridad de sistemas informáticos (Asamblea Nacional, 2014, arts. 230, 232 y 234); los delitos informáticos de carácter patrimonial, con la apropiación fraudulenta por medios electrónicos y la transferencia electrónica de activo patrimonial (arts. 190 y 231); y los delitos relacionados con el contenido, con los tipos que protegen a los menores frente a los medios electrónicos (arts. 173 y 174). La Tabla 1 sintetiza esta correspondencia.

Tabla 1. *Tipificación del ciberdelito en el Código Orgánico Integral Penal y categorías del Convenio de Budapest.*

Norma o fuente	Disposición	Alcance	Problema identificado
COIP (2014)	Art. 234: acceso no consentido a un sistema informático	Protege la confidencialidad del sistema	Dificultad para identificar al autor que actúa desde el extranjero
COIP (2014)	Arts. 230 y 232: interceptación ilegal y ataque a la integridad de sistemas	Protegen la integridad y disponibilidad de datos y sistemas	Volatilidad de la evidencia y necesidad de pericia especializada
COIP (2014)	Arts. 190 y 231: apropiación fraudulenta y transferencia electrónica	Protegen el patrimonio frente al fraude electrónico	Rastreo de fondos en plataformas y monedas virtuales
COIP (2014)	Arts. 178 y 229: violación a la intimidad y revelación de bases de datos	Protegen la intimidad y los datos personales	Concurrencia con el régimen administrativo de protección de datos
COIP (2014)	Arts. 173 y 174: contacto y oferta sexual con menores por medios electrónicos	Protegen la indemnidad sexual de menores	Detección tardía y subregistro
Convenio de Budapest (2001)	Tipificación, medidas procesales y cooperación	Armonización internacional	Requiere adecuación procesal y cooperación efectiva

Nota. Elaboración propia (2026) a partir de Asamblea Nacional (2014) y Consejo de Europa (2001).

La suplantación de identidad digital constituye, sin embargo, un ámbito en el que la cobertura es menos clara. Cuando la suplantación es un medio para obtener un beneficio patrimonial, puede encuadrarse en los tipos de fraude; pero cuando se utiliza para dañar la reputación o acosar a la víctima, su encuadre depende de la concurrencia de otros tipos, lo que genera incertidumbre. Moreno-Arvelo et al. (2022) proponen, en ese sentido, una regulación global para evitar la suplantación de identidad digital.

La protección de los datos personales muestra, por su parte, una doble vía de respuesta. La revelación ilegal de bases de datos y la violación a la intimidad son delitos (Asamblea Nacional, 2014, arts. 178 y 229), mientras que la Ley Orgánica de Protección de Datos Personales impone a los responsables y encargados del tratamiento deberes de seguridad y establece un régimen administrativo propio (Asamblea Nacional, 2021). Esta concurrencia es positiva, porque permite combinar la prevención administrativa con la sanción penal de las conductas más graves, pero exige criterios claros para distinguir cuándo una brecha de seguridad constituye una infracción administrativa y cuándo una conducta penalmente relevante. La Constitución ofrece el fundamento común de ambas vías, al reconocer la protección de datos personales como un derecho autónomo (Asamblea Nacional Constituyente, 2008, art. 66, num. 19) y garantizar su tutela mediante el hábeas data (art. 92).

Desafíos probatorios y de cooperación

El tercer resultado se refiere a la prueba. La validez jurídica de los mensajes de datos está reconocida (Congreso Nacional, 2002, art. 2), y el Código Orgánico Integral Penal contiene reglas sobre el contenido digital (Asamblea Nacional, 2014, art. 500). No obstante, Saca-Condo et al. (2023) consideran

que la falta de regulación específica compromete la viabilidad de la prueba digital en los delitos informáticos, e Imaicela Revilla y Alvarado Ajila (2024) analizan las dificultades de su incorporación en el proceso. La cadena de custodia, cuyo vínculo con la prueba digital estudia González Reyes (2021), y las técnicas forenses que revisan Echeverría-Espinoza y Álvarez-Vera (2024) son, por tanto, condiciones indispensables para que los tipos penales sean eficaces.

El cuarto resultado es que la dimensión transnacional del ciberdelito exige cooperación internacional. El Convenio de Budapest (Consejo de Europa, 2001) prevé mecanismos de conservación rápida de datos y asistencia mutua, y su lógica muestra que la persecución eficaz depende de la capacidad de obtener datos alojados en servidores extranjeros. La Tabla 2 resume los desafíos identificados.

Tabla 2. *Desafíos jurídicos y tecnológicos en la persecución del ciberdelito en Ecuador.*

Desafío	Dimensión tecnológica	Dimensión jurídica	Línea de respuesta
Prueba digital	Volatilidad y facilidad de alteración de los datos	Regulación procesal insuficiente (Saca-Condo et al., 2023)	Protocolos de cadena de custodia digital y peritos certificados
Identificación del autor	Anonimización y uso de servidores extranjeros	Límites de la jurisdicción territorial	Cooperación internacional y conservación rápida de datos
Nuevas modalidades	Monedas virtuales e inteligencia artificial	Tipos penales diseñados para tecnologías anteriores	Revisión periódica de la tipificación
Suplantación de identidad	Creación de perfiles falsos en redes sociales	Encuadre típico incierto fuera del fraude	Regulación específica (Moreno-Arvelo et al., 2022)
Protección de datos	Brechas de seguridad en bases de datos	Concurrencia entre la vía penal y la administrativa	Coordinación entre la autoridad de datos y la Fiscalía

Nota. Elaboración propia (2026) a partir de Asamblea Nacional (2014, 2021), Consejo de Europa (2001) y de la doctrina citada.

DISCUSIÓN

Los resultados muestran que el ordenamiento ecuatoriano ha incorporado una tipificación amplia del ciberdelito, que se corresponde en lo esencial con las categorías del Convenio de Budapest. Esta constatación matiza la percepción de que el problema del ciberdelito en Ecuador sea, ante todo, una ausencia de tipos penales. Los problemas más relevantes se sitúan en la aplicación: en la obtención y preservación de la prueba, en la identificación de los autores y en la adaptación de la tipificación a las nuevas modalidades.

La cuestión probatoria es central. La afirmación de Saca-Condo et al. (2023) sobre la inviabilidad de la prueba digital por falta de regulación debe leerse junto con la existencia de reglas generales sobre el contenido digital y sobre el valor jurídico de los mensajes de datos. Lo que se advierte no es tanto una ausencia total de normas como la falta de protocolos técnicos detallados, de peritos especializados y de estándares uniformes de cadena de custodia. González Reyes (2021) e Imaicela Revilla y Alvarado Ajila (2024) coinciden en que la prueba digital requiere garantías específicas de autenticidad e integridad, y Echeverría-Espinoza y Álvarez-Vera (2024) muestran que las herramientas forenses disponibles deben acompañarse de un marco legal que asegure su admisibilidad.

La evolución tecnológica plantea, por su parte, un desafío de técnica legislativa. Los tipos penales redactados en términos excesivamente técnicos corren el riesgo de quedar obsoletos, mientras que los tipos demasiado abiertos pueden vulnerar el principio de legalidad. La experiencia de las monedas virtuales (Cevallos-Pachacama, 2024) y de la inteligencia artificial (Becerril-Gil, 2021) sugiere que la tipificación debe

centrarse en el resultado lesivo y en el bien jurídico afectado, antes que en la tecnología empleada. Este enfoque, tecnológicamente neutral, permitiría que los tipos penales sigan siendo aplicables cuando cambien las herramientas.

La protección de los menores merece una atención particular. Lobo (2023) y Sani et al. (2021) muestran que los riesgos de internet y de las redes sociales para niños y adolescentes, como el grooming, requieren respuestas que combinen la sanción penal con la educación digital de los menores y de sus familias. Los tipos de contacto con finalidad sexual y de oferta de servicios sexuales con menores por medios electrónicos (Asamblea Nacional, 2014, arts. 173 y 174) ofrecen una base adecuada, pero su eficacia depende de la detección temprana, que exige la participación de las familias, de las escuelas y de las plataformas digitales.

Finalmente, la dimensión transnacional confirma la importancia de la cooperación internacional. Gamón (2017) vincula el ciberdelito con la legislación y la ciberseguridad, y el Convenio de Budapest (Consejo de Europa, 2001) ofrece un marco de referencia para la armonización y la asistencia mutua. La protección de datos personales (Asamblea Nacional, 2021) complementa la respuesta penal al imponer deberes de seguridad a quienes tratan información, lo que contribuye a la prevención. La limitación principal del estudio es su carácter documental, que no permite valorar la eficacia práctica de la persecución penal, aspecto que deberían abordar investigaciones empíricas posteriores.

CONCLUSIONES

El ciberdelito ha evolucionado desde conductas dirigidas contra los sistemas informáticos hacia conductas que afectan directamente a las

personas, a su patrimonio, a su identidad y a su intimidad, y se adapta continuamente a nuevas tecnologías como las monedas virtuales y la inteligencia artificial. El Código Orgánico Integral Penal tipifica las principales categorías de ciberdelitos, en una línea coherente con el Convenio de Budapest.

Los principales problemas del ordenamiento ecuatoriano no se sitúan en la ausencia de tipos penales, sino en la obtención, preservación y valoración de la prueba digital, en la identificación de autores que operan desde el extranjero, en la incertidumbre sobre el encuadre de la suplantación de identidad cuando no persigue un fin patrimonial y en la necesidad de actualizar la tipificación ante nuevas modalidades.

La respuesta al ciberdelito exige protocolos técnicos de cadena de custodia digital, capacidades forenses especializadas, una técnica legislativa tecnológicamente neutral, mecanismos de cooperación internacional y una articulación entre la vía penal y la protección de datos personales. La educación digital, especialmente de niños, adolescentes y familias, constituye un complemento indispensable de la respuesta jurídica.

FINANCIAMIENTO

No monetario.

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A UNIANDES.

REFERENCIAS

Asamblea Nacional. (2014). Código Orgánico Integral Penal [Comprehensive Organic Criminal Code]. Registro Oficial Suplemento 180, 10 de febrero de 2014.

Asamblea Nacional. (2021). Ley Orgánica de Protección de Datos Personales [Organic Law on Personal Data Protection]. Registro Oficial Suplemento 459 de 26 de mayo de 2021.

Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial N.° 449 de 20 de octubre de 2008. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Becerril-Gil, Anahiby Anyel. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. Revista IUS, 15(48), 9-34. Epub 14 de marzo de 2022. https://doi.org/10.35487/rius.v15i48.2021.705

Cevallos-Pachacama, I. A. (2024). Lavado de activos a través de monedas virtuales, una perspectiva jurídica y académica. MENTOR Revista De investigación Educativa Y Deportiva, 3(8), 651–699. https://doi.org/10.56200/mried.v3i8.8016

Congreso Nacional. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos [Law on Electronic Commerce, Electronic Signatures and Data Messages]. Registro Oficial Suplemento 557, 17 de abril de 2002.

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (Serie de Tratados Europeos n.º 185) [Convention on Cybercrime]. Budapest, 23 de noviembre de 2001.

Domínguez Arteaga, Rosa Amelia, & Vázquez, Rodrigo Vera. (2022). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. Podium, (41), 21-40. Epub 30 de junio de 2022.https://doi.org/10.31095/podium.2022.41.2

Echeverría-Espinoza, E., & Álvarez-Vera, M. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador: Una revisión sistemática. 593 Digital Publisher CEIT, 9(6), 644-652. https://doi.org/10.33386/593dp.2024.6.2775

Gamón, Vicente Pons. (2017). Internet, la nueva era del delito: ciberdelito,ciberterrorismo,legislación y ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

González Reyes, J. (2021). La prueba digital y la cadena de custodia [Digital evidence and the chain of custody]. Anales de la Facultad de Derecho (Universidad de La Laguna), (38).

Imaicela Revilla, J. A., & Alvarado Ajila, L. A. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano [The incorporation of digital evidence in Ecuadorian procedural law]. Revista Lex, 7(27), 1338-1350. https://doi.org/10.33996/revistalex.v7i27.247

Lobo, J. M. R. (2023). La protección de los menores en internet y redes sociales [The protection of minors on the internet and social networks]. En J. H. C. Suntura & V. S. Ortega (Eds.), La protección del menor: Un análisis desde las ciencias jurídicas [The protection of minors: An analysis from legal sciences] (1.ª ed., pp. 237–254). J.M Bosch. https://doi.org/10.2307/jj.11786252.14

Macías-Lara, R. A., Bedoya-Benavides, J. O., Manchay-Orbea, J. C., Nazareno-Vivero, G., & Mina Angulo, R. M. (2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales.: Innovative strategies to mitigate identity theft on social networks. Revista Científica Multidisciplinar G-Nerando, 5(1), 544–561. https://doi.org/10.60100/rcmg.v5i1.212

Moreno-Arvelo, Pamilys Milagros, Paucar-Paucar, Cesar Elías, & Cajas-Parraga, Cinthia Mariela. (2022). Regulación global para evitar la suplantación de identidad digital. Revista Universidad y Sociedad, 14(6), 690-696.

Saca-Condo, H., Marquez-Barreto, A., & Arciniegas-Castro, C. (2023). La inviabilidad de la prueba digital por falta de regulación en los delitos informáticos [The unfeasibility of digital evidence due to lack of regulation in computer crimes]. 593 Digital Publisher CEIT, 8(4), 21-34. https://doi.org/10.33386/593dp.2023.4.1887

Sani, Ana Isabel, Vieira, Ana Paula, & Dinis, Maria Alzira Pimenta. (2021). Social Networks, the Internet, and risks: Portuguese parents' perception of online grooming. Avaliação Psicológica, 20(4), 486-494. https://doi.org/10.15689/ap.2021.2004.22001.10

Derechos de autor: 2026 Por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0)
https://creativecommons.org/licenses/by-nc-sa/4.0/