

ANALYSIS OF THE RATIFICATION OF THE BUDAPEST CONVENTION AND ITS IMPACT ON CYBERCRIMES IN ECUADORJostin Sebastián Iñiguez-Narváez¹**E-mail:** dt.jostinsin20@uniandes.edu.ec**ORCID:** <https://orcid.org/0009-0004-9102-9040>Carmen Marina Méndez-Cabrita¹**E-mail:** ut.carmenmme56@uniandes.edu.ec**ORCID:** <https://orcid.org/0000-0001-8672-3450>Johana Lisbeth Mafla-Sánchez¹**E-mail:** dt.johanalms64@uniandes.edu.ec**ORCID:** <https://orcid.org/0000-0003-4390-1848>Jairo Mauricio Puetate-Paucar¹**E-mail:** ut.jairopuetate@uniandes.edu.ec**ORCID:** <https://orcid.org/0000-0003-2784-0141>¹ Universidad Regional Autónoma de los Andes. Ecuador.**Cita sugerida (APA, séptima edición)**

Iñiguez-Narváez, J. S., Méndez-Cabrita, C. M., Mafla-Sánchez, J. L., & Puetate-Paucar, J. M. (2025). Análisis de ratificación del Convenio de Budapest y su impacto en delitos informáticos en Ecuador. *Revista UGC*, 3(3), 16-21.

Fecha de presentación: 06/05/2025**Fecha de aceptación:** 12/07/2025**Fecha de publicación:** 01/09/2025**RESUMEN**

Los delitos informáticos representan una amenaza creciente en el ámbito global, y Ecuador no es la excepción, enfrentando un aumento en fraudes electrónicos, ataques cibernéticos y robo de identidad. Este estudio tuvo como objetivo analizar las implicaciones y beneficios de la ratificación del Convenio de Budapest para la lucha contra los delitos informáticos en Ecuador. Se empleó una metodología cuantitativa, utilizando el método hipotético-deductivo, el Analítico-Sintético y el hermenéutico para evaluar el marco normativo ecuatoriano en relación con estándares internacionales. La investigación se enmarca en un enfoque socio-jurídico, dado que analiza la funcionalidad del derecho en la práctica, verificando la aplicabilidad del Convenio en el contexto ecuatoriano. Los resultados evidencian deficiencias en la legislación vigente y en la capacidad operativa de las instituciones judiciales y de seguridad para combatir la ciberdelincuencia. Se identificó que el 100% de los encuestados considera necesaria la ratificación del Convenio, y los expertos entrevistados coinciden en que su adopción permitiría fortalecer la cooperación internacional y mejorar las herramientas de investigación digital. No obstante, existen desafíos como la necesidad de reformas legislativas y la capacitación de los operadores de justicia. Se concluye que la ratificación del Convenio de Budapest es fundamental para modernizar el marco normativo ecuatoriano, mejorar la respuesta institucional y fortalecer la ciberseguridad, garantizando una lucha más efectiva contra los delitos informáticos en el país.

Palabras clave:

Ciberdelincuencia, seguridad digital, Convenio de Budapest, cooperación jurídica internacional, marco normativo ecuatoriano.

ABSTRACT

Cybercrimes represent a growing threat on a global scale, and Ecuador is no exception, facing an increase in electronic fraud, cyber-attacks, and identity theft. This study aimed to analyze the implications and benefits of ratifying the Budapest Convention on Cybercrime in Ecuador. A quantitative methodology was employed, using the hypothetical-deductive, Analytical-Synthetic, and hermeneutic methods to evaluate the Ecuadorian regulatory framework in relation to international standards. The research takes a socio-legal approach, analyzing the functionality of law in practice and verifying the applicability of the Convention in the Ecuadorian context. The results reveal deficiencies in the current legislation and the operational capacity of judicial and security institutions to combat cybercrime. It was found that 100% of respondents consider the ratification of the Convention necessary, and interviewed experts agree that its adoption would strengthen international cooperation and improve digital investigation tools. However, there are challenges such as the need for legislative reforms and the training of justice operators. It is concluded that the ratification of the Budapest Convention is essential to modernize the Ecuadorian regulatory framework, improve institutional response, and strengthen cybersecurity, ensuring a more effective fight against cybercrimes in the country.

Keywords:

Cybercrime, digital security, Budapest Convention, international legal cooperation, Ecuadorian legal framework.

INTRODUCCIÓN

En la era digital, los delitos informáticos una amenaza creciente para la seguridad y la economía global. Ecuador no es ajeno a esta problemática, enfrentando un incremento significativo en actividades delictivas cibernéticas como el fraude, el robo de identidad y los ataques a la infraestructura crítica. A nivel internacional, el Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 por el Consejo de Europa, se ha convertido en el principal tratado para enfrentar este tipo de delitos a través de la coordinación de las legislaciones nacionales, la mejora de las técnicas investigativas y la promoción de la cooperación internacional. Sin embargo, a pesar de la importancia de este convenio, Ecuador aún se encuentra en proceso de ratificación.

El Convenio de Budapest, conocido también como el Convenio sobre Ciberdelincuencia, es el primer tratado internacional que aborda los crímenes informáticos mediante la armonización de leyes nacionales, la mejora de técnicas de investigación y el aumento de la cooperación entre naciones. Este convenio ha sido ratificado por más de 56 países, incluyendo varias naciones no europeas, destacando su relevancia y alcance global (Linares, 2013).

El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como la única solución internacional existente para el tratamiento de la cuestión ciberdelictiva. A pesar de sus deficiencias, se convierte en una herramienta adecuada para la armonización legislativa interestatal y la lucha contra los ciberdelitos (Díaz Gómez, 2010).

En América Latina, la ratificación y adopción del Convenio de Budapest ha sido desigual. Países como Chile, Costa Rica y República Dominicana han avanzado en la implementación de sus y en la actualización de su legislación, mientras que otros, como Argentina, Brasil y México, aún no han completado el proceso de ratificación formal. Ecuador, aunque ha mostrado interés en fortalecer su marco legal y operativo para combatir los delitos informáticos, enfrenta desafíos específicos como limitaciones en recursos técnicos y humanos y marcos legislativos que necesitan actualización (Zambrano & Ordoñez, 2016).

Según Rodríguez (2020), *“Ecuador no se ha suscrito al Convenio de Budapest desde 2001, y los ciberdelitos transnacionales se investigan a través de asistencias penales. Esto es motivo de preocupación, ya que el país no cuenta con una ley específica para luchar contra los ciberdelitos. Por lo tanto, es crucial que Ecuador ratifique el convenio para facilitar el intercambio de información y sancionar la criminalidad informática entre los países miembros”*.

La delincuencia informática y su aumento se deben a varios factores, como la evolución de la tecnología y la falta de conocimiento sobre cómo protegerse de posibles ataques a través de las nuevas tecnologías. Esta falta de información y conocimiento permite a los delincuentes realizar

potenciales ataques con mayor facilidad. Se explorarán las razones detrás de la no ratificación del Convenio de Budapest por parte de Ecuador, las implicaciones de esta decisión para la lucha contra los delitos informáticos en el país, y cómo podría cambiar el panorama de la ciberseguridad en Ecuador al ratificar este convenio.

La situación plantea varias interrogantes clave: ¿Por qué se ha tardado tanto en ratificar un convenio tan importante contra la ciberdelincuencia? ¿Cuáles son las barreras legales y operativas que enfrenta Ecuador? ¿Qué pasos deben tomarse para alinear la legislación ecuatoriana con las normativas internacionales en materia de ciberseguridad?

La presente investigación pretende aportar un análisis detallado sobre la postura de Ecuador frente a la regulación internacional en materia de ciberdelincuencia y generar recomendaciones que contribuyan al fortalecimiento de su marco legal y operativo en la lucha contra los delitos informáticos.

MATERIALES Y MÉTODOS

Este estudio se enmarca dentro de una investigación de tipo cuantitativa, empleando la recolección y análisis de datos para responder preguntas de investigación y probar hipótesis formuladas previamente. La metodología utilizada permite examinar la relación entre variables, analizar tendencias y establecer inferencias sobre el impacto de la ratificación del Convenio de Budapest en la lucha contra los delitos informáticos en Ecuador.

Desde el nivel teórico, se han empleado diversos métodos de análisis jurídico. En primer lugar, se ha aplicado el método Hipotético-Deductivo, el cual establece un procedimiento de razonamiento lógico que busca explicar los problemas planteados mediante la formulación y contrastación de hipótesis. En este estudio, se analizan las implicaciones normativas y operativas de la ratificación del Convenio de Budapest, postulando su impacto positivo en la persecución y sanción de delitos informáticos.

Asimismo, se ha empleado el método Analítico-Sintético (Gómez et al., 2017), que permite descomponer los elementos del fenómeno estudiado en sus componentes fundamentales para luego integrarlos en una visión global. Este método ha sido útil para examinar las deficiencias normativas y operativas actuales en Ecuador, comparándolas con el marco jurídico internacional propuesto por el Convenio de Budapest.

Por otro lado, el método hermenéutico ha sido clave para interpretar la información obtenida de fuentes documentales, doctrinales y normativas. La hermenéutica jurídica facilita la comprensión de los principios del Convenio de Budapest y su aplicabilidad en el contexto ecuatoriano, consolidando elementos de juicio para explicar la vulnerabilidad del sistema legal frente a la ciberdelincuencia y proponer soluciones viables.

En cuanto a la tipología de la investigación, este estudio se sitúa predominantemente dentro del enfoque socio-jurídico, ya que examina la funcionalidad del Derecho en la realidad ecuatoriana y evalúa si las normas sobre ciberdelincuencia son eficaces en la práctica. Se basa en el análisis de la aplicación y cumplimiento del Derecho en el ámbito digital, considerando el marco normativo vigente y la percepción de expertos en el área. Como señala Tantaleán (2016), este tipo de investigación busca verificar la operatividad del Derecho en sede real, permitiendo discutir, criticar y reformular normativas según su impacto social.

No obstante, también incorpora elementos del enfoque dogmático-jurídico, dado que examina el ordenamiento normativo ecuatoriano y su compatibilidad con el Convenio de Budapest. Se analizan las disposiciones legales actuales desde una perspectiva doctrinal, con el fin de determinar su validez y coherencia en el marco internacional.

Si bien este estudio no se centra en una reconstrucción histórica del Derecho ni en un análisis filosófico profundo de sus fundamentos, sí reconoce que estos enfoques pueden complementar la comprensión del fenómeno en estudios posteriores. La investigación presente, al enfocarse en la funcionalidad y aplicación de la norma, prioriza el análisis práctico del impacto jurídico y social de la adhesión de Ecuador al Convenio de Budapest.

Finalmente, la combinación de estos métodos permite desarrollar un estudio integral que no solo identifica falencias normativas, sino que también evalúa la capacidad institucional del país para hacer frente a la ciberdelincuencia desde una perspectiva legal y operativa, apoyándose en la triangulación de datos (Okuda Benavides & Gómez-Restrepo, 2005). Este enfoque metodológico proporciona un análisis riguroso y aplicable para la formulación de políticas públicas en materia de seguridad digital.

El presente estudio ha analizado la ratificación del Convenio de Budapest y su impacto en la legislación ecuatoriana, resaltando sus beneficios y los principales desafíos que enfrenta el país. Para la recolección de datos, se han aplicado diversas técnicas metodológicas, como la encuesta (Feria Ávila et al., 2020), que ha permitido evaluar la percepción y conocimiento de la ciudadanía sobre la problemática de la ciberdelincuencia, y la entrevista estructurada, que ha facilitado la identificación de los factores determinantes que obstaculizan la ratificación del Convenio.

El proceso de recolección de datos se ha llevado a cabo siguiendo un enfoque de triangulación metodológica, como se visualiza en la Figura 1.

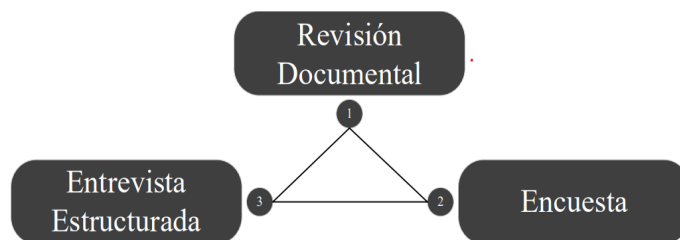


Figura 1. Triangulación de datos.

Asimismo, se ha empleado el Análisis de Contenido, a partir del cual se han establecido categorías de análisis que han permitido una descripción detallada del objeto de estudio.

RESULTADOS Y DISCUSIÓN

A continuación, se presentan los hallazgos obtenidos en función de dichas categorías.

- Categoría 1: Necesidad de ratificación del Convenio de Budapest

Los entrevistados han coincidido en que la ratificación del Convenio de Budapest es crucial para fortalecer el marco legal ecuatoriano en materia de ciberdelincuencia. Según el Dr. Landívar Alexander Escobar Cadena, “los convenios y tratados internacionales buscan erradicar delitos en materia penal que carecen de jurisprudencia internacional. La ratificación del Convenio de Budapest contribuiría a disminuir los delitos informáticos y el crimen organizado transnacional”.

Por su parte, el Dr. Juan Carlos Villareal Tapia enfatiza que “las normas deben ajustarse al desarrollo de la sociedad. Los delitos informáticos han evolucionado rápidamente, por lo que Ecuador necesita ratificar el Convenio para facilitar la cooperación internacional y mejorar su normativa nacional”.

En la misma línea, el Dr. Leonardo Ruales Reinoso considera que “el marco legal actual es insuficiente para enfrentar la creciente sofisticación de los delitos informáticos. La ratificación del Convenio de Budapest proporcionaría un marco legal robusto y actualizado”.

- Categoría 2: Beneficios de la ratificación

Uno de los principales beneficios identificados es la armonización legislativa, permitiendo una tipificación clara de los ciberdelitos. Como señala el Dr. Escobar Cadena, “actualmente Ecuador no cuenta con una ley específica para la tipificación de todos los ciberdelitos, ya que estos se encuentran dispersos en el Código Orgánico Integral Penal y la Ley de Comercio Electrónico. Con la ratificación, se podría incorporar un capítulo específico sobre ciberdelincuencia”.

Otro beneficio clave mencionado por los entrevistados es el acceso a capacitación y tecnología especializada para jueces, fiscales y fuerzas del orden. El Dr. Villareal Tapia

sostiene que “es fundamental proporcionar formación especializada y recursos tecnológicos avanzados, además de fomentar la cooperación interinstitucional”.

Finalmente, el Dr. Ruales Reinoso destaca que “la ratificación mejoraría la cooperación internacional y el acceso a herramientas especializadas para la investigación de estos delitos”.

- Categoría 3: Desafíos en la ratificación

Entre los principales desafíos identificados está la necesidad de reformas legislativas sustanciales. Según el Dr. Escobar Cadena, “el crimen organizado transnacional innova constantemente en técnicas delictivas, lo que exige una legislación flexible y actualizada. La Asamblea Nacional debe otorgarle la prioridad necesaria para su ratificación”.

Además, se identificó la falta de capacitación de los operadores de justicia como un obstáculo significativo. En palabras del Dr. Villareal Tapia, “se requiere capacitación continua para jueces, fiscales y fuerzas de seguridad en tendencias y herramientas de ciberseguridad, así como establecer protocolos de intercambio de información”.

El Dr. Ruales Reinoso advierte que “la falta de prioridad política en la Asamblea Nacional podría retrasar la ratificación y su aplicación efectiva”.

- Categoría 4: Preparación institucional

Los entrevistados coinciden en que las instituciones ecuatorianas no están preparadas para manejar eficazmente los delitos informáticos. El Dr. Escobar Cadena indica que “aunque existen profesionales capacitados, es necesaria una agresiva socialización y capacitación de jueces, fiscales y abogados en temas de ciberdelincuencia”.

El Dr. Villareal Tapia enfatiza que “no hay fiscales especializados en delitos informáticos en todas las provincias, ni peritos en la Policía Judicial, lo que obliga a recurrir a especialistas de otras localidades”.

- Categoría 5: Influencia en la cooperación internacional

Los entrevistados coinciden en que la ratificación del Convenio de Budapest fortalecería la cooperación internacional de Ecuador en la lucha contra los delitos informáticos. El Dr. Escobar Cadena señala que “al integrarse al Convenio de Budapest, Ecuador contaría con un respaldo internacional que facilitaría la colaboración con otros países para enfrentar la ciberdelincuencia”.

Por su parte, el Dr. Villareal Tapia destaca que “el Convenio de Budapest es crucial para combatir la delincuencia cibernética, ya que facilita la cooperación internacional necesaria para enfrentar delitos transnacionales. Ratificarlo permitiría a Ecuador alinear sus leyes con estándares globales, mejorando la colaboración judicial y el intercambio de información con otros países”.

Finalmente, el Dr. Ruales Reinoso enfatiza que “la ratificación del Convenio de Budapest mejoraría significativamente la cooperación internacional de Ecuador, facilitando la colaboración con otros países y fortaleciendo la capacidad del país para combatir eficazmente los delitos informáticos”.

Encuestas

Los resultados de la encuesta refuerzan los hallazgos de las entrevistas. Se destacan los datos siguientes:

- 85.7% de los encuestados están familiarizados con el Convenio de Budapest.
- 100% consideran que Ecuador debería ratificarlo.
- 94.3% opinan que la legislación actual es poco efectiva o inefectiva contra los delitos informáticos.
- 100% creen que los delitos informáticos han aumentado en los últimos años.
- 54.3% tienen dudas sobre si la ratificación mejoraría la capacidad de lucha contra estos delitos.
- 100% afirman que las instituciones ecuatorianas no están preparadas para implementar las medidas del Convenio.
- 77.1% consideran que la cooperación internacional es importante o muy importante para combatir estos delitos.
- 100% han sido víctimas o conocen a alguien que ha sido víctima de un delito informático.
- 68.6% se sienten poco informados o neutrales respecto a las leyes de protección contra estos delitos.

Estos resultados evidencian la preocupación ciudadana sobre la ciberdelincuencia y la necesidad de fortalecer la legislación ecuatoriana a través de la ratificación del Convenio de Budapest.

Los hallazgos reflejan un consenso sobre la importancia de ratificar el Convenio de Budapest, la necesidad de actualizar la legislación, fortalecer la cooperación internacional y mejorar la capacitación de los operadores de justicia para enfrentar eficazmente los delitos informáticos en Ecuador.

Los resultados obtenidos en este estudio reflejan un consenso generalizado sobre la necesidad de ratificar el Convenio de Budapest como una medida clave para fortalecer el marco legal ecuatoriano en materia de ciberdelincuencia. La percepción de los encuestados y entrevistados indica que la legislación actual es insuficiente para hacer frente al avance de los delitos informáticos, lo que pone de manifiesto la urgencia de modernizar las normativas existentes.

Uno de los puntos más relevantes en la discusión es la necesidad de reformas legislativas. Si bien la ratificación del Convenio proporcionaría una base jurídica más sólida, su implementación requiere modificaciones en el Código

Orgánico Integral Penal y en otras normativas relacionadas con la seguridad digital. Sin estas reformas, la adhesión al Convenio podría quedar limitada en su efectividad.

Otro aspecto clave es la preparación institucional. Los hallazgos evidencian que Ecuador aún carece de infraestructura tecnológica y capital humano capacitado para abordar de manera efectiva los ciberdelitos. La falta de fiscales especializados, peritos forenses digitales y mecanismos de cooperación internacional impide una respuesta rápida y eficaz ante amenazas cibernéticas. En este sentido, se requiere una inversión significativa en capacitación y recursos tecnológicos.

La cooperación internacional es otro elemento fundamental en la discusión. La ciberdelincuencia es un fenómeno transnacional, por lo que la falta de adhesión al Convenio de Budapest limita la capacidad de Ecuador para intercambiar información y coordinar esfuerzos con otros países. Sin embargo, para que esta cooperación sea efectiva, Ecuador debe demostrar capacidad operativa y voluntad política para implementar los compromisos adquiridos.

El presente estudio guarda estrecha relación con el trabajo de Molina Mora et al. (2022), quienes analizan los principios democráticos de la Constitución ecuatoriana. Su investigación resalta la importancia de la seguridad jurídica y el respeto a los derechos fundamentales en la consolidación del Estado de derecho. En este sentido, la falta de un marco normativo adecuado en materia de ciberdelincuencia no solo compromete la capacidad del Estado para prevenir y sancionar estos delitos, sino que también debilita la protección de derechos fundamentales como la privacidad y la seguridad de la información. La ratificación del Convenio de Budapest contribuiría a fortalecer la gobernanza digital y la protección de los derechos ciudadanos en un entorno cada vez más interconectado, alineando la legislación ecuatoriana con estándares internacionales y garantizando una respuesta estatal más eficaz frente a las amenazas cibernéticas.

Asimismo, este estudio se vincula con el trabajo de Atencio González et al. (2022); y Medina-Peña & Torres (2024), quienes analizan la legislación ecuatoriana desde la perspectiva de los derechos humanos. Dicho estudio enfatiza que un marco normativo efectivo debe garantizar el respeto a los derechos fundamentales en todos los ámbitos, incluyendo el entorno digital. La ausencia de regulaciones adecuadas sobre ciberdelincuencia en Ecuador genera vulnerabilidades que pueden traducirse en violaciones a la privacidad, el acceso a la información y la protección de datos personales. En este sentido, la ratificación del Convenio de Budapest no solo fortalecería la capacidad estatal para enfrentar los delitos informáticos, sino que también alinearía la legislación ecuatoriana con los estándares internacionales de derechos humanos, promoviendo un equilibrio entre seguridad digital y garantías fundamentales.

Finalmente, la investigación sugiere que, aunque existe un fuerte respaldo social y académico a la ratificación del Convenio, su viabilidad dependerá de la alineación de actores clave dentro del sistema judicial y legislativo. La implementación de políticas públicas orientadas a la prevención, detección y persecución de delitos informáticos será determinante para el éxito de esta iniciativa.

CONCLUSIONES

El análisis jurídico de la ratificación del Convenio de Budapest en Ecuador permite identificar diversos puntos clave. En primer lugar, se evidencia que este tratado es fundamental para armonizar la legislación nacional con estándares internacionales, promoviendo una cooperación más efectiva en la lucha contra la ciberdelincuencia. Su adopción proporcionaría un marco normativo sólido que fortalecería las capacidades investigativas y judiciales del país.

El diagnóstico del estado actual de los delitos informáticos en Ecuador revela que la frecuencia de estos ilícitos está en aumento y que el marco normativo vigente no ofrece respuestas adecuadas para contrarrestarlos de manera eficiente. La ratificación del Convenio facilitaría la modernización de las normativas y permitiría una mejor respuesta del sistema judicial y de las fuerzas de seguridad, reduciendo la impunidad de los ciberdelincuentes.

Desde una perspectiva crítica-jurídica, se destaca la necesidad de reformas estructurales en la legislación ecuatoriana para garantizar la efectiva implementación del Convenio. Esto implica no solo la actualización del Código Orgánico Integral Penal, sino también la capacitación de los operadores de justicia en técnicas especializadas de investigación digital.

Asimismo, la cooperación interinstitucional y el establecimiento de protocolos claros para el intercambio de información son esenciales para optimizar la respuesta ante amenazas cibernéticas. Se recomienda la implementación de campañas de concienciación en ciberseguridad dirigidas tanto a la ciudadanía como a las autoridades encargadas de la aplicación de la ley.

Finalmente, la inversión en investigación y desarrollo en ciberseguridad es un elemento crucial. Mantenerse actualizado con las últimas tendencias y amenazas en el ámbito digital permitirá a Ecuador fortalecer su capacidad de prevención y respuesta ante delitos informáticos, garantizando una protección efectiva de su infraestructura crítica y de sus ciudadanos en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Atencio González, R. E., Molina Mora, J. F., & Andrade Olvera, G. A. (2022). La legislación ecuatoriana y los derechos humanos desde su perspectiva. *Universidad Y Sociedad*, 14(S3), 498–503. <https://rus.ucf.edu/cu/index.php/rus/article/view/2979>

- Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, (8), 169-203. <https://doi.org/10.18172/redur.4071>
- Feria Ávila, H., Matilla González, M., & Mantecón Licea, S. (2020). La entrevista y la encuesta: ¿métodos o técnicas de indagación empírica? *Didasc@lia: didáctica y educación*, 11(3), 62-79. <https://dialnet.unirioja.es/descarga/articulo/7692391.pdf>
- Gómez, C., Álvarez, G., Romero, A., Castro, F., Vega, V., Comas, R., & Velásquez, M. (2017). *La investigación científica y las formas de titulación. Aspectos conceptuales y prácticos*. Editorial Jurídica del Ecuador.
- Llinares, F. M. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista española de investigación criminológica*, 5(11), 1-35. <https://reic.criminologia.net/index.php/journal/article/view/77774>
- Medina-Peña, R., & Torres-Espinoza, J. J. (Coord.) (2024). *El neoconstitucionalismo en la protección de los nuevos derechos*. Sophia Editions.
- Molina Mora, J. F., Atencio González, R. E., & Moreno Arvelo, P. M. (2022). La Constitución Ecuatoriana y los principios democráticos. *Universidad Y Sociedad*, 14(S3), 487-497. <https://rus.ucf.edu.cu/index.php/rus/article/view/2978>
- Okuda Benavides, M., & Gómez-Restrepo, C. (2005). Métodos en investigación cualitativa: triangulación. *Revista colombiana de psiquiatría*, 34(1), 118-124. http://www.scielo.org.co/scielo.php?pid=S0034-74502005000100008&script=sci_arttext
- Rodríguez, O. (2020). *Análisis de los delitos informáticos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito*. (Tesis de Licenciatura). Universidad Laica Vicente Rocafuerte de Guayaquil.
- Tantaleán, R. (2016). Tipología de las investigaciones jurídicas. *Derecho y cambio social*, 13(43), 1-37. <https://dialnet.unirioja.es/descarga/articulo/5456267.pdf>
- Zambrano-Mendieta, J. E., Dueñas-Zambrano, K. I., & Macías-Ordoñez, L. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio De Las Ciencias*, 2(2), 204-215. <https://doi.org/10.23857/dc.v2i2.159>