Revista científica Sociedad & Tecnología

ISSN: 2773-7349

fecha de presentación: 12/02/2025, fecha de aceptación: 15/03/2025, fecha de publicación: 01/05/2025

Liseth Eliana Zúñiga-Ortega
E-mail: ur.lisethzo66@uniandes.edu.ec
Orcid: https://orcid.org/0009-0002-8592-5506

José Mateo Muñoz-Cortes
E-mail: josemc69@uniandes.edu.ec
Orcid: https://orcid.org/0009-0005-7727-0951

Jonathan Josue Pilamunga-Malan
E-mail: jonathanpm37@uniandes.edu.ec
Orcid: https://orcid.org/0009-0007-2935-0695

Universidad Regional Autónoma de Los Andes, Riobamba. Ecuador.

Cita sugerida (APA, séptima edición)

Zuñiga Ortega, LE, Muñoz Cortes, JM, Pilamunga Malan, JJ. (2025). Delitos cibernéticos y su tratamiento en la jurisdicción ecuatoriana. *Revista Sociedad & Tecnología*, 8(S1), 249-261. DOI: https://doi.org/10.51247/st.v8iS1.582.

==== o ====

Delitos cibernéticos y su tratamiento en la jurisdicción ecuatoriana

RESUMEN

El presente estudio tuvo como objetivo analizar la problemática de los delitos de ciberseguridad en Ecuador, en el contexto del desarrollo y la globalización de internet y sus plataformas, así como evaluar la suficiencia del marco legal ecuatoriano, específicamente el Código Orgánico Integral Penal (COIP) de 2014, para abordar estos delitos. Se empleó una metodología cualitativa basada en la revisión documental y el análisis de la legislación vigente, así como de información secundaria relacionada con la incidencia de delitos cibernéticos y la percepción de la población sobre la ciberseguridad en Ecuador. La investigación determinó que existe una falta generalizada de conocimientos en la población ecuatoriana sobre ciberseguridad, lo que facilita la ocurrencia de delitos cibernéticos. Se evidenció que el COIP de 2014, si bien contempla algunos elementos relacionados con estos delitos, resulta insuficiente en cuanto a la profundidad con la que aborda las diversas tipologías y la severidad de las penas aplicadas. Se concluye la necesidad de reformar las leyes ecuatorianas en materia de ciberseguridad para abordar de manera más integral y con sanciones más severas los delitos cibernéticos. Asimismo, se destaca la importancia de implementar programas de preparación y concienciación para la población, así como de fortalecer las acciones de combate contra estos delitos en el país.

Palabras clave: leyes, educación, delitos, seguridad, tratamiento.

==== o ====

Cybercrimes and their treatment in Ecuadorian jurisdiction

ABSTRACT

This study aimed to analyze the problem of cybersecurity crimes in Ecuador, in the context of the development and globalization of the internet and its platforms, as well as to evaluate the adequacy of the Ecuadorian legal framework, specifically the 2014 Comprehensive Organic Criminal Code (COIP), to address these crimes. A qualitative methodology was used based on a documentary review and analysis of current legislation, as well as secondary

information related to the incidence of cybercrimes and the public's perception of cybersecurity in Ecuador. The research determined that there is a widespread lack of knowledge among the Ecuadorian population about cybersecurity, which facilitates the occurrence of cybercrimes. It was evident that the 2014 COIP, while it addresses some elements related to these crimes, is insufficient in terms of the depth with which it addresses the various types and the severity of the penalties applied. The conclusion is drawn that Ecuadorian cybersecurity laws need to be reformed to address cybercrimes more comprehensively and with more severe penalties. The importance of implementing preparedness and awareness programs for the population, as well as strengthening efforts to combat these crimes in the country, is also highlighted.

Keywords: laws, education, crimes, security, treatment.

==== o ====

Crimes cibernéticos e seu tratamento na jurisdição equatoriana

RESUMO

O presente estudo teve como objetivo analisar o problema dos crimes de segurança cibernética no Equador, no contexto do desenvolvimento e globalização da Internet e suas plataformas, bem como avaliar a adequação do arcabouço legal equatoriano, especificamente o Código Penal Orgânico Integral (COIP) de 2014, para enfrentar esses crimes. Foi utilizada uma metodologia qualitativa baseada em revisão documental e análise da legislação vigente, bem como informações secundárias relacionadas à incidência de crimes cibernéticos e à percepção do público sobre a segurança cibernética no Equador. A pesquisa determinou que há uma falta generalizada de conscientização sobre segurança cibernética entre a população equatoriana, o que facilita a ocorrência de crimes cibernéticos. Constatou-se que o COIP de 2014, embora aborde alguns elementos relacionados a esses crimes, é insuficiente em termos da profundidade com que aborda os vários tipos de crimes e da gravidade das penas aplicadas. Fica estabelecida a necessidade de reformar as leis de segurança cibernética do Equador para abordar os crimes cibernéticos de forma mais abrangente e com penalidades mais severas. Da mesma forma, destaca-se a importância da implementação de programas de preparação e conscientização da população, bem como do fortalecimento das ações de combate a esses crimes no país.

Palavras-chave: leis, educação, crimes, segurança, tratamento.

==== o ====

INTRODUCCIÓN

El marco legal y la penalización de los delitos cibernéticos en Ecuador han experimentado una notable evolución en las últimas dos décadas. La base de este progreso se encuentra en la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en 2002 (Ley No. 2002-67), que marcó un punto de partida importante al reconocer legalmente los documentos y firmas electrónicas, así como al regular los mensajes de datos y la contratación electrónica (Registro Oficial, 2002). No obstante, la capacidad inicial de esta legislación para enfrentar la creciente complejidad de los desafíos de ciberseguridad era limitada, lo que dejaba a individuos y organizaciones potencialmente expuestos a diversas amenazas digitales en un entorno en rápida transformación.

La aparición y la progresiva expansión de internet y los sofisticados sistemas informáticos marcaron un punto de inflexión en la manera en que las personas acceden e interactúan con los sistemas de información. En este nuevo panorama digital, cada acción deja una huella, reflejando cómo "la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día" (García, 2018, p. 25).

El nacimiento y la continua evolución de las tecnologías de la información y la comunicación (TIC), así como todo lo derivado del uso generalizado de internet y las redes globales del conocimiento, han constituido transformaciones evidentes en la sociedad contemporánea (Tirado y Cáceres, 2021). Con este vertiginoso desarrollo tecnológico, se ha incrementado exponencialmente el comercio electrónico y la interacción digital de las personas para la realización de pagos y diversas transacciones en línea, lo que, a su vez, ha ampliado significativamente la posibilidad del cometimiento de delitos en el ciberespacio (Vereau, 2021).

Con el avance exponencial de la tecnología digital, se volvió imperativo actualizar y ampliar de manera sustancial el marco legal ecuatoriano para contrarrestar la creciente sofisticación y diversidad de los delitos cibernéticos (Córdova, 2024). Las amenazas digitales se diversificaron a un ritmo vertiginoso, trascendiendo las formas iniciales para abarcar un espectro cada vez más amplio y complejo, que incluye desde el phishing y la proliferación de malware hasta los devastadores ataques de ransomware que paralizan infraestructuras críticas y el intrusivo espionaje cibernético que compromete la seguridad nacional y la privacidad individual.

Esta evolución constante del panorama de amenazas digitales evidenció de manera inequívoca la necesidad de una legislación más robusta, específica y adaptable, que pudiera proporcionar una protección efectiva a los ciudadanos, las empresas y el Estado en un entorno digital en continua transformación (Reincisol, 2024).

El cibercrimen se distingue por presentar un nivel elevado de lesividad en comparación con los delitos tradicionales que se cometen en el mundo físico (Gorostidi, 2020; Flores, 2019). Esta mayor capacidad de daño se deriva de la naturaleza transfronteriza del ciberespacio, la facilidad para cometer delitos de forma remota y a gran escala, y el potencial para causar perjuicios económicos, sociales y personales significativos en un corto período de tiempo.

Esta intrínseca peligrosidad del cibercrimen justifica que sea abordado con una atención especial y un tratamiento diferenciado en las leyes penales, buscando establecer sanciones proporcionales al daño potencial y real causado por estas actividades ilícitas (Sarmiento-Chamba & Maldonado-Ruiz, 2024). La legislación debe, por lo tanto, evolucionar para no solo tipificar de manera clara y precisa las nuevas formas de criminalidad digital, sino también para establecer mecanismos de investigación y persecución eficaces que permitan llevar a los responsables ante la justicia.

En este contexto, la promulgación y posterior reforma del Código Orgánico Integral Penal (COIP) en Ecuador representaron esfuerzos importantes para integrar disposiciones específicas relacionadas con los delitos informáticos (Registro Oficial, 2014). Sin embargo, la naturaleza dinámica y la constante innovación en las tácticas y técnicas del cibercrimen exigen una revisión y actualización continua del marco legal. Es fundamental que la legislación ecuatoriana se mantenga a la vanguardia en la lucha contra las amenazas digitales, incorporando las mejores prácticas internacionales y adaptándose a los nuevos desafíos que surgen en el ciberespacio para garantizar una protección efectiva de los derechos y la seguridad de todos los ciudadanos en la era digital (Meythaler Zambrano Abogados, 2024).

Sin embargo, a pesar de estos avances, persisten desafíos significativos, como la insuficiencia de recursos y la necesidad de actualizar continuamente la legislación para enfrentar nuevas formas de cibercrimen. Existe falencias en relación a la tipificación del delito informático y no se posee una estructura legislativa que respalde la seguridad de la información de los ciudadanos (Tubay, 2021).

La cooperación internacional ha sido un componente clave en la lucha contra el cibercrimen en Ecuador. La naturaleza transnacional de los delitos cibernéticos hace que la colaboración con otros países y organizaciones sea vital para enfrentarlos de manera efectiva. Ecuador ha

participado activamente en acuerdos y foros internacionales sobre ciberseguridad, lo que ha permitido al país acceder a recursos, capacitación y apoyo en la investigación de delitos cibernéticos. Iniciativas como el Convenio de Budapest sobre Ciberdelincuencia han permitido a Ecuador alinearse con estándares internacionales y mejorar su marco legal y operativo.

Se destaca la importancia de un enfoque integral y dinámico para enfrentar las amenazas cibernéticas. Se menciona la necesidad de capacitación continua, cooperación internacional y actualización de la legislación. Se propone la creación de una Agencia Nacional de Ciberseguridad para coordinar los esfuerzos a nivel nacional y mejorar la respuesta a incidentes. Además, se enfatiza la inversión en infraestructura tecnológica y formación del personal para fortalecer la capacidad de las fuerzas del orden contra el cibercrimen. Se subraya la protección de datos personales como un componente crítico a fortalecer, y se resalta la importancia de la educación y concienciación pública para prevenir delitos cibernéticos.

Sin embargo, a pesar de estos avances legislativos y la creciente conciencia sobre la amenaza del cibercrimen en Ecuador, persisten desafíos significativos que requieren atención continua. ¿Cómo se están abordando concretamente la insuficiencia de recursos técnicos y humanos dedicados a la investigación y persecución de estos delitos? Y, más aún, ¿cómo se puede garantizar una actualización legislativa constante y ágil que pueda hacer frente a la velocidad con la que evolucionan las tácticas y técnicas del cibercrimen? Un aspecto crítico que aún presenta falencias importantes se relaciona con la tipificación precisa y exhaustiva de todas las formas de delito informático, así como la ausencia de una estructura legislativa sólida y específica que respalde de manera integral la seguridad de la información de los ciudadanos en el entorno digital (Tubay, 2021). Estas interrogantes resaltan la necesidad de una evaluación continua y proactiva del marco legal y las capacidades operativas del país en materia de ciberseguridad.

La elaboración de este trabajo tiene como objetivo principal analizar la evolución del marco legal ecuatoriano en relación con los delitos cibernéticos, identificar los avances significativos alcanzados y, crucialmente, señalar las persistentes brechas y desafíos que aún deben ser abordados. A través de la revisión de la legislación existente, la literatura especializada y el análisis del contexto nacional e internacional, se busca ofrecer una perspectiva informada sobre la situación actual y proponer líneas de acción futuras que permitan fortalecer la capacidad del Estado ecuatoriano para prevenir, investigar y sancionar eficazmente el cibercrimen, garantizando así un entorno digital más seguro y confiable para todos sus ciudadanos.

Metodología

La investigación se basa en un enfoque descriptivo, utilizando el método histórico lógico el cual hace hincapié en la necesidad de analizar tanto los aspectos históricos como lógicos de un fenómeno en una investigación, abordando su evolución a lo largo del tiempo y su naturaleza cualitativa (López y Ramos, 2021); inductivo deductivo, que se fundamenta en el razonamiento que parte de casos particulares para derivar conclusiones generales que reflejan lo común en los fenómenos individuales (López y Ramos, 2021), y el analítico sintético, se centra en desglosar lo complejo en partes y, posteriormente, sintetizar estas partes para comprender las relaciones y características generales (Delgado y Romero, 2021), en este caso analizar los riesgos y tipos penales en el marco legal de los delitos cibernéticos en Ecuador.

Se emplearon metodologías cuantitativas y cualitativas para recopilar opiniones y criterios sobre la penalización de estos delitos en la jurisdicción ecuatoriana. La encuesta fue elaborada de forma organizada siguiendo pasos que posibiliten el desarrollo eficiente de su estructura para la obtención de los datos requeridos, se tuvo en cuenta que la misma en su

concepción debe ser clara y de forma sencilla (Santamaria et al., 2020), de forma que facilite la compresión de los encuestados.

La metodología cuantitativa proporciona una base sólida para identificar puntos críticos y realizar un estudio detallado del mismo que se llevara a análisis de datos para dar una conclusión, mientras que la cualitativa permite una comprensión profunda del marco legal y las penas asociadas. Ambos enfoques permiten explorar percepciones y experiencias de diferentes actores involucrados en este ámbito, contribuyendo a un análisis completo de la situación de los delitos cibernéticos en Ecuador. En el desarrollo de la investigación se prevee la necesidad de conocer los fundamentos de los principales métodos utilizados, sus características, requerimientos y las condiciones en las que hay que escoger el más adecuado (Polgar y Thomas, 2021).

La aplicación de los métodos permitió determinar los resultados que se exponen en la investigación. Para los datos principales obtenidos en la encuesta fue empleada en la investigación una muestra al azar compuesta de 52 encuestados, los que oscilan en las edades comprendidas entre 21 a 48.

RESULTADOS Y DISCUSIÓN

La encuesta consta de una serie de preguntas que fundamentan los puntos importantes que evidencia la falta de protección ante el marco legal y penalización de delitos cibernéticos en la jurisdicción ecuatoriana.

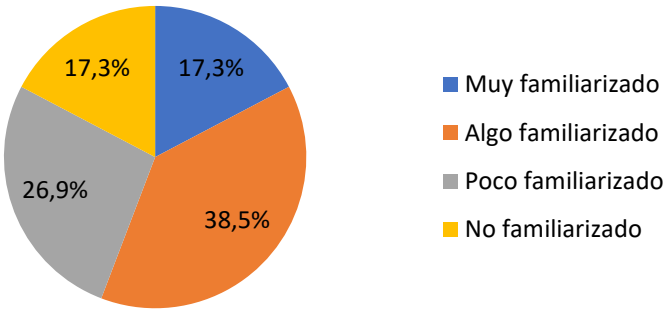

Figura 1. ¿Está usted familiarizado con las disposiciones del COIP sobre delitos cibernéticos?

Tras los resultados de una encuesta realizada para medir el grado de familiaridad de los encuestados con las disposiciones del Código Orgánico Integral Penal (COIP) respecto a los delitos cibernéticos (Figura 1), la que contó con un total de 52 respuestas, que se distribuyeron en cuatro categorías de familiaridad.

En primer lugar, el 17.3% de los participantes, correspondiente a 9 personas, declararon estar muy familiarizados con las disposiciones del COIP sobre delitos cibernéticos, denotado por el color azul en la gráfica. En segundo lugar, un 26.9% de los encuestados, es decir, 14 personas, indicaron estar algo familiarizados, representado por el color naranja.

En contraste, un mayor porcentaje de los encuestados mostró niveles más bajos de familiaridad. Un 38.5% de los participantes, que equivale a 20 personas, manifestó estar poco familiarizado con las disposiciones legales en cuestión, lo cual está representado por el color amarillo en la gráfica. Finalmente, un 17.3% de los encuestados, también 9 personas, señaló no estar familiarizado con dichas disposiciones, lo cual está denotado por el color verde.

Estos resultados sugieren que, si bien existe un grupo significativo que tiene algún nivel de conocimiento sobre el COIP en lo que concierne a los delitos cibernéticos, la mayoría de los encuestados posee un conocimiento limitado o nulo al respecto. Esto podría indicar la necesidad de una mayor difusión y educación sobre estas disposiciones legales para asegurar que un mayor número de personas esté informado sobre este importante tema.

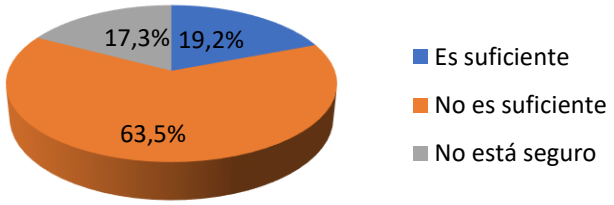

Figura 2. ¿Considera que la legislación ecuatoriana actual es suficiente para enfrentar las amenazas cibernéticas modernas?

Tras la encuesta realizada a 52 individuos sobre la suficiencia de la legislación ecuatoriana vigente para enfrentar las amenazas cibernéticas modernas (Figura 2). Según los datos obtenidos, una abrumadora mayoría del 63.5% de los encuestados considera que la legislación actual es insuficiente para abordar los desafíos cibernéticos contemporáneos, lo que sugiere una percepción generalizada de inadecuación en las normativas existentes. Por otro lado, un 19.2% de los participantes opina que la legislación es suficiente, indicando que una minoría confía en la capacidad de las leyes actuales para proteger contra las amenazas cibernéticas.

Además, un 17.3% de los encuestados se mostró indeciso, afirmando no estar seguro sobre la efectividad de la legislación vigente en este ámbito. Estos resultados ponen de manifiesto la necesidad de evaluar y posiblemente reforzar las leyes ecuatorianas en materia de ciberseguridad para garantizar una mejor protección contra las amenazas que evolucionan constantemente en el entorno digital.

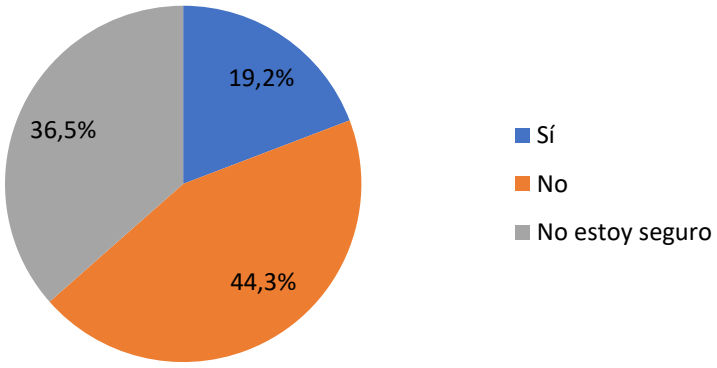

Figura 3. ¿Cree que las fuerzas del orden en Ecuador están adecuadamente capacitadas para manejar delitos cibernéticos?

De acuerdo con los datos obtenidos, una mayoría del 44.2% de los encuestados considera que las fuerzas del orden no están adecuadamente capacitadas para enfrentar los desafíos que representan estos delitos en el ámbito digital. Este alto porcentaje indica una

significativa preocupación respecto a la preparación y formación de las autoridades encargadas de la seguridad cibernética en el país.

Por otro lado, un 36.5% de los participantes se manifestó indeciso, expresando que no están seguros sobre la capacidad de las fuerzas del orden en este contexto, lo cual evidencia una falta de confianza o conocimiento claro sobre las competencias actuales de estas instituciones en el manejo de delitos cibernéticos. Finalmente, solo un 19.2% de los encuestados opina que las fuerzas del orden están adecuadamente capacitadas para gestionar estos casos, lo que representa una minoría que confía en la efectividad de las autoridades en el combate contra la ciberdelincuencia. En conjunto, estos resultados destacan la necesidad de fortalecer y mejorar la formación y recursos destinados a las fuerzas del orden en Ecuador para asegurar una respuesta eficaz ante las crecientes amenazas cibernéticas.

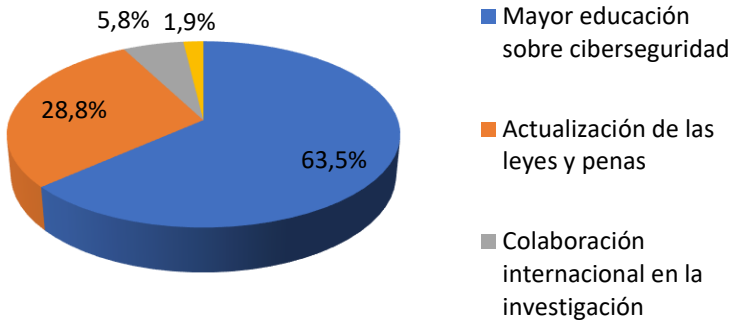

Figura 4. ¿Qué medidas crees que deberían implementarse para mejorar la lucha contra los delitos cibernéticos en Ecuador?

La mayoría significativa, representada por el 63.5% de los participantes, subraya la importancia de una mayor educación en ciberseguridad. Esto refleja una percepción general de que el conocimiento y la concienciación sobre las amenazas cibernéticas son esenciales para prevenir y mitigar los riesgos asociados. La educación en ciberseguridad puede incluir desde programas de formación para el público en general hasta cursos especializados para profesionales del sector, y se considera una herramienta fundamental para crear una cultura de seguridad en la era digital.

En segundo lugar, el 28.8% de los encuestados destaca la necesidad de actualizar las leyes y penas relacionadas con los delitos cibernéticos. Esta perspectiva sugiere que las normativas actuales pueden no estar adecuadamente equipadas para enfrentar las nuevas y emergentes formas de criminalidad en el ciberespacio. La actualización de las leyes y penas permitiría una mayor adaptabilidad y eficacia en la persecución y sanción de los delitos, asegurando que el sistema legal esté alineado con las realidades tecnológicas y las tácticas empleadas por los ciberdelincuentes. Este enfoque legal es visto como un complemento esencial a las iniciativas educativas, creando un marco integral de prevención y respuesta ante los desafíos cibernéticos.

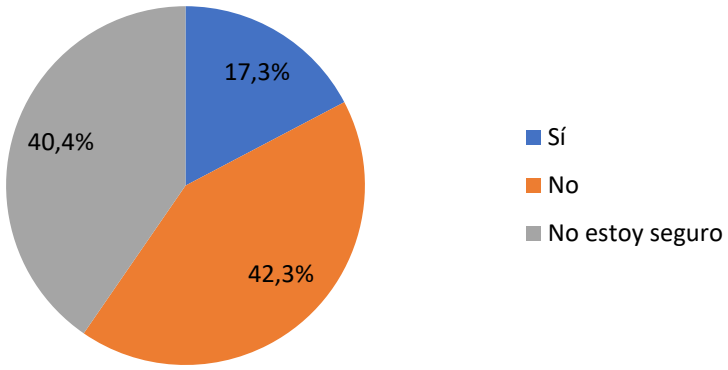

Figura 5. ¿Cree que las penas actuales para los delitos cibernéticos en Ecuador son lo suficientemente severas?

El gráfico refleja las percepciones de los encuestados sobre la severidad de las penas actuales para los delitos cibernéticos en Ecuador (Figura 5). De un total de 52 respuestas, un 42.3% de los participantes manifestó que las penas no son lo suficientemente severas, lo que sugiere una opinión predominante de que el marco legal vigente no disuade ni sanciona de manera adecuada estos delitos. Esta percepción puede indicar la necesidad de una revisión y fortalecimiento de las leyes actuales para garantizar que sean efectivas en la prevención y castigo de los delitos cibernéticos.

Asimismo, un 40.4% de los encuestados indicó que no está seguro sobre la severidad de las penas. Este resultado pone de manifiesto una posible falta de información o de claridad respecto a las normativas y sanciones existentes. La incertidumbre en este grupo podría deberse a una comunicación insuficiente por parte de las autoridades o a la complejidad de la legislación en materia de ciberseguridad, lo que resalta la importancia de campañas informativas y educativas sobre este tema.

Finalmente, sólo un 17.3% de los participantes considera que las penas actuales son adecuadas. Esta minoría sugiere que hay un segmento reducido de la población que percibe las medidas punitivas como suficientes para abordar los desafíos que plantean los delitos cibernéticos. En conjunto, los resultados del gráfico subrayan la necesidad de evaluar y posiblemente reformar el marco legal vigente, así como de mejorar la difusión de información para aumentar la comprensión pública sobre la severidad y efectividad de las sanciones aplicadas a los delitos cibernéticos en Ecuador.

La regulación de los delitos cibernéticos en Ecuador comenzó con la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en 2002. Esta ley representó un hito significativo al proporcionar un marco legal inicial para el comercio electrónico y la validez de las firmas electrónicas. Estableció las bases para el reconocimiento legal de los documentos digitales y la infraestructura necesaria para la autenticación de firmas electrónicas, cruciales en una economía digital emergente. Sin embargo, aunque constituyó un paso avance, en términos de ciberseguridad y protección contra delitos cibernéticos esto aún era carente.

A lo largo de los años siguientes, se hizo evidente que la legislación inicial no era suficiente para abordar la creciente sofisticación de los delitos cibernéticos. No eran suficientes para contrarrestar el surgimiento de nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia, que describen de forma genérica los aspectos ilícitos

cometidos en el ciberespacio y que tienen cuatro características específicas: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas" (Zunzunegui, 2018).

La ciberseguridad es un desafío creciente en la era digital, y la legislación juega un papel crucial en la protección contra las amenazas cibernéticas. En Ecuador, el Código Orgánico Integral Penal (COIP) establece las disposiciones legales para abordar los delitos cibernéticos. Sin embargo, una reciente encuesta realizada a 52 individuos entre 21 y 48 años revela preocupaciones significativas sobre la efectividad y el conocimiento de estas normativas. Este análisis se basa en los resultados de dicha encuesta para discutir la familiaridad, suficiencia y efectividad de la legislación ecuatoriana en ciberseguridad.

La familiaridad con las disposiciones del COIP sobre delitos cibernéticos varía considerablemente entre los encuestados, dichos datos sugieren que, aunque hay una fracción de la población con cierto nivel de conocimiento, la mayoría tiene un conocimiento insuficiente o nulo. Esto subraya la necesidad de iniciativas educativas y de concienciación sobre las disposiciones legales en ciberseguridad.

La participación activa de Ecuador en foros internacionales sobre ciberseguridad es crucial para fortalecer sus capacidades en esta área. A través de su involucramiento en organizaciones como la Organización de los Estados Americanos (OEA) y la Unión Internacional de Telecomunicaciones (UIT), Ecuador ha tenido la oportunidad de intercambiar conocimientos y mejores prácticas con otros países. Estos foros proporcionan una plataforma para discutir estrategias efectivas y coordinar acciones contra el cibercrimen a nivel regional y global, lo que permite la aparición de nuevos modos de combate del cibercrimen.

Aseguran que las estrategias se mantengan relevantes y efectivas frente a un entorno de amenazas en constante evolución. La cooperación con expertos internacionales y la incorporación de mejores prácticas globales también pueden contribuir a fortalecer las estrategias nacionales de ciberseguridad en Ecuador (Toapanta et al., 2020), la cual no es suficiente porque atreves de la percepción sobre la suficiencia de la legislación actual para enfrentar las amenazas cibernéticas modernas es crítica, esto reflejan una percepción generalizada de que la legislación ecuatoriana necesita ser evaluada y posiblemente reforzada para garantizar una protección efectiva contra las amenazas cibernéticas.

Según Torres existe una fuerte tendencia a que los hechos delictivos se concentren hacia la parte empresarial, siendo este un blanco elegido por los antisociales, en muchos casos, por descuidos en cuanto al sistema de seguridad de las mismas organizaciones (Torres, 2018). En una investigación realizada por Luna uno de los delitos de informática más utilizados por los ciberdelincuentes, es el espionaje informático. Explica el autor, que el mismo actúa como acechador, instigador y vigila de manera disimulada, a una persona clave para luego abordarla y obtener información sobre alguien o de una empresa o del gobierno. El espionaje industrial, ha cobrado mucho auge mediante la tecnología y, representa una buena plaza donde los cibercriminales pueden obtener mejores ganancias metálicas (Luna, 2018).

Finalmente, la percepción sobre la severidad de las penas actuales es variada, esto principalmente destaca en la necesidad de revisar y posiblemente reforzar el marco legal, así como de mejorar la difusión de información sobre las sanciones para aumentar la comprensión pública. Según Bum Suk menciona que las tecnologías digitales son usadas a menudo para "restringir los derechos a la libertad de expresión, el acceso a información, y la libertad de reunión pacífica" (Organización de las Naciones Unidas, 2022).

LIMITACIONES DEL ESTUDIO

La presente investigación se basó principalmente en la revisión documental y el análisis de la legislación vigente, lo que proporciona una perspectiva general sobre la problemática de los delitos cibernéticos y su tratamiento legal en Ecuador. Sin embargo, esta metodología no permitió obtener datos primarios sobre la incidencia real de estos delitos, las experiencias de las víctimas o las perspectivas de los operadores de justicia. Futuras investigaciones podrían complementar estos hallazgos mediante estudios cuantitativos sobre la prevalencia de los delitos cibernéticos, análisis de casos judiciales o entrevistas con expertos en ciberseguridad y derecho penal para obtener una comprensión más profunda y detallada del fenómeno.

ESTUDIOS FUTUROS

Para profundizar en la comprensión y el abordaje de los delitos cibernéticos en Ecuador, se sugieren diversas líneas de investigación futura. Sería valioso realizar estudios empíricos para determinar la tipología y la frecuencia de los delitos cibernéticos más comunes en el país, así como analizar el impacto socioeconómico de estos delitos en la población y las empresas. Asimismo, se recomienda investigar la efectividad de las campañas de concienciación y los programas de educación en ciberseguridad implementados hasta el momento. Otra área relevante para futuras investigaciones podría ser el análisis comparativo del marco legal ecuatoriano con las legislaciones de otros países de la región y a nivel internacional, con el fin de identificar mejores prácticas y posibles reformas.

RECONOCIMIENTO

Se extiende un sincero agradecimiento a todas las personas e instituciones que, de manera directa o indirecta, contribuyeron a la realización de este estudio. En particular, se reconoce la valiosa colaboración de colegas y profesionales que aportaron su conocimiento y perspectiva sobre la temática de los delitos cibernéticos y el marco legal ecuatoriano.

CONTRIBUCIÓN DE LOS AUTORES

Liseth Eliana Zúñiga-Ortega: Concibió la idea original de la investigación, definió el objetivo principal del estudio y participó activamente en la selección y análisis de las fuentes documentales relevantes para la comprensión del marco legal ecuatoriano en materia de delitos cibernéticos.

José Mateo Muñoz-Cortes: Contribuyó significativamente en la revisión y análisis de la legislación vigente, específicamente el Código Orgánico Integral Penal, identificando las disposiciones relacionadas con los delitos cibernéticos y evaluando su alcance y limitaciones en el contexto actual.

Jonathan Josue Pilamunga-Malan: Participó en la búsqueda y sistematización de información secundaria relacionada con la incidencia de delitos cibernéticos en Ecuador y la percepción de la población sobre la ciberseguridad, aportando elementos clave para contextualizar la problemática analizada en el estudio.

CONCLUSIONES

La investigación sobre el marco legal y la penalización de los delitos cibernéticos en Ecuador revela importantes hallazgos y consideraciones para fortalecer la ciberseguridad en el país. Mediante la investigación se muestra que una parte significativa de la población tiene un conocimiento limitado o nulo sobre las disposiciones del Código Orgánico Integral Penal (COIP) en relación con los delitos cibernéticos. Esta falta de familiaridad sugiere una necesidad urgente de programas educativos y campañas de concienciación que informen a la ciudadanía sobre la legislación vigente en materia de ciberseguridad.

En cuanto a la percepción sobre la suficiencia de la legislación actual la mayoría de los encuestados considera que la legislación ecuatoriana es insuficiente para enfrentar las amenazas cibernéticas modernas. Este resultado resalta la necesidad de evaluar y posiblemente reforzar las leyes existentes para garantizar una protección efectiva contra los delitos cibernéticos, adaptándose a la evolución constante de las amenazas digitales, elemento que debe ir aparejado a la capacitación de las Fuerzas del Orden que no están adecuadamente capacitadas para manejar los desafíos de los delitos cibernéticos, elementos mostrados por las encuestas a la muestra y los resultados de los métodos aplicados a los especialista que fueron seleccionados.

Ecuador ha realizado avances significativos en la legislación sobre ciberseguridad, persisten desafíos importantes que deben ser abordados. Es fundamental adoptar un enfoque integral y dinámico que incluya la educación continua, la cooperación internacional, la actualización legislativa, la capacitación de las fuerzas del orden y la concienciación pública para enfrentar eficazmente los delitos cibernéticos. Además, se propone la creación de una Agencia Nacional de Ciberseguridad para coordinar estos esfuerzos y mejorar la respuesta a incidentes, fortaleciendo así la capacidad del país para protegerse contra las amenazas en el entorno digital.

REFERENCIAS

Aparicio, V. V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(1), 1057-1063. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/284

Córdova, L. A. O. (2024). Análisis Jurídico del Acto Administrativo: Presunción de Legalidad y Garantías de los Administrados en el Contexto Constitucional Ecuatoriano. *Reincisol*, *3*(5), 1-15.

Córdova, L. A. O. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. *Reincisol.*, *3*(5), 1447-1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

Delgado , P. y Romero, M. (2021). Elaboración de un proyecto de investigación con metodología cualitativa. *Enfermería Intensiva*, 24. https://dialnet.unirioja.es/servlet/articulo?codigo=8424703

Ecuador. Asamblea Nacional (2014). Código Orgánico Integral Penal Registro Oficial 180. Gobierno del Ecuador. https://www.asambleanacional.gob.ec/es/system/files/document.pdf

Flores, A. (2019). *Ciberdelincuencia: Aspectos generales y su tratamiento jurídico*. Editorial Jurídica del Perú.

Flores, F. (2019). Análisis del lugar de comisión de los ciberdelitos de contenido.¿Impunidad ó universalización del delito?. *Cuadernos de Política Criminal*, (128). https://openurl.ebsco.com/EPDB%3Agcd%3A6%3A26994294/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A143299393&crl=c&link_origin=scholar.google.com

Garcia, A. (23 de 09 de 2018). *Internet la nueva era del delito*. Obtenido de Internet la nueva era del delito: https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/2108

Garcia, F. (2018). *La sociedad de la información*. Editorial UOC.

Gorostidi, A. (2020). *Derecho penal informático*. Editorial B de F.

Gorostidi, J. L. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Estudios de Deusto: revista de Derecho Público*, *68*(1), 201-221. https://dialnet.unirioja.es/servlet/articulo?codigo=7483941

Juca, F., & Medina, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Portal de la Ciencia*, *4*(3), 325-337. https://institutojubones.edu.ec/ojs/index.php/portal/article/view/394

López, A., y Ramos, G. (2021). Acerca de los métodos teóricos y empíricos de investigación: significación para la investigación. *CONRADO*, 24.

Luna, V. (2018). Espionaje informático, robo de identidad e información. *Quanti Solutions, 2*(1), 6-14. https://www.quanti.com.mx/2018/03/05/espionaje-informatico-robo-identidad-e-informacion/

Meythaler Zambrano Abogados. (2024, 28 de marzo). *Ecuador y el Convenio de Budapest: Fortaleciendo la Lucha contra la Ciberdelincuencia*. https://www.meythalerzambranoabogados.com/post/ecuador-y-el-convenio-de-budapest-contra-la-ciberdelincuencia

Organización de las Naciones Unidas (01 de 09 de 2022). *Los derechos humanos deben formar parte esencial de la gobernanza tecnológica*. https://www.ohchr.org/es/stories/2022/09/human-rights-should-be-heart-tech-governance#:~:text=A%20pesar%20de%20sus%20numerosas,del%20Consejo%20de%20Derechos%20Humanos

Polgar, S. y Thomas, S. (2021). *Introducción a la investigación en ciencias de la salud*. Elsevier Health Sciences. https://www.elsevier.com/books/introduccion-a-la-investigacion-en-ciencias-de-la-salud/polgar/978-84-9113-848-8

Registro Oficial. (2002, 17 de abril). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)*. Suplemento del Registro Oficial No. 577.

Registro Oficial. (2014, 10 de febrero). *Código Orgánico Integral Penal* (Suplemento No. 180).

Reincisol. (2024). *El Marco Legal de los Delitos Cibernéticos en Ecuador*. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

Santamaría, D., Andachi, J. y Montoya, Ó. (2020). Method for Evaluating the Principle of Interculturality in the Custodial Sentence using the Iadov Technique. *Neutrosophic Sets and Systems*, *37*, 125-131. https://doi.org/10.5281/zenodo.4122047

Sarmiento-Chamba, J. A., & Maldonado-Ruiz, L. M. (2024). Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador. *MQRInvestigar*, *8*(3), 1753–1781.

Tirado, F., & Cáceres, M. D. (2021). Tecnologías de la información y la comunicación (TIC) en la sociedad actual: Una revisión teórica. *Revista Científica y Tecnológica UPSE*, *8*(1), 15-22.

Tirado, M., & Cáceres, V. M. (2021). La política criminal frente al ciberdelito sexual contra niños, niñas y adolescentes en Colombia. *Revista Científica General José María Córdova*, *19*(36), 1011-1033. http://www.scielo.org.co/scielo.php?pid=S1900-65862021000401011&script=sci_arttext

Toapanta Toapanta, S. M., Tacuri López, I. L., & Mafla Gallegos, L. E. (2020). Analysis of the Legal Basis to Mitigate Cyberbullying in Social Networks in Ecuador. In *Fuzzy Systems*

and Data Mining VI (pp. 223-233). IOS Press. https://ebooks.iospress.nl/volumearticle/55944

Torres, L. (09 de 2018). *Delitos informaticos*. Obtenido de Delitos informaticos: https://www.redalyc.org/journal/290/29062641023/html/

Tubay, M. A. P. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, *1*(58), 119-123. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667

Van, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review, 36*, 105377. https://www.sciencedirect.com/science/article/abs/pii/S0267364919303887

Vereau, J. (2021). *Ciberdelincuencia y comercio electrónico: Desafíos para la legislación*. Editorial Jurídica del Ecuador.

Vereau, R. V. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, (053), 95-110. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995

Zunzunegui, S. (24 de 09 de 2018). *La nueva era del delito*. Obtenido de La nueva era del delito: https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/2108