Revista científica Portal de la Ciencia

ISSN: 2953-6502

Fecha de presentación: 07/05/2023
Fecha de aceptación: 20/07/2023
Fecha de publicación: 01/09/2023

Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.

Fernando Juca-Maldonado
E-mail: fjuca@umet.edu.ec
Orcid: https://orcid.org/0000-0001-7430-2157

Rolando Medina-Peña
E-mail: rolandormp74@gmail.com
Orcid: https://orcid.org/0000-0001-7530-5552

Universidad Metropolitana del Ecuador, sede Machala.

Cita sugerida (APA, séptima edición)

Juca-Maldonado, F., & Medina-Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas**.** Revista *Portal de la Ciencia*, 4(3), 325-337**,** DOI: https://doi.org/10.51247/pdlc.v4i3.394.

RESUMEN

La era digital ha dado lugar a la aparición de nuevos tipos de delitos, los ciberdelitos, que representan una amenaza creciente a la sociedad ecuatoriana. El presente estudio tiene como objetivo analizar los ciberdelitos en Ecuador y su impacto social. La metodología utilizada se basó en el análisis documental y la exegética, que facilitaron el estudio del marco legal para combatir este flagelo e interpretación de la información obtenida mediante una búsqueda rigurosa en fuentes especializadas relevantes y actualizadas, de esta forma se logró identificar los tipos de ciberdelitos más comunes en Ecuador, así como, las estrategias utilizadas por los delincuentes. Entre los resultados se destacan, el robo de información personal, el fraude en línea, los ataques informáticos a empresas y entidades públicas, la sextorsión y el ciberacoso. Se evidencia un aumento significativo de los ciberdelitos en el país, lo que requiere fortalecer las medidas de seguridad digital y promover la conciencia sobre los riesgos asociados. Se concluye que es necesario crear conciencia sobre la seguridad digital, fortalecer la capacidad de respuesta del gobierno, promover la investigación y desarrollo de tecnologías de seguridad cibernética, además de establecer una colaboración internacional contra los ciberdelitos.

Palabras claves: ciberdelitos, tipologías, seguridad digital

Cybercrime in Ecuador and its social impact; current outlook and future prospects

ABSTRACT

The digital era has given rise to the appearance of new types of crimes, cybercrimes, which represent a growing threat to Ecuadorian society. The objective of this study is to analyze cybercrime in Ecuador and its social impact. The methodology used was based on documentary and exegetical analysis, which facilitated the study of the legal framework to combat this scourge and interpretation of the information obtained through a rigorous search in relevant and updated specialized sources, in this way it was possible to identify the types of most common cybercrimes in Ecuador, as well as the strategies used by criminals. Among the results, the theft of personal information, online fraud, computer attacks on companies and public entities, sextortion and cyberbullying stand out. There is evidence of a significant increase in cybercrimes in the country, which requires strengthening digital security measures and promoting awareness of the associated risks. It is concluded that it is necessary to raise awareness about digital security, strengthen the government's response capacity, promote research and development of cybersecurity technologies, in addition to establishing international collaboration against cybercrime.

Keywords: cybercrimes, typologies, digital security

Cibercrime no Equador e seu impacto social; perspectivas atuais e perspectivas futuras

RESUMO

A era digital deu origem ao aparecimento de novos tipos de crimes, cibercrimes, que representam uma ameaça crescente para a sociedade equatoriana. O objetivo deste estudo é analisar o cibercrime no Equador e seu impacto social. A metodologia utilizada assentou na análise documental e exegética, o que facilitou o estudo do quadro legal de combate a este flagelo e a interpretação da informação obtida através de uma rigorosa pesquisa em fontes especializadas relevantes e atualizadas, desta forma foi possível identificar os tipos dos crimes cibernéticos mais comuns no Equador, bem como as estratégias utilizadas pelos criminosos. Entre os resultados destacam-se o roubo de informação pessoal, fraude online, ataques informáticos a empresas e entidades públicas, sextortion e cyberbullying. Há evidências de um aumento significativo de crimes cibernéticos no país, o que exige o fortalecimento das medidas de segurança digital e a promoção da conscientização sobre os riscos associados. Conclui-se que é preciso conscientizar sobre a segurança digital, fortalecer a capacidade de resposta do governo, promover a pesquisa e desenvolvimento de tecnologias de cibersegurança, além de estabelecer colaboração internacional contra o cibercrime.

Palavras-chave: cibercrimes, tipologias, segurança digital

INTRODUCCIÓN

Los avances de las telecomunicaciones y la informática, que experimenta la sociedad desde el pasado siglo XX, han dado paso a lo que conoce como era digital (Pérez-Rodríguez et al., 2015; Medina Cruz et al., 2018). Estas tecnologías han transformado todo el quehacer humano; hoy son otras las formas de comunicación, trabajo, estudio, comercio, etc. lo que reporta beneficios a favor del desarrollo económico y social (Ruiz, 2019).

Sin embargo, también han dado lugar a la aparición de nuevos tipos de delitos: los ciberdelitos (United Nations Office on Drugs and Crime [UNODC], 2013). En Ecuador, como en muchos otros países, los ciberdelitos son una amenaza presente que va en aumento (Narváez-Montenegro, 2019; Ortiz-Campos, 2019). Los ciberdelitos afectan a cualquier persona, pero, los grupos más vulnerables son los niños y adolescentes, quienes utilizan con mayor frecuencia las redes sociales y otras plataformas en línea. Además, las empresas y entidades públicas también son objetivos frecuentes de los ciberdelincuentes (Castillo-González, 2017; Montoya, 2017).

Estos actos delictivos no solo impactan económicamente, sino que también pueden tener consecuencias emocionales y psicológicas en las víctimas. La exposición de información personal y la difusión de imágenes o vídeos íntimos pueden generar sentimientos de vergüenza, miedo y ansiedad en las personas afectadas, lo cual puede, en algunos casos, culminar en decisiones fatales (Thackray et al., 2016; Bada & Nurse, 2019; Gómez & López, 2022). Ante esta realidad, se hace necesario realizar estudios del panorama actual de los ciberdelitos en Ecuador y su impacto en la sociedad, así como de las futuras perspectivas en materia de seguridad digital. De esta manera, se podrán identificar las estrategias más efectivas para prevenir y combatir los ciberdelitos en el país y proteger a la ciudadanía, especialmente a los grupos más vulnerables.

En consecuencia, se lleva a cabo la presente investigación con el objetivo de analizar los ciberdelitos en Ecuador y su impacto en la sociedad, con el fin de proporcionar información relevante y actualizada sobre el tema, que permita a las autoridades y a la ciudadanía en general tomar medidas efectivas para combatir este tipo de delito y proteger a la población. Igualmente, se busca conocer la situación actual del cibercrimen en Ecuador, los tipos de ciberdelitos más comunes, las principales estrategias utilizadas por los ciberdelincuentes y las medidas a tomar para contrarrestarlos (García, 2021).

El desarrollo del presente estudio se estructura en cuatro epígrafes, el primero de ellos se dedica a la aproximación a la noción de ciberdelito y sus características, en un segundo apartado se analiza el panorama actual de los ciberdelitos en el mundo, Latinoamérica y Ecuador, así como su impacto en la sociedad; en el tercero se expresan las prácticas utilizadas por los ciberdelincuentes; seguido por el cuarto y último epígrafe donde se identifican los tipos de ciberdelitos más frecuentes en Ecuador y su tratamiento en el Código Orgánico Integral Penal (COPI). Además, se abordan brevemente las medidas que se están tomando para prevenirlos y combatirlos, y se proponen recomendaciones para mejorar la seguridad digital y proteger a la población.

METODOLOGÍA

La metodología utilizada en esta investigación se fundamenta en la búsqueda y selección de fuentes de referencia sobre el estado del arte de los ciberdelitos a través de un proceso sistemático y riguroso para asegurar la calidad y relevancia de la información obtenida, siguiendo los procedimientos orientados por Bramer et al. (2017) y García et al. (2020) para la realización de revisiones sistemáticas de la literatura y las recomendaciones de Grant y Booth (2009), Moher et al. (2015) y Espinoza (2022) para la búsqueda de información en bases de datos a través de las herramientas de las tecnologías de la información y las comunicaciones (TIC). Tomando en cuenta estas consideraciones para la búsqueda, selección y análisis de la información se siguieron los siguientes pasos:

Paso 1

Se definió un conjunto de palabras clave relacionadas con el tema de investigación, tales como: "ciberdelitos", "cibercrimen", "seguridad digital", "delitos informáticos", "ciberseguridad", "ciberataques", "fraude electrónico", entre otros. Estas palabras clave se

utilizaron para realizar búsquedas en diferentes bases de datos con el auxilio de los motores de búsqueda: Google Scholar, Scopus, Web of Science, IEEE Xplore, entre otros.

Paso 2

Posteriormente, se aplicaron filtros de búsqueda para limitar los resultados a publicaciones relevantes y recientes, que se ajustaran a los objetivos de la investigación y estuvieran relacionados con los ciberdelitos en Ecuador y Latinoamérica. Para garantizar la calidad de las fuentes seleccionadas, se consideraron criterios de inclusión y exclusión, como la relevancia del título, el resumen y las palabras clave, la autoría, el año de publicación, la reputación de la revista científica y la calidad del estudio.

Paso 3

Se seleccionaron las fuentes más relevantes y actualizadas, las que facilitaron el contenido para la elaboración del artículo. Cabe mencionar que la búsqueda y selección de fuentes de referencia fue un proceso iterativo y continuo, que se ajustó y mejoró a medida que se avanzaba en la investigación y se identificaban nuevas fuentes de información relevante.

Paso 4

Una vez seleccionada la información se realizó su estudio, interpretación y síntesis con el auxilio del análisis documental. Por su parte la exegética facilitó el análisis e interpretación de las normas contenidas en el COIP relacionadas con este flagelo.

Paso 5

Con las síntesis elaboradas y con el apoyo del software EndNote versión 3.0 se confeccionó una base de datos referencial, la cual permitió la construcción del discurso escrito de este artículo.

Es importante acotar que la metodología aplicada en esta investigación es similar la empleada por Torres et al. (2021) en un estudio sobre ciberseguridad en Ecuador, en cuanto al uso de palabras clave y filtros de búsqueda para identificar fuentes relevantes en bases de datos especializadas. Sin embargo, la presten investigación se enfoca específicamente en los ciberdelitos y su impacto en la sociedad ecuatoriana, mientras que el estudio de Torres et al. (2021) se centra en la ciberseguridad y la protección de infraestructuras críticas.

DESARROLLO

1. Aproximación a la noción de ciberdelito y sus características

Los ciberdelitos son actividades ilícitas que se llevan a cabo en el ámbito digital y que están destinadas a generar beneficios económicos, políticos o personales para los delincuentes (Wall, 2007).

Según Alcívar et al. (2015), el término se utilizó por primera vez a finales de los años noventa del pasado siglo XX. En la medida que el uso de Internet se extendía, también surgían nuevos delitos que se cometían a través de las redes informáticas. Estos delitos se han convertido en un fenómeno global que afecta a todos los países, lo que representan importantes desafíos para la seguridad de la información y la privacidad de las personas (Choo, 2011).

En el Comprehensive Study on Cybercrime de la United Nations Office on Drugs and Crime (UNODC], 2013) se afirma que, en las legislaciones nacionales de los diferentes países se describen los ciberdelitos como "el acceso no autorizado a un sistema informático, o la interferencia con un sistema informático o de datos" (p.12).

De igual forma en el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se definieron los ciberdelitos de la siguiente manera:

> los actos comprendidos habitualmente en la categoría de "ciberdelincuencia" son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito (ONU, parr. 15).

De estas definiciones se desprende una de las características principales de los ciberdelitos, el empleo por parte de los delincuentes de las herramientas y recursos que ofrece el entorno digital para llevar a cabo sus objetivos. Los delincuentes utilizan técnicas como el phishing, el malware, el ransomware, entre otras, para acceder a sistemas informáticos y robar información confidencial o extorsionar a los usuarios (Anderson et al., 2013).

También, entre las principales características de los ciberdelitos se encuentra el anonimato. Los delincuentes utilizan técnicas de enmascaramiento de su identidad para evitar ser detectados por las autoridades (Yar, 2005). Además, los ciberdelitos suelen ser muy sofisticados y requieren un alto nivel de conocimientos técnicos por parte de los delincuentes, lo que hace que la investigación y la persecución de estos delitos sean aún más complicadas (McGuire, 2018).

Los ciberdelitos también presentan una gran variedad de objetivos y modalidades. Algunos delitos se enfocan en el robo de información financiera, mientras que otros buscan manipular la opinión pública o acceder a información confidencial de empresas y organizaciones (Leukfeldt, 2017). También, existen delitos que buscan el acoso, la difamación y/o el chantaje de individuos (Furnell, 2010).

2. Situación actual del ciberdelito

La proliferación de los ciberdelitos ha generado una gran preocupación a nivel global. Los costos económicos y sociales de estos delitos son cada vez mayores, y afectan no solo a las empresas y organizaciones, sino también a los individuos y a la sociedad en su conjunto (Kshetri, 2010). Además, la rápida evolución de las tecnologías digitales y la aparición de nuevas formas de delitos digitales plantean importantes desafíos para las autoridades y para la sociedad en general (Europol, 2020). El creciente uso de las TIC, así como esta constante y rápida evolución de sus herramientas y recurso permite que los delitos informáticos sean cada vez más sofisticados y difíciles de detectar (Wall, 2007).

En respuesta a este problema, se han desarrollado diversas estrategias para prevenir y combatir los ciberdelitos. Estas estrategias incluyen la mejora de la seguridad de los sistemas informáticos, la educación y concientización de los usuarios sobre los riesgos de seguridad en línea, el fortalecimiento de la cooperación internacional para la persecución de delitos transnacionales y la mejora de la legislación en materia de ciberdelitos. La globalización y la interconexión de las redes informáticas han hecho que estos delitos trasciendan fronteras y se conviertan en un problema internacional (Castells, 2015); es por eso que, cada uno de los países implementa leyes y regulaciones específicas para abordar los ciberdelitos (Choo & Smith, 2008).

La ciberdelincuencia es un fenómeno global que ha estado presente desde la popularización de la informática y la conectividad en la década de 1980 (Thomas & Loader, 2000). El primer caso documentado de un ataque cibernético se remonta a 1986, cuando un estudiante alemán de informática infectó la red de la NASA con un virus informático (Clough, 2010). Desde entonces, la ciberdelincuencia ha evolucionado significativamente; en la actualidad se estima que se producen más de 4.000 ataques cibernéticos por día en todo el mundo (Symantec, 2021); esto se traduce en un promedio de más de 1,5 millones de ataques al año, y la cifra sigue aumentando.

En términos estadísticos, según el Informe de Amenazas de Seguridad de Internet de Symantec del año 2021, se detectaron más de 5,6 mil millones de ataques cibernéticos en todo el mundo en el 2020, esto representa un aumento del 40% en comparación con el año

anterior. Asimismo, según el mismo informe, los ataques de ransomware aumentaron un 62% en el 2020 respecto al año 2019 y se registraron más de 304 millones de intentos de phishing (Symantec, 2021).

En cuanto a las víctimas, el sector empresarial es el más afectado por los ciberataques (Verizon, 2020), aunque también se han registrado casos de ataques a gobiernos y organizaciones sin fines de lucro (Choo & Smith, 2008). En promedio, una empresa tarda unos 280 días en detectar y contener un ataque cibernético (Ponemon Institute, 2021), lo que puede tener consecuencias económicas y reputacionales graves.

En medio de esta situación, se espera que, la ciberdelincuencia continúe aumentando en la medida en que se amplíe la conectividad y se adopten nuevas tecnologías (Choucri & Clark, 2013; Goodman, 2015). Por esta razón, es esencial que los gobiernos y las organizaciones implementen medidas de seguridad y concientización para reducir el riesgo de ataques y minimizar su impacto en caso de producirse (McGuire & Dowling, 2013).

En Latinoamérica, varios países han adoptado leyes y normativas para prevenir y sancionar los ciberdelitos. En Ecuador, el COIP es el marco legal que regula los delitos informáticos. Este código establece sanciones penales para diversas conductas, como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones electrónicas, la difusión de virus informáticos, el acoso por medios digitales, entre otros (Solines, 2014). Además, instaura la creación de la Unidad de Investigaciones Tecnológicas y de Telecomunicaciones (UITT) dentro de la Policía Nacional, cuya función es la investigación de los delitos informáticos. Asimismo, el código instituye la obligación de las empresas de proveer servicios de internet de colaborar con las autoridades en la investigación de delitos informáticos.

Por otro lado, en el ámbito regional, la Organización de los Estados Americanos (OEA, 2004) ha desarrollado el "Modelo Interamericano de Legislación sobre Delitos Informáticos", que sirve como guía para los países miembros en la elaboración de leyes y políticas para combatir los ciberdelitos. Este modelo establece los principios fundamentales para la prevención, investigación y sanción de los delitos informáticos, y promueve la cooperación internacional en la lucha contra los mismos.

Por lo cual, se puede reafirmar que, en Latinoamérica y Ecuador se han desarrollado leyes y normativas específicas para combatir los ciberdelitos (Barrios & Soria, 2018). Estas leyes instituyen sanciones penales para diversas conductas delictivas y establecen la creación de unidades especializadas en la investigación de delitos informáticos (Solines, 2014). Asimismo, existe una guía regional que promueve la cooperación internacional en la lucha contra los ciberdelitos (OEA, 2004). Es importante fortalecer el marco legal y normativo para prevenir y combatir los ciberdelitos, ya que estos aun representan un desafío para la seguridad digital y la protección de los derechos de los ciudadanos (Bello, 2016; Primicias, 2019).

Según un informe de la compañía de seguridad informática Kaspersky (2021), en 2020 se registraron más de 1,4 millones de ataques de phishing en América Latina, lo que representa un aumento del 27,5% en comparación con el año anterior. En el mismo informe, Brasil y México lideran la lista de países latinoamericanos con mayor cantidad de ataques de phishing, seguidos de Perú, Colombia y Chile.

La pandemia de COVID-19 ha sido aprovechada por los ciberdelincuentes para aumentar su actividad delictiva en Latinoamérica. Según un informe de la empresa de seguridad informática ESET (2021), en 2020 se registró un aumento del 124% en la cantidad de ataques informáticos en la región.

En Ecuador, el número de denuncias de ciberdelitos ha ido en aumento en los últimos años. Según Pazan (2022), en la Fiscalía General del Estado en el año 2019 se registraron 718 denuncias por delitos informáticos, mientras que en el 2020 se registraron 1.030 denuncias,

las cuales aumentaron a 1.851 en el año 2021 y en poco más de seis meses del 2022 la policía ya había iniciado 650 nuevas investigaciones en todo el país; las cifras evidencian un incremento considerable durante el tiempo de pandemia del COVID-19.

3. Tipos de prácticas de los ciberdelitos

Entre las prácticas más comunes y peligrosas de los ciberdelitos se encuentran: el phishing, el ransomware y los ataques Denial of Service o DDoS (Radware, 2021):

- El phishing es una técnica que consiste en engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios (Jagatic et al., 2007).
- El ransomware, por su parte, es un tipo de malware que cifra los archivos del usuario y exige un rescate para recuperarlos (Kovacs, 2016).
- Por último, los ataques DDoS buscan saturar un servidor con una gran cantidad de solicitudes, lo que provoca su caída y la interrupción del servicio (Mirkovic y Reiher, 2004).

4. Tipos de ciberdelitos más comunes en Ecuador

En cuanto a los tipos de ciberdelitos más comunes en Ecuador, destacan (Fiscalía General del Estado, 2020; Aparicio-Izurieta, 2022):

- Robo de información personal.

  Los ciberdelincuentes utilizan técnicas como el phishing y el malware para obtener datos confidenciales de sus víctimas, como contraseñas, números de tarjetas de crédito, entre otros.

- Fraude en línea.

  Los delincuentes utilizan sitios web falsos, correos electrónicos fraudulentos y mensajes de texto para engañar a las personas y obtener su dinero. Por ejemplo, pueden hacerse pasar por bancos o entidades gubernamentales y solicitar información personal o pagos.

- Ataques informáticos a empresas y entidades públicas.

  En los últimos años, se han registrado varios ataques informáticos a empresas y entidades públicas en Ecuador. En 2019, por ejemplo, se registró un ataque cibernético a la Contraloría General del Estado, que afectó a más de 16.000 cuentas de correo electrónico.

- Sextorsión.

  La sextorsión es otra modalidad de ciberdelito que ha ido en aumento en Ecuador en los últimos años. Consiste en el chantaje a través de la obtención de imágenes o videos íntimos de la víctima, que son utilizados para extorsionarla.

- Ciberacoso.

  Esta forma de delito informático afecta a niños y adolescentes en Ecuador. Los acosadores utilizan las redes sociales y otras plataformas en línea para intimidar, hostigar o amenazar a sus víctimas.

Vale la pena señalar de que cada una de estas y otras modalidades de ciberdelitos en el Ecuador están tipificadas en el COIP, órgano encargado de sancionar estas infracciones, entre las cuales se encuentran las relacionadas en la siguiente tabla 1:

Tabla 1. Delitos más comunes y su sanción en el artículo respectivo

Descripción	Artículo	Sanción (años de prisión)
Pornografía infantil	103	13 a 16
Violación del derecho a la intimidad	178	1 a 3
Revelación ilegal de información de bases de datos	229	1 a 3
Interceptación de comunicaciones	476	3 a 5
Ataque a la integridad de sistemas informáticos	232	3 a 5
Delitos contra la información pública reservada legalmente	233	3 a 5
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	234	3 a 5

Fuente: Asamblea Nacional (2021). COIP

En resumen, el análisis de la información recaudada en esta investigación reveló que los ciberdelitos en Ecuador han aumentado significativamente en los últimos años, convirtiéndose en una de las principales amenazas para la seguridad digital en el país; delitos que son perpetrados por ciberdelincuentes tanto locales como internacionales que afectan a empresas y particulares por igual, tal como se evidencia en los estudios de Pérez et al. (2020) y Rosero (2020).

En cuanto a las medidas que se están tomando, para prevenir y combatir los ciberdelitos en Ecuador, se han implementado una serie de iniciativas y políticas públicas que buscan fortalecer la seguridad digital en el país. Sin embargo, la investigación reveló que estas medidas son insuficientes y requieren de una mayor inversión y capacitación en tecnologías de la información y seguridad cibernética, tal como lo indica Ochoa y Valenzuela (2021), sobre lo ciberdelitos en México y, Silva y López (2019), en Colombia.

CONCLUSIONES

Las averiguaciones realizadas permiten concluir que:

- En Ecuador los ciberdelitos han aumentado significativamente en los últimos años, convirtiéndose en una de las principales amenazas para la seguridad digital en el país; situación que también aumento en la región, por lo que es necesario fortalecer la capacidad de respuesta de los gobiernos y promover la concienciación sobre la seguridad digital en la sociedad.
- Los principales tipos de prácticas de los ciberdelitos son el phishing, el malware, el ransomware y el robo de identidad, que son perpetrados por ciberdelincuentes tanto locales como internacionales, y afectan a empresas y particulares. Estas estrategias son cada vez más avanzadas y difíciles de detectar, lo que hace que los ciberdelincuentes puedan operar de manera más efectiva y rentable.
- En Ecuador se implementa iniciativas y políticas públicas para fortalecer la seguridad digital en el país. Sin embargo, estas medidas son insuficientes y requieren de una mayor inversión y capacitación en tecnologías de la información y seguridad cibernética.
- Es preciso establecer una colaboración internacional para prevenir y combatir los ciberdelitos.
- Es necesario crear conciencia y educación sobre la importancia de la seguridad digital en la sociedad ecuatoriana.

Los ciberdelitos son una amenaza cada vez más presente en la sociedad y requieren de una atención inmediata y continua. La investigación realizada aporta información valiosa sobre el panorama actual de los ciberdelitos en el país, así como sobre las medidas necesarias para prevenir y combatir estos delitos.

Limitaciones del estudio y direcciones futuras de investigación

Es importante también tener presente las limitaciones del estudio ya que la investigación se centró en fuentes de información en línea y no se consideraron otras fuentes, como entrevistas a expertos o encuestas a la población. Así también, la cantidad de información disponible sobre ciberdelitos en Ecuador podría ser limitada, especialmente en lo que respecta a datos oficiales y las estrategias utilizadas por los ciberdelincuentes pueden cambiar con frecuencia, lo que significa que los datos y conclusiones obtenidos pueden no ser aplicables a largo plazo.

En cuanto a las posibles direcciones futuras de investigación, podrían realizarse encuestas y entrevistas a la población para conocer su percepción y experiencia con respecto a los ciberdelitos; analizar los casos de ciberdelitos resueltos y los métodos utilizados para capturar a los delincuentes; examinar las políticas y estrategias de otros países en la lucha contra los ciberdelitos y evaluar su aplicabilidad en el contexto de Ecuador y estudiar el impacto económico de los ciberdelitos en Ecuador y su relación con el desarrollo tecnológico del país.

RECONOCIMIENTO

Los autores reconocen y agradecen la ayuda prestada por los colegas, quienes a través de sus críticas y sugerencias contribuyeron a la realización exitosa de este trabajo.

CONTRIBUCIÓN DE LOS COAUTORES

Cuadro resumen de la contribución de los coautores

Coautor	Responsabilidad
Fernando Juca Maldonado	Determinar el tema y objetivo de trabajo. Análisis, interpretación y resumen de los textos seleccionados. Elaboración de la base de datos referencial. Redacción del artículo.
Rolando Medina Peña	Búsqueda y recuperación de los materiales bibliográficos utilizados. Selección de los materiales bibliográficos según valor científico y actualidad. Análisis, interpretación y síntesis de los materiales bibliográficos seleccionados. Revisión final de la redacción del artículo.

REFERENCIAS

Alcívar, C., Domenech, G., & Ortíz, C. (2015). La seguridad jurídica frente a los delitos informáticos. *Avances*, 10(12), 41-57.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., ... & Savage, S. (2013). *Measuring the cost of cybercrime. The economics of information security and privacy* (pp. 265-300). Springer, Berlin: Heidelberg.

Aparicio-Izurieta, V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. *Sapienza*. *International Journal of Interdisciplinary Studies*, 3(1), 1057-1063. https://doi.org/10.51798/sijis.v3

Asamblea Nacional (17 de febrero del 2021). *Código Orgánico Integral Penal (COIP)*. Ley 0, Registro Oficial Suplemento 180 de 10-feb.-2014 (última modificación 17/02/2021). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Bada, M., & Nurse, J. R. C. (2019). *The Social and Psychological Impact of Cyber-Attacks*. https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf

Barrios, E., & Soria, C. (2018). Ciberseguridad en América Latina: un análisis comparativo de la legislación en Argentina, Brasil, Chile, Colombia, Ecuador, México y Perú. *Revista Chilena de Derecho y Tecnología*, 7(1), 1-39.

Bello, S. E. (2016). *Cybersecurity and human rights in the age of cyberveillance*. Editorial Rowman & Littlefield Publishers https://www.amazon.com/Cybersecurity-Human-Rights-Age-Cyberveillance/dp/1442260416

Bramer, W. M., Rethlefsen, M. L., Kleijnen, J., & Franco, O. H. (2017). Optimal database combinations for literature searches in systematic reviews: a prospective exploratory study. *Systematic Reviews*, 6(1), 245.

Castells, M. (2015). *The rise of the network society: The information age: Economy, society, and culture (Vol. 1)*. John Wiley y Sons. h https://deterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

Castillo-González, G. (2017). *Plan de continuidad del negocio basado en servicios en la nube para el área de tecnología*, Universidad Galileo, Guatemala. http://biblioteca.galileo.edu/tesario/handle/123456789/578

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers y Security*, 30(8), 719-731.

Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology*, 3(1), 37-59.

Choucri, N., & Clark, D. D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists,* 69(5), 21-31.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

ESET (2021). *Security report LATAM 2021*. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Espinoza-Freire, E. E. E. (2022). El problema, el objetivo, la hipótesis y las variables de la investigación. *Portal de la Ciencia*, *1*(2), 1-71.

Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. European Union Agency for Law Enforcement Cooperation. Europol. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Fiscalía General del Estado. (2020). *Fiscalía General del Estado | Cifras de robos*. https://www.fiscalia.gob.ec/estadisticas-de-robos

Furnell, S. (2010). *Cybercrime: Vandalizing the information society*. Addison-Wesley Longman Publishing Co., Inc. https://www.semanticscholar.org/paper/Cybercrime%3A-Vandalizing-the-Information-Society-Furnell/705861aa64d6b6de0a681f8999a55874fbd48ebd

García-Campos, N. P. (2021). La atipicidad de la violación con fines pornográficos en el código orgánico integral penal ecuatoriano. *Sociedad & Tecnología*, *4*(S1), 1–12. https://doi.org/10.51247/st.v4iS1.110

García, L., Pérez, M. A., & Villagrán, J. M. (2020). Metodologías para la realización de revisiones sistemáticas de la literatura. *Anales de Documentación*, 23(1).

Gómez-Barroso, F. B., & López-Soria, Y. (2022). La perfilación criminal como herramienta forense en la investigación de delitos contra la vida. Ecuador. *Sociedad & Tecnología*, *5*(2), 365–378. https://doi.org/10.51247/st.v5i2.220

Goodman, M. (2015). *Los delitos del futuro. Traducción de Gemma Deza Guil*. España: Editorial Planeta S.A

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91-108.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., y Menczer, F. (2007). Social phishing. *Communications of the ACM,* 50(10), 94-100.

Kaspersky. (2021). *Kaspersky Security Bulletin 2020/2021*. https://securelist.com/files/2021/02/KSB-2020_2021_ENG.pdf

Kovacs, E. (2016). The evolution of ransomware. *Symantec Security Response.https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf*

Kshetri, N. (2010). The global cyber-crime industry: Economic, institutional and strategic perspectives. *Springer Science & Business Media. https://www.researchgate.net/publication/285998465_The_global_cybercrime_industry_Economic_institutional_and_strategic_perspectives*

Leukfeldt, R. (2017). *Research agenda the human factor in cybercrime and cybersecurity*. [S.l.]: Eleven International Publishing.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. *Home Office Research Report,* 75.

Medina-Cruz, H., Lagunes-Domínguez, A., & Torres-Gastelú, C. (2018). Percepciones de Estudiantes de Nivel Secundaria sobre el uso de las TIC en su Clase de Ciencias, *Información Tecnológica,* 29(4), 259-266. doi.org/10.4067/S0718-07642018000400259

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2015). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: *The PRISMA Statement*. *PLoS Medicine,* 6(7).

Montoya, B. (2017). *¿Cómo minimizar el riesgo de afectación de un ataque cibernético en los blancos estratégicos nacionales*? http://hdl.handle.net/10654/15693

Narváez-Montenegro, B. D., & Recalde-Machado, G. E. (2018). El delito informático en América. *Debate Jurídico Ecuador*, 1(1), 3-14.

Ochoa, S., & Valenzuela, C. (2021). Ciberdelitos en México: análisis de la evolución y perspectivas de la ciberseguridad. *Revista Mexicana de Investigación en Ciberseguridad,* 1(1), 10-22.

Organización de las Naciones Unidad. ONU. (2015). *El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución,*

como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional. [Documento de antecedentes. 13º Congreso de Naciones Unidas sobre Prevención del Delito y Justicia Penal] Doha. A/CONF.222/12

Organización de los Estados Americanos. OEA. (2004). *Modelo Interamericano de Legislación sobre Delitos Informáticos*. http://www.oas.org/juridico/spanish/cyber_mod_leg_inf_delitos.pdf

Ortiz-Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos 21*, 4(1), 100-111.

Pazan, C. (2022). *3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. El Comercio. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Pérez-Rodríguez, M., Delgado-Ponce, A., García-Ruiz, R., & Caldeiro, M. (2015). *Niños y jóvenes ante las redes y pantallas*, Barcelona: Gedisa.

Pérez, G., Morales, J., & González, R. (2020). Ciberdelitos y ciberseguridad en América Latina: un análisis comparativo de políticas públicas y marcos regulatorios. *Revista de Investigación en Ciberseguridad*, 4(2), 18-30.

Ponemon Institute. (2021). *Cost of a Data Breach Report 2021*. https://www.ponemon.org/library/cost-of-a-data-breach-report

Primicias. (2019). Ecuador es uno de los tres países de la región donde falta una ley que proteja los datos personales. *Primicias* https://www.primicias.ec/noticias/tecnologia/ecuador-desprotegido-leydatos-personales

Radware. (2021). *Global application and network security report 2021*. https://www.radware.com/lp/global-application-network-security-report/

Rosero, A. (2020). *Los robos cibernéticos encienden las alertas en Ecuador.* https://www.elcomercio.com/actualidad/robos-ciberneticos-alertasecuador-denuncias.html

Ruiz, A. (2019). Competencia digital y TICs en interpretación: «renovarse omorir». *EDMETIC, Revista de Educación Mediática y TIC*, 8(1), 55-71. DOI: https://doi.org/10.21071/edmetic.v8i1.1106

Silva, M., & López, D. (2019). Análisis de la situación de los ciberdelitos en Colombia: un enfoque desde la perspectiva del marco normativo y la ciberseguridad. *Revista Colombiana de Derecho y Tecnología*, 2(1), 47-65.

Solines, M. (2014). La ciberdelincuencia en el Código Orgánico Integral Penal del Ecuador. *Revista de la Facultad de Derecho de México*, 64(254), 249-273.

Symantec. (2021). *Internet Security Threat Report 2021*. https://www.symantec.com/security-center/threat-report

Thackray, H. y otros (2016). *Social Psychology: An under-used tool in Cybersecurity*. http://eprints.bournemouth.ac.uk/25051/1/Social%20Psychology%20-%20An%20under-used%20tool%20in%20Cybersecurity.pd

Thomas, D., & Loader, B. (Eds.). (2000). *Cybercrime: Law enforcement, security and surveillance in the information age. Routledge*.https://www.routledge.com/Cybercrime-Law-enforcement-security-and-surveillance-in-the-information/Loader-Thomas/p/book/9780415213264

Torres, R., Sandoval, S., & Cevallos, J. (2021). Ciberseguridad en Ecuador: protección de infraestructuras críticas y desafíos en la era digital. *Revista de Investigación y Desarrollo en Tecnologías de la Información y Comunicación*, 2(1), 45-60.

United Nations Office on Drugs and Crime [UNODC]. (2013). *Comprehensive Study on Cybercrime* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Verizon (2020). *Informe de Verizon sobre investigaciones de fugas de datos 2020. Guía rápida para los CISO*. https://es.sentinelone.com/blog/the-cisos-quick-guide-to-verizons-2020-data-breach-investigations-report/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age. Polity.* https://www.wiley.com/en-ie/Cybercrime:+The+Transformation+of+Crime+in+the+Information+Age-p-9780745627359

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology,* 2(4):407 427.