Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VIII. Vol. VIII. N° 3. Edición Especial 3. 2023
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

https://doi.org/10.35381/racji.v8i3.3116

Cibercrimen y ciberseguridad: protegiendo el futuro digital, Babahoyo, Ecuador

Cybercrime and cybersecurity: protecting the digital future, Babahoyo, Ecuador

Domenica Vishely Pico-Verdezoto
domenicaverdezoto11@gmail.com
Universidad Regional Autónoma de los Andes, Babahoyo, Los Ríos
Ecuador
https://orcid.org/0009-0000-9680-7105

Christian Emmanuel Bohorquez-Rizzo
christianbr55@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Babahoyo, Los Ríos
Ecuador
https://orcid.org/0009-0000-6123-6779

Sthefanie Alexandra Delgado-Jiménez
sthefanie172022@gmail.com
Universidad Regional Autónoma de los Andes, Babahoyo, Los Ríos
Ecuador
https://orcid.org/0009-0007-0472-6385

Troya Terranova Katherine-Tatiana
ub.katherinett77@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Babahoyo, Los Ríos.
Ecuador
https://orcid.org/0009-0005-8609-390X

Recepción:20 de septiembre 2022
Revisado: 15 de octubre 2022
Aprobación: 15 de diciembre 2022
Publicación: 15 de enero 2023

RESUMEN

El objetivo general de la investigación fue analizar jurídicamente el Cibercrimen y ciberseguridad: Protegiendo el Futuro Digital, Babahoyo, Ecuador. El planteamiento realizado por los investigadores para el desarrollo del método, fue a partir del enfoque cuantitativo, mediante la indagación, recolección y análisis crítico documental y referencial bibliográfico, basándose en la exploración metódica, rigurosa y profunda de diversas fuentes documentales conformadas por artículos, tesis, normas y leyes entre otros, describiendo los hallazgos encontrados. Se recurrió, además, al método inductivo-deductivo. Además, se aplica un cuestionario. Se concluye que, Ecuador no cuenta con un instrumento legal que emita lineamientos para gestionar los riesgos cibernéticos y proteger las infraestructuras críticas de manera integral desde una perspectiva nacional, en colaboración y coordinación con los sectores público y privado, la academia y la sociedad civil.

Descriptores: Cibercrimen; derecho a la informática; acceso a la información. (Tesauro UNESCO).

ABSTRACT

The general objective of the research was to legally analyze Cybercrime and cybersecurity: Protecting the Digital Future, Babahoyo, Ecuador. The approach taken by the researchers for the development of the method was based on the quantitative approach, through inquiry, collection and critical analysis of documents and bibliographic references, based on the methodical, rigorous and in-depth exploration of various documentary sources consisting of articles, theses, regulations and laws, among others, describing the findings. The inductive-deductive method was also used. In addition, a questionnaire was applied. It is concluded that Ecuador does not have a legal instrument that issues guidelines to manage cyber risks and protect critical infrastructures in a comprehensive manner from a national perspective, in collaboration and coordination with the public and private sectors, academia and civil society.

Descriptors: Cybercrime; right to information technology; access to information. (UNESCO Thesaurus).

INTRODUCCIÓN

En la era digital actual, el Ayuntamiento de Babahoyo se enfrenta a un problema creciente de ciberdelincuencia y a la necesidad urgente de reforzar suciberseguridad para asegurar su futuro digital. Los rápidos avances tecnológicos y la proliferación de Internet y los dispositivos conectados han abierto nuevas oportunidades para que los ciberdelincuentes exploten las vulnerabilidades de los ciudadanos y las organizaciones. La falta de concienciación y preparación en materia de ciberseguridad, así como la ausencia de políticas y normativas eficaces,exponen a Babahoyo a diversas formas de ciberataques, entre ellos: robo de datospersonales y financieros, fraude en línea y violación de la privacidad. Protección dedatos: en caso de que se produzca un acto fraudulento, es posible que éste esté relacionado con la protección de datos personales. Esta situación supone una graveamenaza para la estabilidad y sostenibilidad de la Ciudad, ya que un entorno digitalinestable puede socavar la confianza pública, repercutir negativamente en la economía local e impedir el progreso tecnológico. La ausencia de una definición específica se demuestra a partir de las diferentes denominaciones que reciben este tipo de conductas, “delitos informáticos”, “crímenes cibernéticos” “delitos relacionados con computadoras” “delitos electrónicos”, “crímenes por computadoras”, “cibercrimen”, “delitos telemáticos”, entre otros (Sain, 2012).

En el 2017 se registraron 8.421 casos; subieron a 9.571 y 10.279 en 2018 y 2019. Estas son las cifras de las denuncias. La tendencia se mantiene. Dentro de este artículo se menciona que los más recurrentes son las estafas digitales con modalidades como la suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos. (El Universo, 2021).

El problema de la ciberdelincuencia y la ciberseguridad en Babahoyo requiere una atención inmediata y medidas concretas por parte de las partes interesadas. Es necesario establecer y reforzar normativas y políticas que promuevan la ciberseguridad en los sectores público y privado. Esto incluye trabajar en estrecha colaboración con las administraciones locales, las empresas, las instituciones educativas y la sociedad civil para desarrollar estrategias integrales de prevención,

detección y respuesta a los incidentes cibernéticos. También debemos invertir en tecnologías de seguridad avanzadas y en la formación de profesionales de la ciberseguridad para proteger eficazmente los sistemas y datos de la ciudad. Solo a través de un enfoque integral y colaborativo podremos avanzar en la protección del futuro digital de la ciudad de Babahoyo y garantizar un entorno en línea seguro para todos los ciudadanos.

El compromiso del Ecuador con la ciberseguridad ha progresado recientemente con la adopción de varias políticas y estrategias sectoriales que definen el enfoque del gobierno con respecto a la ciberseguridad. Dichas estrategias precisan de coordinación general. Cabe resaltar que más allá de la ausencia de marcos reglamentarios a nivel nacional para la protección de infraestructura crítica, los sectores financieros y de telecomunicaciones han establecido y adoptado procesos de gestión de riesgos de ciberseguridad y las mejores prácticas en medidas de seguridad.

La Constitución de 2008 se establece como la norma jurídica de mayor jerarquía dentro del ordenamiento jurídico ecuatoriano, primando inclusive sobre los convenios ytratados internacionales salvo excepciones en casos de derechos humanos más beneficiosos, leyes orgánicas y ordinarias, así como las demás normas. Los cuales se pueden mencionar: Artículos. 3, 16, 66 (Núm. 19 y 21), 158, 313 y 393.

Así mismo, el Código Orgánico Integral Penal. (2014), a menudo referido por sus siglas COIP, es un conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, es decir un compendio legislativo que establece delitos y penas conforme al sistema penal ecuatoriano. Artículos: 103, 104, 170, 178, 188, 190, 194, 202.1, 202.2, 229 al 234, 262, 353.1, 415.1,415.2, 472, 476, 526, 553.

En este mismo tenor, Ley Orgánica de Comercio Electrónico, Firmas, electrónicas y Mensajes de Datos. Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. Artículos: 5, 7,8, 9,10, 29, 51, 54, 58, 62, 63, 64.

Además, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e innovación. Protección a los derechos intelectuales y a asumir la defensa de estos, como un aspecto imprescindible para el desarrollo tecnológico del país. La ley, incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software).
En la presente investigación se plantea como objetivo general analizar jurídicamente el Cibercrimen y ciberseguridad: Protegiendo el Futuro Digital, Babahoyo, Ecuador.

MÉTODO

El planteamiento realizado por los investigadores para el desarrollo del método es a partir del enfoque cuantitativo, mediante la indagación, recolección y análisis crítico documental y referencial bibliográfico, basándose en la exploración metódica, rigurosa y profunda de diversas fuentes documentales conformadas por artículos, tesis, normas y leyes entre otros, describiendo los hallazgos encontrados. En la investigación, se ha empleado como técnica la revisión documental, la cual permite obtener información valiosa para encuadrar los acontecimientos, problemas y reacciones más usuales de personas y culturas que son objeto de análisis (Sánchez et al, 2021). Se recurrió, además, al método inductivo-deductivo, el cual propone que para hallar una verdad se deben escudriñar los hechos y no basarse en meras especulaciones, igualmente a partir de afirmaciones generales para llegar a las específicas (Dávila, 2006). Además, se aplica un cuestionario.

RESULTADOS

Se presentan a continuación los resultados obtenidos luego del desarrollo del método, planteado por los investigadores.

1. ¿Cuáles son los posibles delitos cibernéticos que pueden llevar a la exploración de la responsabilidad legal?

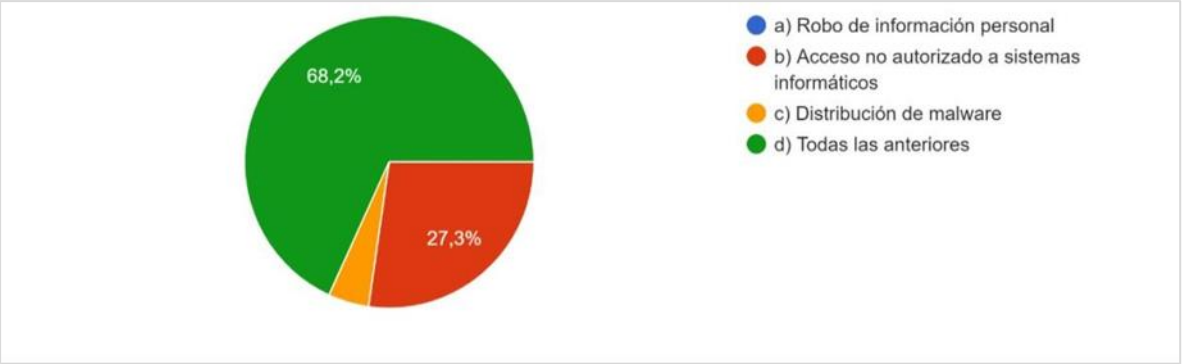

Figura 1. Delitos cibernéticos.
Elaboración: Los autores.

Los porcentajes de respuesta indican que una mayoría abrumadora de los encuestados (68,2%) considera que todos los delitos cibernéticos mencionados(robo de información personal, acceso no autorizado a sistemas informáticos y distribución de malware) pueden llevar a la responsabilidad legal. Además, una proporción considerable (27,3%) también considera el acceso no autorizado a sistemas informáticos como un delito cibernético que puede llevar a laresponsabilidad legal, mientras que una minoría (4,5%) considera la distribución demalware como tal.

2. ¿Cuál es el marco legal que rige la responsabilidad en casos de delitos cibernéticos?

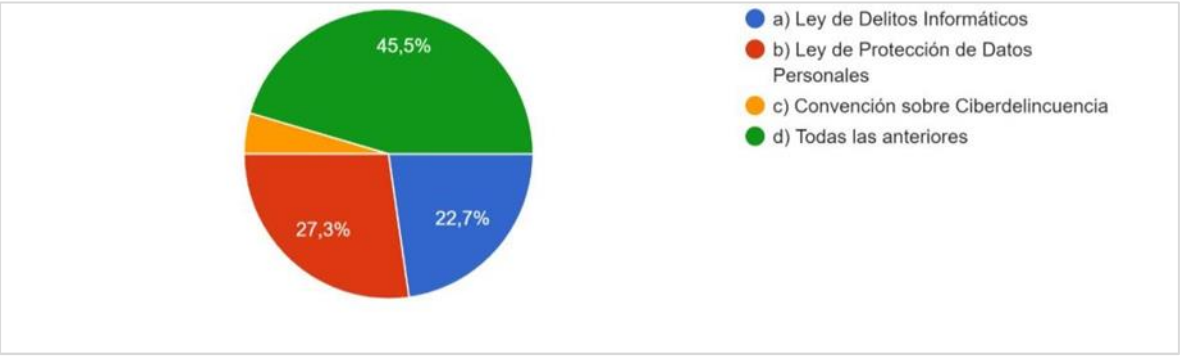

Figura 2. Responsabilidad de delitos.
Elaboración: Los autores

La mayoría de los encuestados (45%) considera que todas las opciones presentadas son parte del marco legal que rige la responsabilidad en casos de delitos cibernéticos, seguido por una alta proporción (22,7%) que reconoce la importancia de la opción b) "Ley de Protección de Datos Personales" y una proporción menor (22,7%) que destaca la relevancia de la opción a) "Ley de Delitos Informáticos". La opción c) "Convención sobre Ciberdelincuencia" es la opción menos mencionada en este análisis (4,5%).

3. ¿Qué factores se consideran al determinar la responsabilidad legal en casos de delitos cibernéticos?

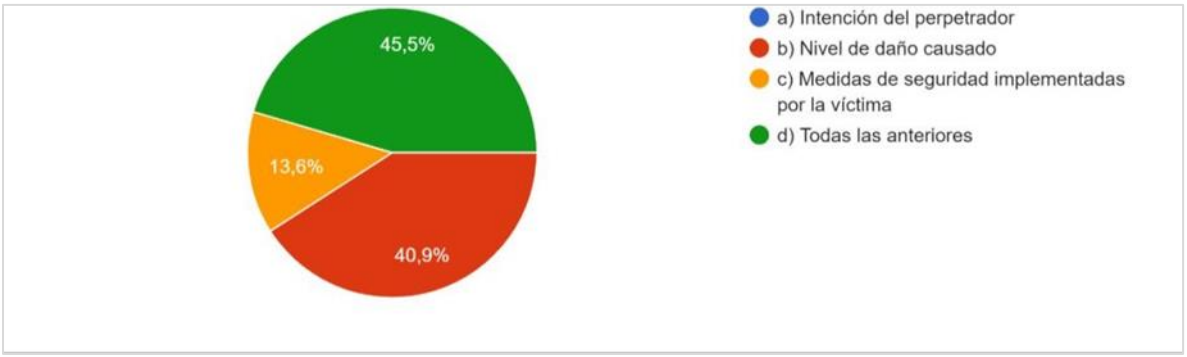

Figura 3. Responsabilidad legal en delitos cibernéticos.
Elaboración: Los autores.

La opción más elegida fue d) "Todas las anteriores" (45,5%), seguida por la opción a) "Intención del perpetrador" (40,9%), y luego la opción b) "Nivel de daño causado" (13,6%) y la opción c) " Medidas de seguridad implementadas por la víctima" (13,6%). Estos resultados indican que la mayoría de las personas consideran que todos los factores mencionados son importantes al determinar la responsabilidad legal en casos de delitos cibernéticos.

4. ¿Qué acciones pueden tomar las víctimas de delitos cibernéticos para proteger sus derechos legales?

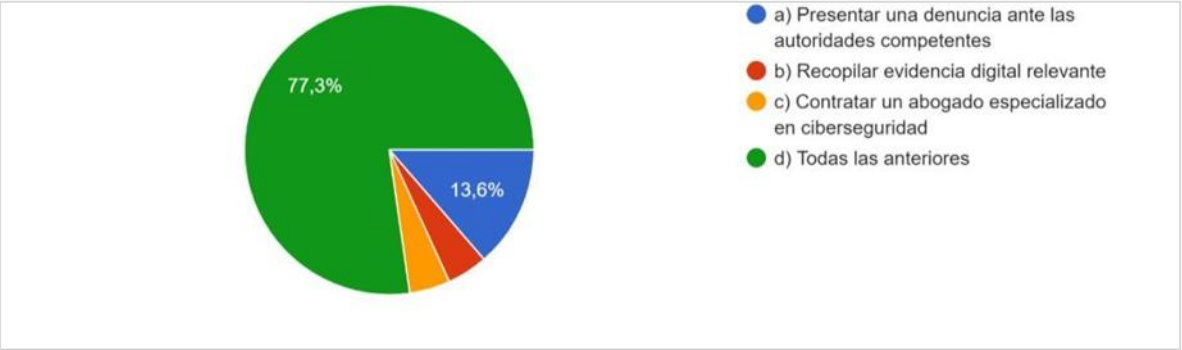

Figura 4. Derechos legales.
Elaboración: Los autores.

La opción más elegida fue la d) "Todas las anteriores" con un (77,3%) de respuestas. Esto sugiere que la mayoría de las personas considera que tomar todas las acciones mencionadas es importante para proteger sus derechos legales en caso de ser víctimas de delitos cibernéticos. La opción a) "Presentar una denuncia ante las autoridades competentes" recibió un (13,6%) de respuestas, lo que indica que una parte significativa de las personas reconoce la importancia de denunciar el delito a las autoridades correspondientes. Las opciones b) "Recopilar evidencia digital relevante" y c) "Contratar un abogado especializado en ciberseguridad" adquirió cada una un (4.5%) de respuestas. Esto sugiere que un pequeño porcentaje de personas reconoce la importancia de recopilar evidencia y contar con asesoría legal especializada en ciberseguridad para proteger sus derechos legales en casos de delitos cibernéticos.

DISCUSIÓN

La información sensible que el sistema judicial maneja constituye un atractivo para los cibercriminales, hackctivistas, entre otros; si la información judicial cae en esas manos criminales, puede llegar a ser muy lesivo para los diferentes usuarios. (Rodríguez, 2021).

Así mismo, el autor Almario Peña. (2022) plantea:

> El crecimiento de la sociedad ha hecho que el comercio electrónico esté a la vanguardia de todos los procesos que se realizan a nivel empresarial. Por este motivo, cobra importancia la ciberseguridad a través de la protección de los sistemas informáticos, aplicando medidas preventivas de protección. (p.28).

Propuesta

- Establecer mecanismos de coordinación interinstitucional que permitan el intercambio efectivo de información y el reporte de incidentes cibernéticos.
- Impulsar el desarrollo y/o actualización de un marco normativo para el sistema nacional de gestión y atención de incidentes en el ciberespacio y definir competencias claras para cada uno de los actores involucrados.
- Implementar sistemas de enlace prioritarios normalizados ante crisis cibernéticas.

CONCLUSIONES

Ecuador no cuenta con un instrumento legal que emita lineamientos para gestionarlos riesgos cibernéticos y proteger las infraestructuras críticas de manera integral desde una perspectiva nacional, en colaboración y coordinación con los sectores público y privado, la academia y la sociedad civil. Implicar a representantes de otras funciones nacionales, empresas que cotizan en bolsa, operadores de infraestructuras críticas, instituciones académicas, centros de respuesta a incidentes, agentes del sector privado y de la sociedad civil y funcionesadministrativas en la elaboración de políticas permitirá a la dirección de la sociedadde las telecomunicaciones y la información fijar el horizonte de aplicación de las distintas líneas de actuación en el proceso de supervisión y seguimiento para lograrresultados a corto y medio plazo.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes, Sede Babahoyo, por motivar el desarrollo de la Investigación.

REFERENCIAS CONSULTADAS

Almario Peña, J. (2022). Análisis de las amenazas y riesgos cibernéticos que afrontan los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos a través de medios electrónicos. [Analysis of cyber threats and risks faced by users and organizations when consulting and/or acquiring tourism services through electronic means]. Tesis de Especialización. https://n9.cl/qen66

Asamblea Nacional (2014). Código Orgánico Integral Penal. [Comprehensive Criminal Code]. Registro Oficial Nº 180. https://url2.cl/53c6h

Asamblea Nacional Constituyente de la República del Ecuador, (2008). Constitución de la República del Ecuador. [Constitution of the Republic of Ecuador]. Montecristi. Registro Oficial 449 de 20-oct-2008. https://n9.cl/sia

Congreso Nacional. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. [Law on Electronic Commerce, Electronic Signatures and Data Messaging]. (Ley No. 2002-67). https://n9.cl/icjz

Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. [Inductive and deductive reasoning within the research process in experimental and social sciences]. *Laurus, 12*(Ext),180-205. https://n9.cl/nx847

EL UNIVERSO. (4 de agosto de 2021) Conozca cuáles son los delitos informáticos con pena de prisión en Ecuador. Los delitos informáticos han ido en aumento en Ecuador. [Learn which computer crimes are punishable by imprisonment in Ecuador. Computer crimes have been increasing in Ecuador]. EL UNIVERSO. https://n9.cl/1gnp8

Asamblea Nacional. (2016). Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación. [Organic Code of the Social Economy of Knowledge, Creativity and Innovation]. Suplemento del Registro Oficial No. 899. https://n9.cl/ictdw

Rodríguez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. [Cybersecurity in digital justice: recommendations for the Colombian case]. *Revista UIS Ingenierías*, *20*(3), 19–46. https://doi.org/10.18273/revuin.v20n3-2021002

Sain, G. (2012). Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet. [Crime and new technologies: fraud, drug trafficking and Internet money laundering]. Buenos Aires: Del Puerto. https://n9.cl/5oi9j

Sánchez Bracho, M., Fernández, M., y Díaz, J. (2021). Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo. [Data collection techniques and instruments: analysis and processing by the qualitative researcher]. *Revista Científica UISRAEL*, 8(1), 107-121. https://doi.org/10.35290/rcui.v8n1.2021.400