REVISTA SAN GREGORIO
ISSN: 1390 - 7247 // e-ISSN: 2528 - 7907

Revista San Gregorio. 2024; 1:58
doi: 10.36097/rsan.v1i58.2667

ARTÍCULO DE REVISIÓN

Delitos informáticos: Caso Ecuador

Computer Crimes: The Ecuador Case

Manuel Alexander Ponce Tubay[12]

[1]Universidad San Gregorio de Portoviejo, Ecuador.
[1]Universidad de Córdoba, España.

Citar como: Ponce, M. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. http://dx.doi.org/10.36097/rsan.v1i58.2667

Recibido: 15-12-2023 **Aceptado:** 31-05-2024 **Publicado:** 30-06-2024

RESUMEN

El presente trabajo tiene como objetivo analizar los desafíos de los delitos informáticos y sus respuestas legales en Ecuador. Para ello el estudio se basó en el método cualitativo con un análisis descriptivo de la bibliografía recopilada, para lo cual se realizó una revisión documental de libros; artículos de revista y la legislación ecuatoriana, sobre los diferentes sucesos acaecidos de delitos informáticos que se comenten en el Ecuador, con un énfasis en los ciberataques; y en cómo se encuentran tipificados los delitos informáticos en las leyes. En conclusión, se establece que el Ecuador no posee una estructura legislativa que respalde la seguridad de la información de los ciudadanos, así mismo, existe falencias en relación a la tipificación del delito informático, así como, el reconocimiento de las diferentes actividades que propenden a este delito y la inexistente promoción de protocolos seguros ante la vulnerabilidad de los usuarios.

Palabras clave: ataque a la integridad; internet, código penal, ciberataque, delitos informáticos.

ABSTRACT

The objective of this work is to analyze the challenges of computer crimes and their legal responses in Ecuador. For this, the study was based on the qualitative method with a descriptive analysis of the collected bibliography, for which a documentary review of books was carried out; magazine articles and Ecuadorian legislation, on the different incidents of computer crimes that are discussed in Ecuador, with an emphasis on cyberattacks; and how computer crimes are classified in the laws. In conclusion, it is established that Ecuador does not have a legislative structure that supports the security of citizens' information, likewise, there are shortcomings in relation to the classification of computer crime, as well as the recognition of the different activities that tend to this crime and the non-existent promotion of safe protocols due to the vulnerability of users.

Keywords: attack on integrity; internet, criminal code, cyber attack, computer crimes.

INTRODUCCIÓN

Desde el inicio de la pandemia, el uso de Internet ha experimentado un crecimiento significativo. Según datos de la Unión Internacional de Telecomunicaciones (ITU, 2023), aproximadamente 5,3 millones de personas se conectaron a Internet en 2022, utilizando dispositivos móviles o computadores personales. Este incremento en la conectividad también ha llevado a un aumento en las vulnerabilidades de seguridad cibernética. Por ejemplo, una encuesta realizada por Verizon entre marzo y junio de 2021 reportó 474 casos de violaciones de datos a nivel mundial, donde el 80% fueron causadas por hacking, datos robados y ataques de fuerza bruta (Mandal & Khan, 2020).

Además, los ataques cibernéticos más comunes durante este período incluyeron el Ransomware, que Min et al. (2022) definen como un virus que encripta archivos y datos del usuario hasta que se paga un rescate para su recuperación. Otros ataques comunes fueron la suplantación de IP y la suplantación de MAC, descritos

por Lema et al. (2018) y Liu (2019) respectivamente, como métodos utilizados para mantener el anonimato y causar explotación en Internet, o para simular un nodo auténtico mediante una dirección MAC falsa.

Dentro de los Objetivos de Desarrollo Sostenible establecidos (Naciones Unidas, 2015), el objetivo 16 enfatiza la importancia de "Promover sociedades justas, pacíficas e inclusivas". Este resalta la relevancia de la investigación actual, que se centra en la seguridad de los individuos, particularmente en el contexto del delito informático. Según Wadha et al. (2020), un delito informático se define como cualquier delito que se lleve a cabo utilizando computadoras u otras herramientas de comunicación para causar miedo y ansiedad a las personas, dañar y destruir propiedades.. Esta definición subraya cómo las tecnologías que facilitan la comunicación y la información pueden también ser utilizadas para perpetrar actos que desestabilizan la seguridad y la paz social.

El problema del delito informático se destaca como una preocupación que trasciende las fronteras geográficas, exacerbado por el alcance global del internet. Esta situación representa un desafío considerable para la delincuencia organizada y resalta la insuficiencia de legislaciones efectivas que regulen las actividades maliciosas que se expanden diariamente en la web. Estas actividades no solo aumentan en número, sino que también vulneran los derechos de más víctimas a través de un espacio virtual.

Según Narváez (2023), la tecnología involucrada comprende "el conjunto de programas y algoritmos... que se ejecutan en servidores informáticos" (p. 42), y facilitan la comprensión y generación del lenguaje natural de manera precisa. Esta capacidad tecnológica, si bien esencial para el progreso digital, también plantea serios riesgos de seguridad cuando es mal utilizada por actores malintencionados para perpetrar delitos en línea, lo que subraya la necesidad urgente de desarrollar marcos legales más robustos y cooperación internacional para abordar estos desafíos de manera efectiva.

En Latinoamérica desde hace algunos años se viene dando un incremento en el alza de los ataques cibernéticos; y el Ecuador no se encuentra exento de esto, especialmente en el sector financiero, y según de la ITU (2022), se encuentra en el lugar 119 de 182 países en cuanto a su vulnerabilidad a ataques cibernético. En general, los ataques cibernéticos en el país han sido dirigidos hacia los usuarios de banca en línea, que utilizan aplicaciones en dispositivos móviles o navegadores web de computadoras. Estos ataques pueden incluir malware, phishing, y ransomware, entre otros tipos de ataques (Echeverría et al., 2020; ITU, 2022)

El problema del acceso no consentido a sistemas informáticos es especialmente frecuente en Ecuador, donde incluso las instituciones gubernamentales han sido vulneradas. Un caso notable implica el uso de un aplicativo desarrollado por un ciudadano, el cual utilizaba un chatbot para recopilar información de los usuarios. Según Maniou & Veglis (2020), un chatbot es cualquier aplicación de software que entabla un diálogo con un humano, utilizando un lenguaje natural. Este aplicativo se promocionaba en una red social y no solo recogía datos de los usuarios, sino que también los almacenaba y revelaba sin su consentimiento, llegando incluso a venderlos para acceder a otras plataformas estatales (Fiscalía General del Estado, 2023).

Este incidente destaca la importancia crítica de reforzar las medidas de seguridad informática y la legislación para proteger la privacidad de los usuarios y la integridad de los sistemas informáticos, especialmente en contextos donde se maneja información sensible. Con lo antecedido, el presente trabajo tiene como objetivo analizar los desafíos de los delitos informáticos y sus respuestas legales en Ecuador, desde una concepción computacional sobre las vulnerabilidades que poseen los usuarios y su accesibilidad en la web.

METODOLOGÍA

El estudio adoptó un enfoque metodológico cualitativo mediante un análisis descriptivo basado en la revisión bibliográfica. Se realizó una búsqueda en diferentes bases de datos académicas y sitios web relevantes, incluyendo Dialnet, IEEE Xplore, Elsevier y la Web of Science (WOS), que sirvió para sustentar este estudio, además de análisis de referentes a la legislación vigente en Ecuador, tipos de delitos y casos relevantes. y Se excluyeron trabajos que abordaram delitos no relacionados al tema investigado, información obsoleta y detalles sensibles. Esto garantizó una cobertura amplia de literatura relevante a los delitos informáticos. Se analizaron finalmente un total de 29 trabajos.

Se analizó la información obtenida para identificar patrones, tendencias y lagunas en la investigación actual. La investigación se encuentra enmarcada en un análisis crítico documental de diferentes sucesos que se han presentado en el Ecuador ante el cometimiento de un delito informático y su respectiva penalización tal cual lo tipifican la legislación. Los hallazgos se documentaron detalladamente mediante una evaluación crítica de los datos y las fuentes recopiladas, debatiendo las implicaciones y se sugieren direcciones para futuras investigaciones.

RESULTADOS Y DISCUSIÓN

Análisis conceptual del delito informático

Con el auge de Internet y los avances en telecomunicaciones, se creó la primera página web, dando lugar a la denominada web 1.0. Esta versión limitaba la interacción del usuario a la visualización de información en

sitios web específicos. En este contexto, emergió la figura del programador web, responsable de actualizar contenidos, mantener la seguridad y otras funciones relacionadas con la gestión de un sitio web. Posteriormente, los desarrollos tecnológicos continuos facilitaron la transición a la web 2.0. Esta nueva etapa permitió que los usuarios no solo consumieran contenido, sino que también participaran activamente en la creación, edición y publicación de información en línea. Este cambio se refleja claramente en el surgimiento de las redes sociales y en sitios web que facilitan actividades diarias como transacciones comerciales, educación y atención médica, entre otras (Lujan, 2002).

Las empresas en su afán de facilitar, agilizar y responder de forma inmediata a los clientes han migrado muchos de sus servicios a la web, de manera que con un solo clic ejecuten diferentes actividades, ya sea desde un ordenador o cualquier dispositivo móvil que cuente con una conexión a internet. Pero como todo tiene sus ventajas y desventajas, la vulnerabilidad que es cualquier fallo o error en el software o en el hardware que hace posible a un atacante o hacker comprometer la integridad y confidencialidad de los datos que procesa un sistema (Aguilar, 2020), puede presentarse en cualquiera de los servicios a los que acceden los clientes que navegan en la web.

Los ataques realizados a través de Internet pueden ser legalmente sancionados como delitos informáticos en muchos países. Sin embargo, como señala Villavicencio (2014), no todos los delitos que implican el uso de computadoras u otros instrumentos tecnológicos califican automáticamente como delitos informáticos. La legislación precisa que la clasificación de un acto como delito informático debe basarse no solo en el uso de la tecnología, sino también en la naturaleza específica del acto delictivo y su conformidad con las definiciones legales establecidas. Este entendimiento es crucial para asegurar que las sanciones se apliquen correctamente y que se mantenga la integridad del sistema legal frente a la evolución tecnológica.

Según Saltos et al. (2021), el delito informático se puede definir como una actividad delictiva en la cual intervienen medios informáticos o electrónicos. Estos delitos han aumentado en Ecuador y en América Latina en la última década, a medida que la tecnología de la información ha avanzado. Sin embargo, se estima que el 80% de estos delitos no son reportados. Ecuador ocupa el tercer lugar en América Latina después de México y Bolivia en cuanto a índices de delitos informáticos, debido a la falta de una cultura de denuncia.

Uno de los delitos que se da con mayor frecuencia en Ecuador es la estafa mediante la obtención de datos de cuentas bancarias o tarjetas de crédito de un usuario. La víctima suele ser engañada por medio de un correo electrónico o sitios web que ofertan ciertos productos para la venta, solicitando la información de su tarjeta de crédito o cuenta bancaria. Luego, ejecutan una compra y resulta que el producto adquirido nunca llega, pero los datos financieros de la víctima ya están en manos del delincuente, quien puede llegar a realizar transacciones sin la autorización del usuario (Aguiar, 2020; Ojeda-Contreras et al., 2020).

Este tipo de estafas se conoce como phishing, y es común en Ecuador debido a la creciente digitalización de los servicios bancarios y la facilidad con que los usuarios pueden ser engañados por mensajes aparentemente urgentes y fraudulentos. Los ciberdelincuentes utilizan técnicas de ingeniería social para persuadir a las personas a compartir sus credenciales financieras, y luego utilizan estas credenciales para realizar transacciones fraudulentas (Aguiar, 2020).

Otro caso en Ecuador fue que una persona responsable del departamento de talento humano de la Fiscalía Provincial de Imbabura, alteró más de 300 registros del sistema biométrico a su favor, lo cual fue denunciado por la institución, la misma que realizó la debida pericia informática de los equipos del cual se obtuvo un informe en donde la Fiscal a cargo del caso pudo demostrar con evidencia la infracción cometida por la funcionaria, quien fue sentenciada a tres años de privación de su libertad por el delito ataque a la integridad de sistemas informáticos (Fiscalía General del Estado, 2022).

Por tanto, los delitos informáticos han aumentado significativamente en Ecuador en la última década, especialmente en el sector financiero, a pesar de que la mayoría de estos casos no se reportan. La falta de una cultura de denuncia y de una legislación robusta han contribuido a que Ecuador ocupe una posición preocupante en la región en cuanto a este tipo de delito.

Respuestas legales que penalizan el delito informático en Ecuador

En cuanto a la legislación, Ecuador ocupa el puesto 12 en la región en términos de representación de la sanción penal para delitos informáticos en su legislación vigente (Saltos et al., 2021). La legislación ecuatoriana define y penaliza varias formas de delito informático a través del Código Orgánico Integral Penal (COIP, 2014), que incluye sanciones específicas para diferentes tipos de actividades ilegales en línea, como el acceso no autorizado a sistemas informáticos, la violencia sexual digital, y otros ciberdelitos.

En el COIP (2014) se trata sobre el delito de "Ataque a la integridad de sistemas informáticos":

> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (art. 232)

http://dx.doi.org/10.36097/rsan.v1i58.2667

Este artículo busca sancionar penalmente a quienes ataquen la integridad de los sistemas informáticos, ya sea directamente o a través de programas maliciosos, con penas de prisión que pueden llegar hasta los 7 años si se afecta infraestructura crítica. No obstante, no tiene una tipificación clara y precisa de los delitos informáticos. Esto puede llevar a confusiones y dificultades en la aplicación. Además, las penas establecidas para los delitos informáticos en el COIP (2014) pueden ser insuficientes para disuadir a los delincuentes. Por ejemplo, la pena de tres a cinco años de privación de libertad para el testaferrismo puede no ser lo suficientemente severa para detener la comisión de este delito.

Entre las leyes relevantes, se encuentra la Ley Orgánica de Protección de Datos Personales (2021), que regula la gestión y protección de datos personales, y la Ley Orgánica de Telecomunicaciones (2015), que también incluye disposiciones sobre la seguridad de las redes y la información. Además, las reformas al Código Orgánico Integral Penal en 2019 y 2021 fortalecen la lucha contra los delitos informáticos, especificando y ampliando las definiciones y sanciones relacionadas con estos crímenes.

Estas leyes buscan proteger la integridad de los sistemas informáticos y la información contenida en ellos, así como prevenir y sancionar los delitos informáticos que afectan la seguridad y la privacidad de los ciudadanos ecuatorianos, sin embargo, el delincuente se podría acoger a otras leyes y de esta forma reducir su pena quedando libre en menos tiempo.

La legislación de Ecuador en relación con los delitos informáticos presenta ciertas debilidades, principalmente en la amplitud y la precisión de las definiciones legales que pueden llevar a aplicaciones desproporcionadas o injustas de la ley. Un problema destacado es la definición de acceso no autorizado en el COIP (2014), que puede interpretarse de manera muy amplia y potencialmente criminalizar actividades que no tienen intención maliciosa, como la investigación de seguridad. Además, la legislación no está completamente alineada con los estándares internacionales, a pesar de los esfuerzos de reforma y actualización de las leyes para abordar las amenazas digitales modernas.

Además, el gobierno, la Asamblea Nacional y demás instituciones del Ecuador no exponen alguna reforma o firman nuevos convenios internacionales que ayuden a combatir los ciberdelitos, para que estos no queden en la impunidad. La Policía Nacional de Ecuador y otros organismos encargados de la seguridad pública pueden carecer de recursos adecuados para investigar y perseguir delitos informáticos. La falta de conciencia pública sobre los delitos informáticos y sus consecuencias puede dificultar la prevención y la denuncia de estos delitos. Esto puede llevar a una mayor comisión de delitos y una menor eficacia en la aplicación de la ley.

CONCLUSIONES

Es imprescindible realizar un análisis jurídico profundo sobre cómo se encuentran tipificados los delitos informáticos en el Ecuador, debiendo hacer mucho más énfasis en mejorar y actualizar el marco legal para afrontar este tipo de delitos de modo asertivo; elaborando nuevas leyes concretas y que se adapten al entorno cambiante de las tecnologías y amenazas que se encuentran en el ciberespacio; con la colaboración del poder judicial, las instituciones de seguridad y gubernamentales para garantizar la aplicación de nuevas leyes y de las ya existentes.

Las leyes que se encuentran vigentes en el Ecuador presentan muchas falencias, el COIP no cuenta con un apartado dedicado a los delitos informáticos, solo sancionan a ciertas activades que atentan a la seguridad de la información, y la pena que estos establecen no va más allá de la privación de la libertad de tres a cinco años, y en ninguno de ellos se establece una sanción económica ante el cometimiento de este tipo de contravenciones.

Es necesario que estructuren o planteen nuevas leyes para proteger la información de los gobiernos, empresas y las personas, pero con los avances tecnológicos que surgen cada día y las nuevas estrategias que utilizan los hackers en el internet para obtener información de forma fraudulenta siempre nos encontraremos vulnerables ya que nos vemos en la necesidad de estar conectados en la web.

Es imperativo que el gobierno determine nuevas fórmulas de protección de la información que cada usuario posee considerando a esta como un bien que contiene una relevante importancia para sus actividades cotidianas. Así mismo, promueva a la ciudadanía mediante campañas protocolos seguros para que no estén vulnerables ante las diferentes amenazas que están presente en el internet.

REFERENCIAS

Código Orgánico Integral Penal [COIP]. (2014, 17 de febrero). Registro Oficial Suplemento 180. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Echeverría, M., Garaycoa, M., & Tusev, A. (2020). Are ecuadorian millennials prepared against a cyberattack?. Revista Chakiñan de Ciencias Sociales y Humanidades, (10), 73-86. https://doi.org/10.37135/chk.002.10.05

Fiscalía General del Estado. (2022, 22 de abril). Exfuncionaria de Fiscalía, sentenciada por ataque a sistemas informáticos. Boletín de prensa FGE N.- 280-DC-2022. https://www.fiscalia.gob.ec/exfuncionaria-de-fiscalia-sentenciada-por-ataque-a-sistemas-informaticos/

Fiscalía General del Estado. (2023, 3 de Marzo). Fiscalía obtiene sentencia por los delitos de acceso no consentido a un sistema informático, telemático o de telecomunicaciones y revelación ilegal de base de datos. Boletín de prensa FGE Nº 204-DC-2023. https://www.fiscalia.gob.ec/fiscalia-obtiene-sentencia-por-los-delitos-de-acceso-no-consentido-a-un-sistema-informatico-telematico-o-de-telecomunicaciones-y-revelacion-ilegal-de-base-de-datos/

Lema, H., Simba, F., y Ally, A. (2018). Preventing Utilization of Shared Network Resources by Detecting IP Spoofing Attacks through Validation of source IP Address. 2018 IST-Africa Week Conference (IST-Africa) (pp. 1-8). Botswana. https://ieeexplore.ieee.org/document/8417335

Ley Orgánica de Telecomunicaciones (2015, 12 de febrero). Registro Oficial Nº 439. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Ley Orgánica de Protección de Datos Personales. (2021, 26 de mayo). Registro Oficial Suplemento 459. https://finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Liu, S. (2019). MAC Spoofing Attack Detection Based on Physical Layer Characteristics in Wireless Networks. 2019 IEEE International Conference on Computational Electromagnetics (ICCEM). Beijing. https://doi.org/10.1109/COMPEM.2019.8779180

Lujan, S. (2002). Programación de aplicaciones web: historia, principios básicos y clientes web. . En S. Lujan, Programación de aplicaciones web: historia, principios básicos y clientes web. (p. 321). Editorial Club Universitario.

Mandal, S., y Khan, D. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. International Conference on Smart Electronics and Communication (pp. 837-842). India. https://doi.org/10.1109/ICOSEC49089.2020.9215374

Maniou, T., y Veglis, A. (2020). Employing a Chatbot for News Dissemination during. Future Internet , 12(7), 2-14. https://doi.org/10.3390/fi12070109

Min, D., Ko, Y., Walker, R., Lee, J., y Kim, Y. (2022). A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, 41(7), 2038-2051. https://doi.org/10.1109/TCAD.2021.3099084

Naciones Unidas. (2015). Objetivos del desarrollo sostenible. https://www.un.org/sustainabledevelopment/es/peace-justice/

Narváez, A. (2023). Espacio virtual e imaginarios urbanos. Centro de Estudios en Diseño y Comunicación(204), 31-47. https://www.researchgate.net/publication/372415867_Espacio_virtual_e_imaginarios_urbanos

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351. http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext

Unión Internacional de Telecomunicaciones [ITU]. (2023). Global offline population steadily declines to 2.6 billion people in 2023. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

Unión Internacional de Telecomunicaciones [ITU]. (2022). Cyberattacks Threaten Security in Ecuador. https://dialogo-americas.com/articles/cyberattacks-threaten-security-in-ecuador/

Villavicencio, F. (2014). Delitos Informáticos. Ius Et Veritas, 49(24), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Wadha, A.-K., Al-Maadeed, S., Ahmed, A., Sadiq, A., y Khan, M. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293-137311. https://doi.org/10.1109/ACCESS.2020.301125

Conflictos de interés:

Los autores declaran no tener conflictos de interés.

Contribución de los autores:

Manuel Alberto Ponce Tubay: Conceptualización, curación de datos, análisis formal, investigación, metodología, supervisión, validación, visualización, redacción del borrador original y redacción, revisión y edición.

Descargo de responsabilidad/Nota del editor:

Las declaraciones, opiniones y datos contenidos en todas las publicaciones son únicamente de los autores y contribuyentes individuales y no de Revista San Gregorio ni de los editores. Revista San Gregorio y/o los editores renuncian a toda responsabilidad por cualquier daño a personas o propiedades resultantes de cualquier idea, método, instrucción o producto mencionado en el contenido.