Detección de fraudes y estafas basadas en ingeniería social en Ecuador

Detection of frauds and scams based on social engineering in Ecuador

Max Guillermo Campos Gallegos
https://orcid.org/0009-0009-3953-8960
maxcmpos2@gmail.com
Investigador independiente. Quito – Ecuador.

Roberto Geovanny Moreno Dillon
https://orcid.org/0009-0007-3895-2743
rgmoreno@institutoicp.edu.ec
Investigador independiente. Quito – Ecuador.

Beatriz Alexandra Jiménez Espín
https://orcid.org/0009-0001-8343-4650
ajimenezdocpol@gmail.com
Investigador independiente. Quito – Ecuador.

RESUMEN

En un contexto cada vez más digital, la proliferación de ciberdelitos se ha convertido en una preocupación significativa para la seguridad de individuos y organizaciones en Ecuador. Esta investigación tiene como objetivo analizar la estadística de los ciberdelitos en Ecuador en el periodo 2019-2024, evaluando sus implicaciones tanto para individuos como para organizaciones, así como la efectividad de las normativas implementadas, especialmente en relación con el Código Orgánico Integral Penal (COIP), que contempla los delitos de estafa (Art. 186) y uso fraudulento de sistemas informáticos (Art. 190). Se empleó un enfoque cualitativo, que incluyó la revisión de literatura y el análisis de datos estadísticos sobre denuncias de ciberdelitos. Los resultados revelan un incremento significativo en estas denuncias, particularmente durante y después de la pandemia de COVID-19, lo que evidencia la vulnerabilidad de la población ante técnicas como el phishing y la suplantación de identidad, métodos comunes para la ejecución de estafas electrónicas. A pesar de iniciativas como el Convenio de Budapest y el Proyecto de Ley Orgánica de Seguridad Digital, persisten desafíos como la alta cifra negra de delitos no reportados y la desconfianza en las autoridades. Además, se identificó la urgente necesidad de mejorar la educación y concienciación en seguridad digital, sobre todo en grupos vulnerables como los adultos mayores. Por último, se recomienda fortalecer las normativas existentes del COIP y promover una cultura de denuncia que empodere a los ciudadanos en la protección de su información personal y financiera.

Palabras claves: ciberdelitos, normativas, fraudes

Recibido: 14-09-24 - Aceptado: 21-11-24

ABSTRACT

In an increasingly digital context, the proliferation of cybercrime has become a significant concern for the security of individuals and organizations in Ecuador. This research aims to analyze the statistics of cybercrime in Ecuador in the period 2019-2024, assessing its implications for both individuals and organizations, as well as the effectiveness of the regulations implemented, especially in relation to the Comprehensive Organic Criminal Code (COIP), which contemplates the crimes of swindling (Art. 186) and fraudulent use of computer systems (Art. 190). A qualitative approach was employed, including literature review and analysis of statistical data on cybercrime complaints. The results reveal a significant increase in these reports, particularly during and after the COVID-19 pandemic, which is evidence of the population's vulnerability to techniques

such as phishing and identity theft, common methods for the execution of electronic frauds. Despite initiatives such as the Budapest Convention and the Draft Organic Law on Digital Security, challenges persist, such as the high number of unreported crimes and distrust in the authorities. In addition, the urgent need to improve digital security education and awareness was identified, especially among vulnerable groups such as the elderly. Finally, it is recommended to strengthen existing COIP regulations and promote a whistleblower culture that empowers citizens to protect their personal and financial information.

Keywords: cybercrime, regulations, frauds

INTRODUCCIÓN

Un tema de creciente relevancia en la actualidad es la detección de fraudes y estafas derivadas de ingeniería social debido a que el entorno mundial se encuentra digitalizado, lo que ha permitido que la ingeniería social se consolide como una de las tácticas predilectas de los delincuentes para llevar a cabo fraudes y estafas. La ingeniería social se define como un conjunto de técnicas psicológicas y de manipulación que los delincuentes emplean para engañar a las personas, con el fin de que revelen información confidencial o realicen acciones que comprometan su seguridad o la de sus activos (Alzas, 2023). A diferencia de otros tipos de ciberataques, que se basan en la explotación de vulnerabilidades técnicas, la ingeniería social explota las vulnerabilidades humanas, tales como la confianza, el miedo o la urgencia (Marín, 2018).

En Ecuador, los fraudes y estafas que utilizan ingeniería social han experimentado un preocupante incremento, afectando tanto a individuos como a organizaciones. Estos delitos se manifiestan de diversas formas, incluyendo phishing, smishing, vishing y baiting, entre otros (Ibarra et al., 2024). Asimismo, el grado de conectividad y el uso generalizado de tecnologías digitales han facilitado la expansión de estos crímenes, lo que hace que su detección y prevención sean desafíos cruciales tanto para las autoridades como para la sociedad en general (Varela, 2024). A pesar del aumento significativo de estos delitos en el país, aún existe un vacío considerable en el conocimiento sobre cómo se están detectando y previniendo de manera efectiva (Escobar, 2022), evidenciando la falta de estudios que analicen la eficacia de las estrategias legales y preventivas actualmente implementadas.

Las estadísticas recientes resaltan la magnitud del problema. Por ejemplo, según datos de la Fiscalía General del Estado (2023), los casos de estafa y apropiación fraudulenta por medios electrónicos han incrementado en más del 40% en los últimos cinco años. Además, el impacto de estos delitos se ha visto exacerbado durante la pandemia de COVID-19, cuando muchas actividades cotidianas se trasladaron al entorno digital, aumentando la vulnerabilidad de las personas frente a tácticas de ingeniería social.

La creciente incidencia y sofisticación de estos delitos amerita un análisis detallado, ya que representan una amenaza significativa para la seguridad de individuos y organizaciones en un contexto de rápida digitalización. Además, una comprensión más profunda de cómo estos delitos impactan a la sociedad ecuatoriana pone en evidencia las insuficiencias en las estrategias actuales de prevención.

En torno al tema, se emplean teorías que exploran las motivaciones y conductas de los delincuentes que recurren a la ingeniería social. Por ejemplo, la Teoría de la Elección Racional sugiere que los delincuentes calculan el costo-beneficio antes de cometer un crimen, eligiendo tácticas de ingeniería social por su alta eficacia y bajo riesgo de detección (Zhao et al., 2021). Este enfoque resulta clave para entender por qué ciertos grupos delictivos prefieren estos métodos, especialmente en contextos donde las medidas de seguridad tecnológica son más robustas, pero las humanas son vulnerables.

A pesar de las medidas del Código Orgánico Integral Penal (COIP) para combatir los ciberdelitos, su efectividad es cuestionada por la falta de estudios que respalden su impacto. Por ello, es crucial identificar las deficiencias normativas y operativas que limitan una respuesta eficiente. Este artículo analiza el alarmante incremento de fraudes en Ecuador, centrándose en los artículos 186 y 190 del COIP, que sancionan la estafa y la apropiación fraudulenta por medios electrónicos. Se evalúan los mecanismos de detección y prevención, así como las estadísticas que evidencian la creciente sofisticación de los ciberdelincuentes, lo que subraya la necesidad de fortalecer las políticas de ciberseguridad. Además, se examina la efectividad de normativas como el Convenio de Budapest y el Proyecto de Ley Orgánica de Seguridad Digital, destacando sus implicaciones para individuos y organizaciones.

METODOLOGÍA

La investigación se enmarca dentro de un enfoque cualitativo debido a la naturaleza exploratoria y analítica del tema investigado. Además, se centra en la revisión y análisis de documentos legales, informes oficiales, estudios académicos y una base de datos proporcionada por la Fiscalía sobre fraudes y estafas basados en ingeniería social en Ecuador. El objetivo es comprender en profundidad el panorama actual relacionado con la detección y prevención en el contexto ecuatoriano. Además, es de tipo descriptivo y explicativo: descriptiva, ya que busca detallar las diferentes tipologías de fraudes y estafas según el

COIP de Ecuador, así como las estrategias de prevención adoptadas; y explicativa, porque pretende entender y explicar las causas de estos fenómenos delictivos y la eficacia de las medidas preventivas implementadas en el país durante el período de estudio.

La población del estudio incluye una amplia gama de documentos legales, informes de la Fiscalía General del Estado, estadísticas oficiales y literatura académica relacionada con el tema de estudio en Ecuador. Para la muestra, se empleó una selección intencional, enfocándose en documentos publicados entre 2019 y 2024 que abordan directamente el fenómeno de fraudes y estafas basados en ingeniería social en el contexto ecuatoriano. La selección de documentos se basó en su relevancia y su contribución al entendimiento del fenómeno investigado. Asimismo, la recolección de datos se llevó a cabo mediante una revisión documental exhaustiva, en la que se recopilaron y analizaron documentos clave, incluyendo el COIP, informes anuales de la Fiscalía, reportes de instituciones relacionadas con la ciberseguridad y estudios académicos sobre fraudes y estafas en Ecuador.

RESULTADOS Y DISCUSIÓN

Los resultados de la investigación se agruparon en cuatro secciones principales. Primero, se realizó un análisis de la situación actual de los ciberdelitos en Ecuador, examinando tendencias y patrones en el contexto nacional. Luego, se abordó los ciberdelitos en Ecuador: normativa y cifras, donde se exploró la legislación vigente y las estadísticas de incidencia. A continuación, se presentó la información sobre denuncias de estafa y apropiación fraudulenta por medios electrónicos (2019-2024), analizando cifras y tipos de estafas reportadas en este período. Finalmente, se discutió el Convenio de Budapest y el Proyecto de Ley Orgánica de Seguridad Digital en Ecuador, evaluando su impacto en la lucha contra los ciberdelitos.

Análisis de la Situación Actual de los Ciberdelitos en Ecuador

En el contexto ecuatoriano, los ciberdelitos han experimentado un incremento preocupante en los últimos años. Este aumento es especialmente notable tras la pandemia de COVID-19, la cual impulsó un mayor uso de servicios en línea y, con ello, amplió el terreno para la acción de los delincuentes digitales (Juca y Medina, 2023). En este sentido, uno de los aspectos más alarmantes es la prevalencia de las cifras negras, que se refieren a aquellos delitos que no son denunciados. Ante este panorama, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2022) ha implementado diversas medidas preventivas como la creación del Centro de Respuesta a Incidentes Informáticos (EcuCERT) y el fortalecimiento del Código Integral Penal como ejemplos de esfuerzos para combatir la ciberdelincuencia. A pesar del crecimiento en el número de denuncias formales, sigue existiendo una gran cantidad de incidentes que no se reportan. Entre las razones principales para este subregistro se encuentran la falta de confianza en las autoridades, el desconocimiento sobre los mecanismos de denuncia y la percepción de que no se recuperará lo perdido. De acuerdo con un informe de la Fiscalía General del Estado (2021), solo una pequeña fracción de los delitos informáticos llega a ser registrada oficialmente, lo que subestima considerablemente la magnitud real del problema.

Los modus operandi más comunes de los ciberdelincuentes en Ecuador incluyen técnicas como el phishing, smishing y vishing, las cuales engañan a las víctimas mediante correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentas, con el fin de obtener información personal o financiera (Pesantes, 2024). Asimismo, los delincuentes suelen suplantar la identidad de empresas legítimas, lo que incrementa la credibilidad de sus ataques al ofrecer promociones falsas o alertar sobre supuestos problemas en las cuentas de las víctimas. No obstante, a pesar de la sofisticación de estas tácticas, en 2023 se reportaron más de 12 millones de ciberataques, aunque el número total de intentos disminuyó en un 27% con respecto al año anterior (El Universo, 2024).

En Ecuador, la regulación de los delitos informáticos mediante el COIP busca adaptar el marco legal a los desafíos que presentan las tecnologías digitales (Janeta et al., 2023). El avance de internet ha facilitado nuevas formas de delito, como la pornografía infantil, el "grooming" y el "sexting", que explotan la vulnerabilidad de los menores a través de medios electrónicos (Janeta et al., 2023). Además, el COIP (2014) sanciona la apropiación fraudulenta, el acceso no autorizado a sistemas informáticos y los ataques cibernéticos, incluidos los daños causados por malware y los ataques de denegación de servicio (DoS y DDoS).

Las desventajas y amenazas para las víctimas de estos delitos incluyen, en primer lugar, pérdidas económicas directas. Además, la información personal y financiera comprometida puede llevar a robos de identidad y otras formas de fraude (Acosta et al., 2020). A menudo, las víctimas enfrentan una falta de conocimiento sobre cómo proceder ante el delito, lo que genera desconfianza en el sistema legal y subestima el impacto que este tipo de crímenes puede tener en su vida.

La suplantación de identidad ha emergido como uno de los fraudes más comunes en Ecuador, con 6,086 casos registrados en 2021. En este delito, los delincuentes crean perfiles falsos en redes sociales o envían mensajes engañosos haciéndose pasar por personas cercanas a la víctima, especialmente a través de plataformas como WhatsApp, Messenger o SMS. Utilizando información previamente obtenida sobre la víctima, como su nombre y detalles familiares, el atacante puede

simular ser un conocido que supuestamente se encuentra en el extranjero, incluso replicando su perfil en redes sociales (La competencia, 2023).

Por otro lado, el angler phishing ha cobrado relevancia como un método de ciberdelincuencia que utiliza las redes sociales para atraer a las víctimas a través de ofertas falsas o supuesta asistencia técnica (Jinde, 2024). En este caso, los delincuentes se valen de estas plataformas para crear anuncios engañosos que prometen beneficios irresistibles. Como resultado, las víctimas son incitadas a proporcionar información sensible, comprometiendo su seguridad personal y financiera. Este método representa un riesgo creciente en el contexto digital ecuatoriano, donde el uso de redes sociales es cada vez más común(Toala, 2021).

Ciberdelitos en Ecuador: normativa y cifras

En Ecuador, cientos de personas y empresas son víctimas de delitos cibernéticos a diario, pero muchos no denuncian los hechos, lo que genera una considerable "cifra negra". Este fenómeno puede atribuirse a varios factores, entre ellos, el analfabetismo digital, que afecta al 8.2% de la población, dejando a muchos ciudadanos vulnerables a trampas cibernéticas (Machado, 2024; Juca y Medina, 2023). Además, la falta de conocimiento sobre cómo protegerse en línea contribuye a que muchas víctimas no reporten los incidentes.

El delito de estafa se caracteriza por el uso de engaños para inducir a error a una persona con el fin de obtener un beneficio patrimonial. Entre las variables que lo definen se encuentra la simulación de hechos falsos, donde el estafador presenta situaciones ficticias como reales para engañar a la víctima. También es relevante el ocultamiento de hechos verdaderos, que consiste en omitir o distorsionar información importante que, de haberse conocido, habría impedido que la víctima cayera en el engaño (Crespo, 2021). Por otro lado, la apropiación fraudulenta por medios electrónicos implica el uso de sistemas tecnológicos para apoderarse de bienes o derechos ajenos sin el consentimiento del propietario. Una de las principales variables de este delito es el uso fraudulento de sistemas informáticos, donde se manipulan plataformas tecnológicas para acceder de manera no autorizada a bienes o información (Toala, 2021).

Tabla 1

Comparativa de delitos: estafa (Art. 186) vs. uso fraudulento de sistemas informáticos (Art. 190)

Variable	Art. 186	Art. 190
Verbo rector	Inducir a error	Utilizar fraudulentamente
Sujeto Activo	Persona física que comete o ejecuta el delito "la estafa".	Persona física que utiliza fraudulentamente sistemas informáticos o redes electrónicas.
Sujeto Pasivo	El titular del bien jurídico protegido, que es inducido a error, cuyo patrimonio o el de un tercero resulta perjudicado.	El titular del bien jurídico protegido o derecho afectado, o una tercera persona que sufra el perjuicio.
Conducta típica	Acción que conlleva a otra persona a una falsa creencia o engaño.	Uso fraudulento de sistemas informáticos que involucra el uso engañoso de éstos, redes electrónicas, y telecomunicaciones.
Medios	Utilización de la simulación de hechos falsos, deformación de una realidad u ocultamiento de hechos verdaderos.	Alteración, manipulación o modificación fraudulenta del funcionamiento de redes electrónicas, programas informáticos, sistemas telemáticos o informáticos, y equipos terminales de telecomunicaciones.
Finalidad	Obtener un beneficio patrimonial para sí mismo o para un tercero.	Facilitar la apropiación de un bien ajeno
Resultado	Ejecución de un acto que perjudique el patrimonio del sujeto pasivo o de un tercero.	Obtención de un beneficio patrimonial en perjuicio del propietario del bien o de un tercero.
Penalidad	Sanción punitiva prevista con pena privativa de libertad de cinco a siete años. Y pena de siete a diez años si se cumplen condiciones agravantes como perjuicio a más de dos personas, o si el delito se comete en contextos específicos como el uso de instituciones financieras o fondos públicos.	Sanción punitiva prevista con pena privativa de libertad de uno a tres años. Igual sanción se aplica si la infracción se comete utilizando métodos específicos como inutilización de alarmas, descubrimiento de claves, o violación de seguridades electrónicas.

El COIP (2014) establece la normativa penal ecuatoriana relacionada con delitos de fraude electrónico, específicamente la estafa y la apropiación fraudulenta por medios electrónicos, en los artículos 186 **y** 190. El artículo 186 define de manera detallada el delito de "estafa", identificando sus elementos esenciales como el verbo rector, el sujeto activo y pasivo, la conducta, los medios, la finalidad, el resultado y la penalidad correspondiente. Por su parte, el artículo 190 establece claramente el delito de "apropiación fraudulenta por medios electrónicos", también desglosando sus elementos constitutivos de la misma manera, lo que permite una comprensión integral de estos delitos en el marco legal ecuatoriano.

Información de denuncias sobre estafa y la apropiación fraudulenta por medios electrónicos. 2019-2024

Las Tablas 2 y 3 ofrecen un análisis sobre las denuncias y noticias relacionadas con los delitos de estafa y apropiación fraudulenta por medios electrónicos en Ecuador durante el periodo de 2019 a 2024. Los datos, obtenidos del Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA de la Fiscalía General del Estado (Fiscalía General del Estado, 2024), reflejan la evolución de estos delitos y las circunstancias modificatorias que pueden haber influido en su comisión, evidenciando la creciente preocupación por la ciberdelincuencia en el país.

Tabla 2

Noticias del delito - por año de registro, según presunto delito

Presunto delito	2019	2020	2021	2022	2023	2024	Total general
Apropiación fraudulenta por medios electrónicos	**1.740**	**2.281**	**5.235**	**3.136**	**3.451**	**2.506**	**18.349**
Consumado	1.704	2.234	5.178	3.111	3.428	2.491	18.146
Tentativa	36	47	57	25	23	15	203
Estafa	**16.889**	**18.267**	**23.905**	**22.699**	**24.240**	**17.344**	**123.344**
Consumado	16.554	17.675	23.378	22.315	23.934	17.165	121.021
Tentativa	335	592	527	384	306	179	2.323
Total general	**18.629**	**20.548**	**29.140**	**25.835**	**27.691**	**19.850**	**141.693**

La Tabla 2 presenta un análisis de la evolución de los delitos de Apropiación Fraudulenta por Medios Electrónicos y Estafa en Ecuador entre 2019 y 2024. En el caso de la Apropiación Fraudulenta, se registraron 1,740 casos en 2019, cifra que aumentó a 2,281 en 2020 y alcanzó un notable salto a 5,235 en 2021. Este incremento podría indicar una mayor sofisticación en los métodos de fraude o una mejor capacidad de detección y denuncia. Sin embargo, en los años siguientes, los casos experimentaron una disminución significativa, alcanzando 3,136 en 2022, 3,451 en 2023 y 2,506 en 2024. Este descenso puede interpretarse como el resultado de mejoras en las medidas de seguridad implementadas, así como una posible reducción en la actividad delictiva, aunque también podría atribuirse a una disminución en la denuncia de estos delitos. En total, se reportaron 18,349 casos, destacando que la gran mayoría fueron consumados (18,146), con una menor proporción de tentativas (203).

Por otro lado, los datos sobre Estafa revelan una tendencia creciente en el número de casos reportados. Desde 2019, cuando se registraron 16,889 casos, hasta 2023, con 24,240, los números reflejan un aumento constante, lo que podría ser indicativo de una mayor prevalencia de este delito o de una mayor disposición de los ciudadanos para reportar tales incidencias. En 2024, se registraron 17,344 casos, acumulando un total general de 123,344 durante el período, donde 121,021 fueron consumadas y 2,323 tentativas. El análisis de ambas categorías de delitos revela una significativa variabilidad a lo largo de los años, con picos en 2021 para ambos tipos de delitos, seguido de una tendencia a la baja hacia el final del período.

Tabla 3

Noticias del delito de estafa - por año de registro, según circunstancia modificatoria

PRESUNTO DELITO	2019	2020	2021	2022	2023	2024	Total general
ESTAFA	15.836	17.318	22.616	21.466	22.675	16.093	116.004
Estafa. Defraude mediante el uso de dispositivos electrónicos	76	150	130	71	139	85	651
Total general	**15.912**	**17.468**	**22.746**	**21.537**	**22.814**	**16.178**	**116.655**

Nota: Esta información corresponde a las noticias del delito de las cuales se conoce la circunstancia modificatoria relacionada con el uso de dispositivos electrónicos. Es posible que al momento de la denuncia se desconozca de dicha información por lo que se registra como "ESTAFA" en general.

La Tabla 3 proporciona un análisis detallado de las noticias relacionadas con el delito de estafa, centrándose en aquellas incidencias en las que se ha utilizado tecnología para la comisión del delito. Este enfoque permite evaluar el impacto de los dispositivos electrónicos en la criminalidad y la eficacia de las medidas de prevención y respuesta. El total de noticias sobre estafa muestra una evolución constante, comenzando con 15,836 casos en 2019 y aumentando hasta 22,675 en 2023, evidenciando un patrón de crecimiento en la incidencia de este delito. Este aumento puede estar asociado con una mayor penetración de las tecnologías digitales en las transacciones comerciales y personales, facilitando así nuevas formas de estafa. Sin embargo, en 2024, se reportaron 16,093 casos, destacando una ligera disminución que podría atribuirse a una mayor conciencia y a las medidas de protección adoptadas tanto por el público como por las instituciones.

Dentro del contexto de las estafas, se ha identificado un subgrupo específico que involucra el uso de dispositivos electrónicos para alterar, modificar, clonar o duplicar dispositivos originales de cajeros automáticos. Estos delitos, que también incluyen la captura y almacenamiento no autorizado de información de tarjetas, han mostrado un patrón de fluctuación. En 2019, se reportaron 76 casos de este tipo, cifra que aumentó a 150 en 2020, pero luego fluctuó, alcanzando un máximo de 139 en 2023 y descendiendo a 85 en 2024. En total, el número de estafas relacionadas con el uso de dispositivos electrónicos durante el período analizado asciende a 651 casos. Aunque esto indica una proporción relativamente baja en comparación con el total de estafas reportadas, subraya la creciente sofisticación en el uso de tecnología para la comisión de estos delitos. Por otro lado, el comportamiento del delito post-pandemia muestra un claro aumento en los casos de estafas y apropiación fraudulenta a través de medios electrónicos, directamente relacionado con el auge de las transacciones digitales y el comercio electrónico durante y después de la pandemia, lo que generó un entorno propicio para la evolución y diversificación de las actividades delictivas, permitiendo a los ciberdelincuentes perfeccionar sus métodos de ataque.

Convenio de Budapest y proyecto de ley orgánica de seguridad digital en Ecuador

El 12 de julio de 2024, el Presidente de la República del Ecuador ratificó el Convenio de Budapest mediante el Decreto Ejecutivo No. 332, estableciendo un marco legal robusto para enfrentar la creciente amenaza de la ciberdelincuencia (Corte Constitucional del Ecuador, 2024). Este acuerdo internacional, conocido formalmente como el Convenio sobre Ciberdelincuencia, fue aprobado en 2001 por el Consejo de Europa con el objetivo de combatir los delitos cibernéticos a nivel global (Ministerio de Gobierno, 2021).

La adhesión de Ecuador al Convenio de Budapest representa un paso importante en la actualización de las leyes nacionales relacionadas con la ciberseguridad y la ciberdelincuencia, así como en la capacitación especializada del personal encargado de aplicar estas normativas. Este convenio facilitará la cooperación internacional, permitiendo el intercambio de información crítica y la adopción de mejores prácticas en la lucha contra la ciberdelincuencia, reforzando así la capacidad del país para enfrentar amenazas cibernéticas y proteger su seguridad nacional. El proceso hacia la adhesión ha sido meticuloso: en diciembre de 2021, Ecuador comunicó formalmente su interés al Consejo de Europa, y en enero de 2024, la Corte Constitucional del Ecuador (2024) determinó que la ratificación del convenio requería aprobación legislativa previa. Finalmente, en julio de 2024, la Asamblea Nacional aprobó la adhesión con 85 votos a favor, consolidando el compromiso del país en la lucha contra la ciberdelincuencia.

El Proyecto de Ley Orgánica de Seguridad Digital en Ecuador se encuentra actualmente en discusión en la Asamblea Nacional (2024), con el propósito de establecer un marco normativo que garantice la protección y respuesta ante las amenazas en el ciberespacio. Este ambicioso proyecto, compuesto por 90 artículos, se enfoca en la creación de un Sistema Nacional de Seguridad Digital, además de subsistemas especializados en áreas como ciberseguridad, ciberdefensa, ciberinteligencia y ciberdiplomacia. Entre los principales objetivos de la ley se destaca la protección y respuesta, que busca crear un sistema integral capaz de prevenir, identificar y mitigar los riesgos y ciberdelitos que emergen en los entornos digitales. Asimismo, se pretende fortalecer la ciberseguridad, mejorando la protección de infraestructuras críticas digitales y garantizando la integridad de los datos personales frente a diversas amenazas.

El avance del proyecto ha sido analizado por la Comisión de Seguridad Integral, que está preparando un informe para su segundo debate en el Pleno de la Asamblea Nacional (2024). No obstante, se han solicitado ajustes adicionales antes de su aprobación final. A pesar de su relevancia, el proyecto ha generado controversias; organizaciones del sector tecnológico han expresado su preocupación por definiciones imprecisas que podrían desvirtuar el objetivo original de la ley. También se ha cuestionado la designación del Ministerio del Interior como ente rector del sistema, sugiriendo que debería ser el Ministerio de Telecomunicaciones, dada la naturaleza de la seguridad digital en el país.

CONCLUSIONES

Ecuador enfrenta un aumento alarmante de ciberdelitos que afecta a miles de personas y empresas, con una gran parte de la población sin denunciar debido a la falta de conocimiento y al analfabetismo digital que impacta al 8.2% de sus ciudadanos. La evolución normativa ha sido significativa, desde la Ley de Comercio Electrónico de 2002 hasta el actual COIP de 2014, que aborda específicamente delitos como la estafa y la apropiación fraudulenta por medios electrónicos. Sin embargo, persiste un vacío en la educación sobre seguridad digital, limitando así la efectividad de estas leyes. Las denuncias por estafa han crecido notablemente, con un total de 123,344 casos reportados, lo que evidencia la sofisticación de los ciberdelincuentes en un contexto de aumento de transacciones digitales tras la pandemia. La ratificación del Convenio de Budapest y el avance del Proyecto de Ley Orgánica de Seguridad Digital representan pasos importantes hacia el fortalecimiento de la ciberseguridad y la lucha contra la ciberdelincuencia, aunque su éxito dependerá de ajustes que aseguren claridad normativa y una implementación efectiva, a fin de empoderar a los ciudadanos y mitigar el impacto de estos delitos en la sociedad ecuatoriana.

La situación de los ciberdelitos en Ecuador es alarmante, con un notable aumento en las denuncias que refleja un problema más amplio, agravado por la alta cifra negra de delitos no reportados. A pesar de los esfuerzos del gobierno, como la creación del EcuCERT y la actualización del Código Orgánico Integral Penal, la falta de confianza en las autoridades y el desconocimiento sobre los mecanismos de denuncia limitan la efectividad de estas iniciativas. Los ciberdelincuentes utilizan métodos comunes como el phishing y la suplantación de identidad, afectando a individuos y organizaciones, mientras que el analfabetismo digital, que impacta al 8.2% de la población, impide que muchos denuncien los delitos. Aunque se han logrado avances normativos desde la Ley de Comercio Electrónico de 2002 hasta el actual COIP, que aborda delitos como la estafa y la apropiación fraudulenta por medios electrónicos, persiste un vacío en la educación sobre seguridad digital. Por ello, es esencial fortalecer la capacitación digital y fomentar la concienciación, especialmente en segmentos vulnerables, como los adultos mayores, para empoderar a la población y facilitar una respuesta más efectiva ante la ciberdelincuencia, así como mitigar su impacto en la sociedad ecuatoriana.

REFERENCIAS

Acosta, M., Benavides, M., y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia: RVG, 25*(89), 351-368. https://dialnet.unirioja.es/servlet/articulo?codigo=8890269

Alzas, J. (2023). *Estudio de fraudes basados en la técnica de Ingeniería Social*. [Tesis de Maestría, Universitat Oberta de Catalunya]. http://hdl.handle.net/10609/148147

Asamblea Nacional Constituyente. (2024). *Comisión de Seguridad aprobó informe para segundo debate de la Ley de Regulación y Control de Armas.* https://www.asambleanacional.gob.ec/es/noticia/98490-comision-de-seguridad-aprobo-informe-para-segundo-debate

Asamblea Nacional Constituyente. (2024). *Ley de Seguridad Digital será tratada en segundo debate en el Pleno de la Asamblea Nacional.* https://www.asambleanacional.gob.ec/es/noticia/95625-ley-de-seguridad-digital-sera-tratada-en-segundo-debate

Código Penal Orgánico Integral . (2014). *Código Penal Orgánico Integral.* https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

Corte Constitucional del Ecuador. (2024). *Caso 1-24-ti, el pleno de la corte constitucional del Ecuador, en ejercicio de sus atribuciones constitucionales y legales, emite el siguiente..* http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiI1Y2JlOGFiZS1kZWRjLTQwYmUtYjk1Yy02MjdjMDI2NWM5OGMucGRmIn0=

Crespo, H. (2021). El delito de estafa en el Código Orgánico Integral Penal. Breve análisis del tipo penal y las reformas del 2019. . *Derecho Penal Central, 3*(3), 135-149. https://revistadigital.uce.edu.ec/index.php/derechopenal/article/view/3341

El Universo. (21 de febrero de 2024). Ciberataques en Ecuador aumentaron un 30 % durante el 2023, según analistas. https://www.eluniverso.com/noticias/ecuador/ciberataques-ecuador-analistas-aumento-seguridad-nota/

Escobar, A. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. *Dominio de las Ciencias, 8*(1). https://dominiodelasciencias.com/ojs/index.php/es/article/view/2622/html

Fiscalia General del Estado. (2021). Omisión impropia en los delitos de apropiación fraudulenta por medios electrónicos. *El perfil criminológico: Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Fiscalia General del Estado. (2023). *Informe de labores Enero_Diciembre 2023.* https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Fiscalia General del Estado. (2024). Estadísticas de apropiación fraudulenta por medios electrónicos y estafas .

Fiscalia General del Estado. (2024). *Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA.*

Gil, L. (2022). *Estudio de los ataques y su defensa en la Ingeniería Social*. [Tesis de Maestría, Universidad Nacional de Educación a Distancia]. https://e-spacio.uned.es/entities/publication/bef19b67-069b-41c3-a7b1-288ee1e52f81

Guaña, E., Chiluisa, M., y Jaramillo, P. (2022). *Ataques de phishing y cómo prevenirlos.* Instituto Superior Tecnológico. http://190.57.147.202:90/xmlui/handle/123456789/3361

Janeta, S., Avilés, M., Fernández, A., y Naranjo, G. (2023). Los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas*, *8*(1). https://dialnet.unirioja.es/servlet/articulo?codigo=9392709

Jinde, A. (2024). *Estrategia para mitigar fraudes de angler-phishing basados en ingeniería social en plataformas de redes sociales.* [Tesis de Pregrado, Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/jspui/handle/123456789/41232

La competencia. (13 de Octubre de 2023). *¿Existe la Ingeniería Social en el Ecuador? La Competencia S.A.* https://www.competencia.com.ec/corporativo/existe-la-ingenieria-social-en-el-ecuador/

Machado, J. (. (10 de Junio de 2024). El 8,2% de ecuatorianos son analfabetos digitales y eso los hace vulnerables», según policía de ciberdelitos. Primicias. https://www.primicias.ec/noticias/seguridad/ciberdelitos-ecuador-estafas-analfabetos-digitales-vulnerables/

Marín, R. (2018). *Estudio de metodologías de ingeniería social.* [Tesis de Maestría, Universitat Oberta de Catalunya]. https://openaccess.uoc.edu/handle/10609/81271

Ministerio de Gobierno . (2021). *Análisis Legislativo Comparada entre el Derecho de Ecuador y la Convención de Budapest.* http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3NvcnRlbycsIHV1aWQ6J2YyZDZhN2VlLWYyZTAtNGQwMS05OTkzLTNhMmI1Y2Y2MjZhMC5wZGYnfQ==

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Ecuador trabaja en medidas preventivas para evitar los "ciberdelitos"*. https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-medidas-preventivas-para-evitar-los-ciberdelitos/

Pesantes, K. (7 de Julio de 2024). «Smishing» y «Vishing», dos nuevas estafas de los ciberdelincuentes que debe conocer. *Primicias*. https://www.primicias.ec/noticias/entretenimiento/tecnologia/smishing-vishing-estafas-ciberseguridad-ecuador/

Toala, Y. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*. [Tesis de Pregrado, Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf

Varela, E. (2024). *Análisis de la Privacidad y Seguridad en las Redes Sociales en un Mundo de Ciberdelitos*. [Tesis de Pregrado, Universidad Pontifica Comillas]. https://repositorio.comillas.edu/xmlui/handle/11531/80324

Zhao, J., Wang, X., Zhang, H., y Zhao, R. (2021). Rational choice theory applied to an explanation of juvenile offender decision making in the Chinese setting. *International Journal of Offender Therapy and Comparative Criminology*, *65*(4), 434-457. https://doi.org/10.1177/0306624X2093142