9 No.2 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.2.2025.e565

The impact of cybercrime in Ecuador and the challenges for justice in the new digital era.

El impacto de la ciberdelincuencia en el Ecuador y los desafíos para la justicia en esta nueva era digital.

Autores:

Jara-Morales, Pablo Andrés
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca– Ecuador
pajaram69@est.ucacue.edu.ec
https://orcid.org/0009-0008-2946-4921

Durán-Ramírez, Andrea Lisseth
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca– Ecuador
aduranr@ucacue.edu.ec
https://orcid.org/0000-0002-8382-1335

Fechas de recepción: 13-ABR-2025 aceptación: 13-MAY-2025 publicación: 30-JUN-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La era digital transformó la sociedad, mejorando la comunicación y la eficiencia, pero también incrementó los ciberdelitos, como fraudes, robo de identidad y ciberataques. En Ecuador, la ciberdelincuencia creció, afectando especialmente a grupos vulnerables como niños y adolescentes, con impactos tanto económicos como emocionales, la legislación ecuatoriana intentó adaptarse a estos desafíos, pero resultó insuficiente debido a la falta de especialización de los operadores judiciales y la infraestructura tecnológica limitada. El objetivo del estudio fue analizar la situación de la ciberdelincuencia en Ecuador, evaluando los desafíos legales y la efectividad de las políticas públicas. Se utilizó una metodología cualitativa, basada en la revisión de literatura, informes oficiales y entrevistas con expertos en ciberseguridad. Los resultados mostraron que, a pesar de los esfuerzos por mejorar la ciberseguridad, las políticas existentes no lograron frenar el aumento de los ciberdelitos, la legislación no se actualizó de manera adecuada para enfrentar las nuevas amenazas digitales, y la cooperación internacional siguió siendo limitada.

Palabras clave: Ciberdelincuencia; ciberseguridad; delitos informáticos; cooperación internacional

Abstract

The digital era transformed society, improving communication and efficiency, but it also increased cybercrimes such as fraud, identity theft, and cyberattacks. In Ecuador, cybercrime has grown, especially affecting vulnerable groups such as children and adolescents, with both economic and emotional impacts. Ecuadorian legislation has attempted to adapt to these challenges, but it has proven insufficient due to the lack of specialization among judicial operators and limited technological infrastructure. The objective of the study was to analyze the situation of cybercrime in Ecuador, evaluating legal challenges and the effectiveness of public policies. A qualitative methodology was used, based on a review of literature, official reports, and interviews with cybersecurity experts. The results showed that, despite efforts to improve cybersecurity, existing policies have not succeeded in curbing the increase in cybercrimes, legislation has not been adequately updated to address new digital threats, and international cooperation remains limited.

Keywords: Cybercrime; cybersecurity; computer crimes; international cooperation

Introducción

Desde el siglo XX, el progreso en las áreas de telecomunicaciones e informática ha impulsado la transformación hacia lo que se denomina era digital (Enrique Alastor, 2023) Estas innovaciones han modificado de manera significativa la forma en que las personas se comunican, trabajan, estudian y realizan transacciones comerciales, generando beneficios notables para el desarrollo económico y social (Picón Contreras et al., 2022)

No obstante, estos avances también han propiciado la aparición de nuevas amenazas, conocidas como delitos informáticos o ciberdelitos. Estas actividades ilícitas abarcan desde el fraude electrónico y el robo de identidad hasta ataques cibernéticos de gran magnitud y espionaje digital, lo que representa un desafío considerable tanto para la sociedad como para el sistema judicial del país. En Ecuador, el impacto de estos delitos ha crecido de forma acelerada, afectando tanto a individuos como a empresas y organismos públicos (Amelia Domínguez Arteaga & Vera Vázquez, 2022) Los grupos más vulnerables, como niños y adolescentes, son especialmente propensos a ser víctimas debido a su alto nivel de interacción en redes sociales y plataformas digitales. Por otro lado, las empresas suelen ser blanco de ataques que comprometen su información y operatividad (Afifi Nikolay Lozinskiy, 2021)

Además de las pérdidas económicas, los efectos de los ciberdelitos se extienden al ámbito emocional y psicológico. Las víctimas pueden experimentar vergüenza, miedo o ansiedad ante la divulgación de datos personales o contenido sensible, llegando incluso a sufrir consecuencias extremas.

Ante este panorama, la ciberdelincuencia presenta grandes retos para el sistema de justicia en Ecuador. La normativa vigente a menudo resulta insuficiente o inadecuada frente a la complejidad de estos delitos. Asimismo, la carencia de formación técnica entre los operadores judiciales y las limitaciones en infraestructura tecnológica dificultan la prevención, investigación y sanción efectiva de estos actos. La dimensión transnacional de muchos ciberdelitos también exige una cooperación internacional que, hasta ahora, sigue siendo limitada.

Ante esta realidad, la presente investigación busca responder a la siguiente pregunta: ¿Cuáles son las principales deficiencias en la legislación penal ecuatoriana para enfrentar los delitos

informáticos? En este contexto, el objetivo principal es analizar los delitos informáticos y su impacto en la seguridad cibernética en el Ecuador, identificando las principales amenazas, los mecanismos de prevención y control implementados por el Estado, y evaluando su efectividad en la reducción de la ciberdelincuencia. Para ello, se examinará el marco jurídico ecuatoriano sobre delitos informáticos, con el fin de identificar sus fortalezas y debilidades en la regulación de esta problemática. Asimismo, se evaluará la tipificación de estos delitos, analizando si las definiciones legales actuales son suficientes para abordar las complejidades de la ciberdelincuencia moderna. Finalmente, se propondrán estrategias para fortalecer la ciberseguridad en el país, diseñando medidas que incluyan mejoras normativas, promoción de la educación digital y el uso de tecnologías avanzadas para prevenir y mitigar los riesgos asociados a los delitos informáticos.

Marco teórico

Los ciberdelitos se refieren a actividades ilícitas realizadas en el entorno digital con el objetivo de obtener beneficios económicos, políticos o personales para quienes los perpetran (Juca-Maldonado & Medina-Peña, 2023) De acuerdo (Hectór Guillermo Saltos Pinto, 2022 en el concepto de ciberdelito se utilizó por primera vez a finales de los años 90 del siglo XX. A medida que el uso de Internet se popularizó, surgieron nuevos tipos de delitos que se llevan a cabo mediante redes informáticas. Estos delitos se han transformado en un problema global que impacta a todos los países y plantea grandes desafíos para la seguridad de la información y la privacidad individual (Juca-Maldonado & Medina-Peña, 2023a)

En el Comprehensive Study on Cybercrime elaborado por la United Nations Office on Drugs and(Afifi Nikolay Lozinskiy, 2021) se define el ciberdelito como el acceso no autorizado a un sistema informático, o la interferencia con un sistema informático o de datos. Del mismo modo, en el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se estableció que la ciberdelincuencia comprende acciones donde los datos o sistemas informáticos son el blanco directo del delito, así como aquellas en las que estos sistemas forman parte fundamental del modus operandi del delito (ONU, 2019).

De estas definiciones surge una característica esencial de los ciberdelitos: el uso de las herramientas y recursos digitales por parte de los delincuentes para cumplir sus objetivos.

Los métodos más comunes incluyen phishing,que es una técnica de ciberdelincuencia que utiliza correos electrónicos, mensajes de texto o sitios web fraudulentos simulando ser de fuentes confiables, malware que en término general sirve para software malicioso que infiltra, daña o interrumpe sistemas informáticos roba información, y espía a los usuarios o tomar control de dispositivos. y ransomware, que es forma específica de malware que bloquea el acceso a datos o sistemas mediante cifrado, exigiendo un pago para restaurar el acceso (Amaiquema Chuquiana Evelyb Maoli, 2023)

Otro rasgo distintivo de los ciberdelitos es el anonimato. Los delincuentes suelen utilizar técnicas que ocultan su identidad, dificultando así su detección por parte de las autoridades. Además, los ciberdelitos suelen caracterizarse por su complejidad y sofisticación, lo que exige un alto nivel de conocimientos técnicos por parte de los responsables, haciendo que su investigación y persecución sean especialmente complicadas (María Maldonado Bautista & Daniela Mollericona Alfaro, 2022)

Los ciberdelitos también abarcan una amplia variedad de objetivos y formas. Algunos están orientados al robo de información financiera, mientras que otros buscan manipular la opinión pública o acceder a datos confidenciales de organizaciones y empresas. Existen también delitos que tienen como finalidad el acoso, la difamación o el chantaje de personas (Catalina Marcillo, 2014)

Situación actual de ciberdelitos

El crecimiento constante de los ciberdelitos ha generado una preocupación considerable a nivel global debido a sus altos costos económicos y sociales. Estos delitos afectan no solo a empresas y organizaciones, sino también a individuos y a la sociedad en general (María Dolores Santos Vidal, 2022) La acelerada evolución de las tecnologías digitales y la aparición de nuevas modalidades de delitos en línea representan desafíos significativos tanto para las autoridades como para la sociedad.

El incremento del uso de las tecnologías de la información y la comunicación (TIC), junto con su rápida innovación, permite que los delitos informáticos sean cada vez más complejos y difíciles de detectar (Soria-Cubilo et al., 2022) Ante esta situación, se han implementado diversas estrategias para prevenir y combatir los ciberdelitos, incluyendo la mejora de la

seguridad en los sistemas informáticos, la promoción de programas de educación y concientización para usuarios sobre los riesgos en línea, el fortalecimiento de la cooperación internacional para perseguir delitos transnacionales, y la creación y actualización de legislaciones específicas en materia de ciberdelincuencia.

La globalización y la interconexión de las redes digitales han hecho que estos delitos trasciendan las fronteras, convirtiéndose en un desafío de alcance internacional Por ello, cada país ha desarrollado leyes y regulaciones particulares para hacer frente a esta problemática (Soledispa Lucas & Murillo Delgado, 2020).

La ciberdelincuencia, presente desde la popularización de la informática en la década de 1980 (INTERPOL, 2020), ha mostrado una evolución constante. El primer incidente documentado ocurrió en 1986, cuando un estudiante alemán infectó la red de la NASA con un virus informático (Medero, 2012). Actualmente, se calcula que se registran más de 4.000 ataques cibernéticos diarios en todo el mundo, lo que equivale a más de 1,5 millones de ataques al año, y estas cifras continúan en aumento

Situación estadística actual de los ciberdelitos

De acuerdo con el Informe ciberseguridad publicado en 2021, por (James Scott, 2021) se registraron más de 5,6 mil millones de ataques cibernéticos a nivel global durante 2020, lo que supone un incremento del 40% en comparación con el año anterior. Asimismo, los ataques de ransomware experimentaron un aumento del 62% en relación con 2019, y se reportaron más de 304 millones de intentos de phishing en el mismo período.

Según el informe de(Luis Fernando Rosero Tejada, 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 2019. Brasil y México encabezan la lista de países con mayor incidencia de estos ataques, seguidos por Perú, Colombia y Chile.

La pandemia de COVID-19 fue utilizada como una oportunidad por los ciberdelincuentes para intensificar sus actividades ilícitas en Latinoamérica. Según un informe de la empresa de seguridad informática (Carlos Vilchez Limay, 2020), en 2020 se registró un incremento del 124% en los ataques informáticos dentro de la región.

En Ecuador, los ataques de grupos dedicados a delitos cibernéticos son frecuentes, según un informe estadístico de la Unidad de Ciberdelitos de la Policía, entre 2020 y el 6 de julio de 2022 se registraron 3.183 delitos informáticos. En 2020 hubo 682 casos; en 2021, la cifra aumentó a 1.851, y en los primeros seis meses de 2022 ya se contabilizaban 650 investigaciones a nivel nacional.

El sector empresarial ha sido el más afectado por estos ataques cibernéticos según (María Maldonado Bautista & Daniela Mollericona Alfaro, 2022) aunque también se han identificado incidentes que involucran a gobiernos y organizaciones sin fines de lucro. Según (Anguera, 2023) una empresa tarda, en promedio, 280 días en detectar y contener un ciberataque, lo que genera graves consecuencias económicas y de reputación.

En este contexto, se espera que la ciberdelincuencia continúe aumentando debido a la expansión de la conectividad y la adopción de nuevas tecnologías Picón, et,al., (2022). Esto subraya la importancia de que los gobiernos y organizaciones adopten medidas de seguridad y concientización para mitigar el riesgo y minimizar el impacto de futuros ataques.

Marco legal en Latinoamérica y Ecuador

En América Latina, varios países han implementado normativas legales para prevenir y sancionar los ciberdelitos. En el caso de Ecuador, el Código Orgánico Integral Penal (COIP, 2014) regula los delitos informáticos, estableciendo sanciones penales para conductas como:

El acceso no autorizado a sistemas informáticos.

La interceptación de comunicaciones electrónicas.

La propagación de virus informáticos.

El acoso a través de medios digitales.

El COIP también ordena la creación de la Unidad de Investigaciones Tecnológicas y de Telecomunicaciones (UITT) dentro de la Policía Nacional, encargada de investigar delitos informáticos. Adicionalmente, las empresas proveedoras de servicios de internet están obligadas a cooperar con las autoridades en las investigaciones correspondientes (COIP, 2014)

A nivel regional, la Organización de los Estados Americanos (OEA) desarrolló en 2004 el Modelo Interamericano de Legislación sobre Delitos Informáticos, que proporciona una guía para los países miembros en la creación de leyes y políticas destinadas a prevenir, investigar y sancionar los ciberdelitos. Este modelo también promueve la cooperación internacional para enfrentar esta problemática (OEA, 2004). Ecuador ha integrado aspectos de este modelo en su legislación, como en el Código Orgánico Integral Penal, donde se tipifican varios delitos informáticos y se establecen sanciones para estos casos, esto demuestra su alineación con los objetivos del modelo de la OEA para fortalecer la ciberseguridad a nivel nacional y regional.

Tipos de ciberdelitos más frecuentes en Ecuador

De acuerdo con (Ibarra Armas & Villacis Mogrovejo, 2024), los ciberdelitos más comunes en Ecuador incluyen robo de información personal, fraude en línea, ataques informáticos a empresas y entidades públicas, sextorsión y ciberacoso. Además, estos delitos han aumentado considerablemente en los últimos años, afectando tanto a individuos como a empresas.

Problemas en la aplicación de la normativa vigente en relación a los delitos informáticos

La evolución de estas leyes refleja un intento de adaptarse al rápido desarrollo de la tecnología y sus implicaciones sociales. Sin embargo, las investigaciones actuales señalan que, a pesar de estos avances, existen lagunas en la legislación. Estas incluyen la insuficiencia en la clasificación de delitos cibernéticos emergentes, como la explotación de vulnerabilidades en infraestructuras digitales y los ciberataques organizados. Además, los esfuerzos institucionales por implementar estas normas han enfrentado desafíos, como la falta de capacitación adecuada para los operadores de justicia y una limitada infraestructura tecnológica para la investigación de este tipo de delitos.

Una de las razones que limita la sanción de este tipo de delitos es el:

“anonimato en la red y la transaccionalidad del delito complican los procesos judiciales debido a que pese que el delito informático se conoce que es cometido por alguien en concreto, en Internet solo se muestra una representación virtual del autor” (Ponce Tubay, 2024)

Al problema antes mencionado se le suma otro que es netamente clave en cuando al proceso que involucra denunciar este tipo de delitos. Así (Salazar Méndez et al., 2021) mismo, no se identificó un protocolo claro o metodología especializada por parte de los entes judiciales para abordar la investigación de ciberdelitos cometidos a través de redes sociales. Esto evidencia una falta de adaptación del sistema judicial a las características específicas de los crímenes digitales, que requieren herramientas técnicas avanzadas y enfoques innovadores. Actualmente, las investigaciones se llevan a cabo bajo los mismos parámetros que los delitos comunes, lo que limita la eficacia en el rastreo de autores, la recopilación de videncia digital y la respuesta ante las complejidades de la criminalidad en línea. Este enfoque generalista pueda dar lugar a vacíos en los procesos judiciales y la impunidad, por lo que es urgente implementar normativas y metodologías especializadas para responder a la creciente sofisticación de los ciberdelitos.

En Ecuador, las medidas relacionadas con la ciberseguridad enfrentan serios desafíos debido a la falta de una estructura normativa sólida y una estrategia unificada que permita abordar las amenazas crecientes en el entorno digital. A nivel nacional, aun no se han establecido objetivos claros para las entidades responsables del control y supervisión de la ciberseguridad. Asimismo, no se ha llevado a cabo una identificación integral de las infraestructuras críticas que podrían ser blanco de ataques cibernéticos, ni se ha evaluado adecuadamente el alcance de los daños potenciales en caso de incidentes de gran escala. Estos problemas reflejan una realidad preocupante: los indicadores de ciberseguridad del país se encuentran por debajo del promedio regional, lo que posiciona a Ecuador como uno de los países más vulnerables frente a las amenazas cibernéticas en América Latina (Ponce Tubay, 2024)

Aunque Ecuador ha experimentado cambios importantes en su estructura social, económica y política debido a la globalización, la capacidad del sistema legislativo para responder a los retos del ciberespacio a sido lenta. Esto se debe, en gran parte, a la falta de conciencia por parte de los líderes políticos sobre la magnitud de las amenazas digitales y su impacto en áreas fundamentales como la economía, la privacidad y la seguridad nacional. A pesar de contar con normativas que regulan aspectos específicos, como el acceso no autorizado a sistemas informáticos o el fraude electrónico, las políticas de ciberseguridad carecen de una

implementación homogénea y estandarizada entre las distintas instituciones gubernamentales. Esta situación que estas medidas resultan insuficientes y requieren una mayor inversión y capacitación en tecnologías de la información y seguridad cibernética, una situación que también se observa en otros países de la región, como señalan (Martínez et al., 2021) en el estudio de caso en México sobre el Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico.

Los ciberdelincuentes no se limitan a los hackers "black hat" que refiere a los hackers que realizan actividades ilícitas con fines maliciosos, como robar información; existen otras categorías como los "crackers," que introducen virus y roban contraseñas; los "phreakers," enfocados en telecomunicaciones; y los "hacktivistas," que actúan con fines políticos.

Para (Salazar Méndez et al., 2021) el Ecuador se encuentra en la etapa de maduración en términos de ciberseguridad, ocupando el puesto 66 a nivel mundial y el noveno en América. Este progreso se debe a esfuerzos centrados en cinco pilares: medidas jurídicas, técnicas, organizativas, creación de capacidades y operación. Además, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) desempeña un papel clave mediante la normativa para la gestión de incidentes y vulnerabilidades, fomentando la adopción de medidas por parte de los proveedores de servicios de telecomunicaciones para garantizar la seguridad de las redes.

Diariamente, el EcuCERT recibe reportes sobre incidentes y vulnerabilidades, trabajando en colaboración con empresas nacionales e internacionales para mitigar riesgos y fortalecer la ciberseguridad. Estas acciones, lideradas por el Gobierno Nacional, buscan proteger a los usuarios de las TIC, promoviendo un entorno más seguro y fortaleciendo la construcción de una Sociedad de la Información y el Conocimiento.

Retos y oportunidades de la Ley de Protección de Datos

La tecnología y la innovación son elementos clave para garantizar la implementación efectiva de la Ley Orgánica de Protección de Datos Personales en Ecuador.

Con el objetivo de analizar el impacto que esta legislación tendrá en el país, A3Sec, en colaboración con la Cámara de Comercio del Pacífico, llevó a cabo el webinar titulado “Retos y oportunidades de la Ley de Protección de Datos en Ecuador”. Durante el evento, expertos

provenientes de los sectores gubernamental, financiero y de ciberseguridad compartieron sus puntos de vista en un diálogo enriquecedor sobre cómo abordar el cumplimiento de esta normativa (Ponce Tubay, 2024)

Para (Juca-Maldonado & Medina-Peña, 2023b)la Ley de Protección de Datos en Ecuador permite a diversas industrias, incluida la bancaria, implementar medidas adecuadas para garantizar un manejo responsable del acceso y la seguridad de la información. Es crucial adoptar buenas prácticas en la gestión de datos, comenzando con un inventario exhaustivo que identifique las fuentes de información de los clientes, como sistemas de cobranza, facturación, CRM o plataformas de gestión de clientes. A partir de esta identificación, es necesario establecer qué políticas de protección están en uso y cuáles deben implementarse como mínimo para garantizar que los accesos a bases de datos o sistemas de información estén resguardados con medidas y capas de seguridad adecuadas, evitando su exposición directa al entorno externo.

Material y métodos

El estudio se desarrolló bajo un enfoque cualitativo, de carácter descriptivo y analítico. La investigación descriptiva se orientó a detallar las principales características de la ciberdelincuencia en Ecuador, considerando aspectos como las modalidades delictivas, los perfiles de las víctimas más afectadas y las respuestas legales e institucionales implementadas. Paralelamente, el componente analítico permitió interpretar las conexiones entre estas características y las deficiencias presentes en el marco normativo y operativo nacional.

El análisis se centró en la información textual obtenida de diversas fuentes, lo que facilitó la exploración profunda de los factores legales, técnicos y sociales vinculados con los delitos informáticos. Este enfoque posibilitó la identificación de patrones, vacíos y relaciones subyacentes, priorizando la comprensión integral del fenómeno desde una perspectiva holística que abarcó tanto el marco jurídico como las experiencias de los actores involucrados.

Para el desarrollo de la investigación, se realizó una revisión documental exhaustiva de la legislación ecuatoriana, tratados internacionales, informes oficiales y literatura científica relevante sobre ciberdelincuencia y ciberseguridad. Asimismo, se llevó a cabo un análisis comparativo de las estrategias empleadas en otros países para combatir la ciberdelincuencia, con el objetivo de identificar prácticas efectivas susceptibles de ser aplicadas en el contexto ecuatoriano. El método analítico-sintético se aplicó para descomponer la información utilizada en el trabajo y reconstruirla a manera de síntesis, lo que permitió un análisis detallado de casos específicos, como el dictamen 1-24-TI/24 emitido por el Pleno de la Corte Constitucional del Ecuador en 2024. Además, se utilizó el método dogmático-jurídico, consistente en el estudio del derecho positivo y su estructura formal, así como el método exegético-jurídico, que sirvió como medio de interpretación de las normas e instituciones del derecho, facilitando la comprensión del problema analizado.

En cuanto a las técnicas empleadas, se aplicó el análisis de contenido para interpretar la información recopilada en documentos normativos, entrevistas e informes, identificando patrones y temas relevantes para la investigación. Esta metodología proporcionó un marco estructurado que permitió analizar el fenómeno de la ciberdelincuencia en Ecuador, identificando tanto las limitaciones actuales como las estrategias necesarias para fortalecer el sistema de justicia frente a esta creciente amenaza digital.

Resultados

La educación y la concienciación pública desempeñan un papel esencial en la prevención de los delitos cibernéticos y en la protección de los usuarios en el ámbito digital. La carencia de conocimientos y habilidades en ciberseguridad representa una de las principales debilidades aprovechadas por los ciberdelincuentes. Por ello, es indispensable desarrollar programas educativos que cubran desde la alfabetización digital básica hasta la formación especializada en ciberseguridad.

Es importante que estos programas comiencen en las escuelas, fomentando una cultura de seguridad digital desde edades tempranas. Esto incluye enseñar a los estudiantes sobre los peligros en línea, prácticas recomendadas para proteger su información personal y cómo reconocer y evitar amenazas comunes, como el phishing y el malware. Asimismo, las

universidades y otras instituciones educativas deben ofrecer formación avanzada en ciberseguridad para preparar a futuros profesionales en este campo crucial (Shin, 2017; Wu & Brush, 2010).

Además de la educación formal, las campañas de concienciación pública son fundamentales para informar a la población sobre los riesgos y las mejores prácticas en ciberseguridad. Estas iniciativas pueden difundirse mediante medios de comunicación, redes sociales y talleres comunitarios. La colaboración entre gobiernos, empresas privadas y organizaciones no gubernamentales es clave para ampliar el alcance y garantizar la efectividad de estas acciones (Mishna et al., 2009).

Los ciberdelitos han experimentado un notable incremento en los últimos años, consolidándose como una de las principales amenazas a la seguridad digital en el país. Este fenómeno afecta tanto a individuos como a empresas y entidades públicas, generando impactos económicos, sociales y psicológicos significativos, en Ecuador destacan el robo de información personal, el fraude en línea, los ataques a empresas y entidades públicas, la sextorsión y el ciberacoso. Estas actividades reflejan la diversidad y complejidad de los desafíos que enfrenta la seguridad cibernética en el país.

A pesar de las políticas públicas y las iniciativas implementadas para enfrentar esta problemática, las estrategias actuales han demostrado ser insuficientes, la falta de inversión en tecnologías avanzadas, capacitación técnica y actualización legislativa limita la capacidad del país para prevenir y mitigar los ciberdelitos. La dimensión transnacional de los ciberdelitos subraya la necesidad de fortalecer la cooperación internacional y adoptar marcos legales integrales. Si bien el Código Orgánico Integral Penal de Ecuador regula algunas conductas delictivas digitales, se requiere un enfoque más amplio y específico que contemple los constantes avances tecnológicos.

Es esencial invertir en programas de educación y sensibilización para promover una cultura de seguridad digital entre los usuarios, este enfoque no solo permite reducir la vulnerabilidad individual, sino que también fomenta una respuesta colectiva frente a los riesgos cibernéticos. Enfrentar la ciberdelincuencia exige un enfoque coordinado entre el sector público, privado y la sociedad civil, la colaboración en áreas como la implementación de tecnologías

avanzadas, la capacitación técnica y la mejora de los marcos legales puede marcar la diferencia en la lucha contra los ciberdelitos en Ecuador.

Conclusiones

Las conclusiones del presente estudio evidencian que la ciberdelincuencia en Ecuador constituye una amenaza creciente y compleja, que afecta tanto a individuos como a empresas y entidades públicas, generando impactos económicos, sociales y psicológicos significativos. A pesar de los esfuerzos realizados en materia legislativa y de políticas públicas, las estrategias implementadas hasta el momento han resultado insuficientes para frenar el aumento de los ciberdelitos. La falta de actualización y especialización en la normativa, sumada a la limitada capacitación técnica de los operadores judiciales y a la carencia de infraestructura tecnológica adecuada, limita la capacidad del sistema de justicia para prevenir, investigar y sancionar eficazmente estos delitos.

El estudio resalta la importancia de fortalecer la educación y la concienciación pública en ciberseguridad, promoviendo programas formativos desde edades tempranas y campañas de sensibilización que involucren a todos los sectores de la sociedad. Asimismo, se identifica la necesidad de una mayor inversión en tecnologías avanzadas y en la capacitación de los profesionales encargados de la seguridad digital, así como la urgencia de establecer protocolos y metodologías especializadas para la investigación y persecución de los delitos informáticos.

Por otro lado, la dimensión transnacional de la ciberdelincuencia subraya la importancia de intensificar la cooperación internacional y de adoptar marcos legales integrales y actualizados, capaces de responder a la constante evolución de las amenazas digitales. Solo a través de un enfoque coordinado entre el sector público, privado y la sociedad civil, que combine la mejora normativa, la educación digital y la innovación tecnológica, será posible enfrentar de manera efectiva los desafíos que plantea la ciberdelincuencia en el Ecuador y fortalecer la seguridad digital en el país.

Referencias bibliográficas

Afifi Nikolay Lozinskiy, A. (2021). La ciberseguridad en las organizaciones del sistema de las Naciones Unidas.

Amaiquema Chuquiana Evelyb Maoli. (2023). Analisis del ataque del modelo Phishing en los sistemas informaticos y Bancarios.

Amelia Domínguez Arteaga, R., & Vera Vázquez, R. (2022). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. https://doi.org/10.31095/podium.202

Anguera, M. T. (2023). Revisiting systematic reviews from a methodological perspective. RELIEVE - Revista Electronica de Investigacion y Evaluacion Educativa, 29(1). https://doi.org/10.30827/relieve.v29i1.27758

Carlos Vilchez Limay, R. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional. https://www.oas.org/juridico/english/cyb_pry_

Catalina Marcillo, A. O. (2014). Desafíos globales del cibercrimen: Caso ecuador periodo 2014- 2029.

COIP. (2014). CODIGO ORGANICO INTEGRAL PENAL, COIP. www.lexis.com.ec

Enrique Alastor, E. S. V. (2023). Tic en la educación en la era digital: propuestas de investigación e intervención.

Ibarra Armas, J. A., & Villacis Mogrovejo, F. D. (2024). Adaptación del marco legal laboral ecuatoriano al impacto de la inteligencia artificial. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(5). https://doi.org/10.56712/latam.v5i5.2747

James Scott. (2021). Ciberseguridad: Resumen de amenazas 2021 y tendencias 2022.

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

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

Luis Fernando Rosero Tejada. (2021). El phishing como riesgo informático, técnicos y prevención los canales electrónicos: un mapeo sistemático.

María Dolores Santos Vidal. (2022). Marco regulatorio dela ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento.

María Maldonado Bautista, L., & Daniela Mollericona Alfaro, M. (2022). Estudio comparativo de dos protocolos anestesicos con Diazepam y Midazolam aplicada en hembras caninas sometidas a cirugia de ovariohisterectomia (Artículo de investigación). 6(1), 2022.

Martínez, C. R., Rubio, E. L., Camarillo, S. D. R., Millán, J. V. F., Romero, F. A., Quintanilla, R. E. L., Álvarez, J. F. M., Flores, M. A. S., Escatell, G. A. S., & Martínez, J. A. Á. (2021). Background and perspectives of certain priority diseases affecting cattle farming in Mexico. In Revista Mexicana De Ciencias Pecuarias (Vol. 12, pp. 111–148). INIFAP-CENID Parasitologia Veterinaria. https://doi.org/10.22319/rmcp.v12s3.5848

Medero, G. S. (2012). La ciberguerra: los casos de Stuxnet y Anonymous.

Pleno La Corte Constitucional Del Ecuador, E. DE. (2024). Dictamen 1-24-TI/24 Juez ponente: Jhoel Escudero Soliz (Vol. 593, Issue 2). www.corteconstitucional.gob.ec

Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

Salazar Méndez, D. D., Mauricio, M., Maldonado, T., Beatriz, M., & Tapia, R. (2021). Perfil Criminológico (FGE).

Soria-Cubilo, R., Altamirano-Cumbajin, J., Cabrera-Barbecho, F., & Tipán -Barros, B. (2022). ¿El uso de las tecnologiás de la información y comunicación productividad de las firmas? Evidencia empírica enEcuador. In abril-junio (Vol. 33)..

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.