Revista de Investigación en Ciencias de la Educación
Vol. 3, No 5, enero - junio 2025, 15-28
ISBN: 3073-1461
https://revistasfiecyt.com/index.php/riced

La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la Legislación en Ecuador

The influence of social media on cybercrimes and the challenges for Legislation in Ecuador

Jacinto Zorobabel Moncada Chachapoya[1]
Alba de los Cielos Miranda Villacís[2]

[1,2]*Universidad Indoamérica. Ambato, Ecuador.*

[1]*Autor de correspondencia: jmoncada2@indoamerica.edu.ec*

Datos del artículo:
Recibido: agosto 16, 2024
Revisado: octubre 14, 2024
Aceptado: noviembre 15, 2024
Publicación: enero 1, 2025

Palabras clave:
redes sociales, criminalidad, delitos informáticos, legislación.

Keywords:
social media, crime, cybercrimes, legislation.

DOI:
https://doi.org/10.53877/riced 3.5-2

Resumen

Este estudio analiza la relación entre el desarrollo tecnológico, especialmente el uso de redes sociales, y el aumento de la criminalidad a nivel global, con un enfoque específico en Ecuador. La investigación busca responder a la pregunta: ¿Están las redes sociales influyendo en el incremento de actividades delictivas? A través de un enfoque cualitativo, se realizó una revisión exhaustiva de literatura académica y fuentes especializadas para comprender cómo las redes sociales facilitan la perpetración de delitos, particularmente las estafas cibernéticas. Además, se examinaron los delitos informáticos tipificados en el Código Orgánico Integral Penal (COIP) y otras legislaciones ecuatorianas, lo cual permitió un análisis detallado de las implicaciones legales de estos delitos en el contexto digital. Como parte de los resultados, se incluyó el análisis de datos provenientes de la lista negra de FireHOL IP, en la que se identificaron 256 direcciones IP ecuatorianas asociadas con actividades sospechosas. Este hallazgo refleja la vulnerabilidad existente en el país y sugiere una necesidad urgente de fortalecer la seguridad en redes, así como de realizar un monitoreo continuo para evitar la afectación de usuarios legítimos, se destaca que uno de los mayores desafíos en la lucha contra los delitos informáticos, como las estafas cibernéticas, es la dificultad de identificar y sancionar a los responsables. La capacidad de estos delitos de trascender fronteras añade complejidad a su persecución y control, haciendo imprescindible un marco legal robusto y una cooperación internacional más amplia. Los hallazgos subrayan la importancia de fortalecer la infraestructura de ciberseguridad y promover políticas que contribuyan a la prevención y detección temprana de cibercrímenes en Ecuador.

Abstract

This study analyzes the relationship between technological development, especially social media use, and the increase in global criminal activity, with a specific focus on Ecuador. The research seeks to answer the question: ¿Are social media platforms influencing the rise in criminal activities? Through a qualitative approach, an extensive review of academic literature and specialized sources was conducted to understand how social media facilitates crime, particularly cyber scams. Additionally, cybercrimes defined in Ecuador's Comprehensive Organic Criminal Code (COIP) and other national legislation were examined, allowing for a detailed analysis of the legal implications of these crimes in the digital context. The results included data from the FireHOL IP blacklist, which identified 256 Ecuadorian IP addresses

linked to suspicious activities. This finding reflects the existing vulnerability within the country and suggests an urgent need to strengthen network security, along with continuous monitoring to avoid impacts on legitimate users. One of the main challenges in combating cybercrime, such as online scams, is the difficulty in identifying and sanctioning those responsible. The cross-border nature of these crimes adds complexity to their prosecution and control, making a robust legal framework and broader international cooperation essential. The findings underscore the importance of strengthening cybersecurity infrastructure and promoting policies that contribute to the prevention and early detection of cybercrimes in Ecuador.

Forma sugerida de citar (APA):

Moncada-Chachapoya, J. Z., Miranda-Villacís, A. (2025). La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la Legislación en Ecuador. *RICEd*: *Revista de Investigación en Ciencias de la Educación. 3*(5), 15-28. https://doi.org/10.53877/riced3.5-2

INTRODUCCIÓN

En la última década, el surgimiento y la creciente popularidad de las redes sociales han transformado la forma en que nos comunicamos, interactuamos y accedemos a la información. Estas plataformas digitales se han convertido en parte integral de nuestra vida cotidiana, y su influencia abarca diversos ámbitos, incluido el ámbito delictivo.

En el contexto específico de Ecuador, el impacto de las redes sociales en la delincuencia ha sido objeto de creciente preocupación. A medida que más y más ecuatorianos se conectan a Internet y participan activamente en plataformas como Facebook, Twitter, Instagram y WhatsApp, se abren nuevas puertas para la comisión de delitos, así como para la propagación de actividades ilegales.

Esta investigación tiene como objetivo analizar y comprender a fondo la influencia de las redes sociales en el ámbito delictivo en Ecuador. Examinaremos cómo estas plataformas han sido utilizadas por individuos y grupos delictivos para cometer una variedad de delitos, como el ciberacoso, la extorsión, el fraude y la difusión de contenido ilegal. Además, exploraremos las consecuencias sociales, legales y éticas de estas prácticas delictivas facilitadas por las redes sociales.

Asimismo, abordaremos las medidas y estrategias implementadas por las autoridades ecuatorianas para combatir la delincuencia en línea y minimizar los riesgos asociados con el uso irresponsable de las redes sociales. Además, se destacarán las iniciativas destinadas a concientizar y educar a la población sobre los peligros y las buenas prácticas en línea.

A través de la investigación, esperamos generar un mayor entendimiento sobre cómo las redes sociales han influido en el ámbito delictivo en Ecuador y cómo podemos abordar este desafío de manera efectiva. Al comprender mejor este fenómeno, estaremos en mejores condiciones de promover un uso responsable y seguro de las redes sociales, así como de desarrollar estrategias más sólidas para prevenir y combatir la delincuencia en línea en nuestro país.

MÉTODOS Y MATERIALES

Para llevar a cabo la investigación sobre "La influencia de las redes sociales en el ámbito delictivo", se siguió una metodología que combinó la consulta de fuentes académicas y la revisión de literatura especializada en SCOPUS. A continuación, se describen los pasos

seguidos en el proceso de selección de artículos y la elección del eje temático de la investigación:
Se realizó una búsqueda en la base de datos de SCOPUS utilizando las palabras clave "social media crimes", "cybercrime" y "online crimes". Estas palabras clave se seleccionaron por su relevancia en el ámbito de estudio y su uso frecuente en la literatura académica. Se limitó la búsqueda a artículos en inglés y español, ya que son los idiomas de mayor relevancia en las ciencias sociales.

Se consideraron aquellos artículos que abordaban temas relacionados con las redes sociales y su relación con delitos y estafas. Se priorizaron los estudios publicados en revistas científicas de reconocido prestigio y categorizadas en el campo de las ciencias sociales para asegurar la calidad de la información recopilada. El eje temático elegido para la investigación se centró en el "cibercrimen" y los lineamientos o parámetros para establecer si un hecho fáctico puede considerarse probado en este contexto. Se profundizó en cómo la verdad es una característica necesaria de una decisión justa en casos de cibercrimen. Se analizaron distintos mecanismos para alcanzar la verdad, como la inferencia lógica a partir de diferentes medios de prueba y la utilización de procedimientos matemáticos en la resolución de estos casos.

Para esta investigación, se utiliza la lista negra de FireHOL IP como un nuevo conjunto de datos de ciberseguridad, que involucraran procedimientos matemáticos en su interpretación y aplicación. Estos casos se utilizaron como ejemplos para mostrar cómo el uso de procedimientos matemáticos puede influir en la resolución de litigios relacionados con cibercrimen y cómo a veces los resultados obtenidos pueden desafiar la intuición.

Se presentaron diversos escenarios relacionados con el cibercrimen en Ecuador para ilustrar la aplicación de procedimientos en el ámbito jurídico en la búsqueda de la verdad y la resolución de disputas.

RESULTADOS

Como primer punto, las redes sociales son plataformas en línea que permiten a las personas conectarse y comunicarse entre sí, compartir contenido y participar en comunidades virtuales. Estas plataformas han revolucionado la forma en que nos relacionamos, ya que nos brindan la oportunidad de mantenernos actualizados sobre las vidas de nuestros amigos y familiares, conocer nuevas personas con intereses similares e incluso promover nuestras ideas o negocios.

Según Boyd & Ellison (2007), "una red social es un servicio basado en Internet que permite a los individuos construir un perfil público o semipúblico dentro de un sistema delimitado, articular una lista de otros usuarios con quienes comparten una conexión y ver y recorrer su lista de conexiones y las hechas por otros dentro del sistema".

Por otro lado, Kaplan y Haenlein (2010) definen las redes sociales como "un grupo de aplicaciones web basadas en internet que se construyen sobre fundamentos ideológicos y tecnológicos subyacentes". Además, agregan que estas plataformas permiten a los individuos crear perfiles personales o profesionales, conectarse con otros usuarios y generar contenido compartido.

Es por eso que las redes sociales tienen su origen en las comunidades en línea y los sistemas de mensajería que surgieron a finales del siglo XX. Sin embargo, el término "red social" se popularizó con el lanzamiento de sitios web como SixDegrees.com en 1997, que permitían a los usuarios crear perfiles personales y conectarse con otros.

Un artículo de la revista Forbes menciona: "SixDegrees.com fue uno de los primeros sitios web que permitió a los usuarios crear perfiles personales y conectarse con amigos". Aunque SixDegrees.com tuvo éxito inicialmente, cerró en 2001 debido a problemas financieros.

Posteriormente, en 2002, se lanzaron dos plataformas importantes: Friendster y MySpace. Friendster fue pionero en el concepto de redes sociales tal como lo conocemos hoy en día. Según un informe de la Universidad Estatal de Pensilvania, "Friendster fue el primer sitio web que combinó elementos clave como perfiles públicos, listas de amigos y posibilidad de enviar mensajes".

Sin embargo, fue MySpace quien realmente despegó y se convirtió en el líder indiscutible de las redes sociales durante varios años. MySpace permitía a los usuarios personalizar completamente sus perfiles utilizando HTML y CSS, lo cual era una característica muy popular entre los jóvenes. El libro "The Facebook Effect" menciona: "MySpace era como una versión más desordenada pero más emocionante del mundo real".

En 2004, Mark Zuckerberg fundó Facebook mientras aún era estudiante universitario. Facebook comenzó inicialmente como una plataforma exclusiva para estudiantes universitarios antes de abrirse al público general en 2006. Desde entonces, ha experimentado un crecimiento exponencial y se ha convertido en la red social más grande del mundo.

Otro hito importante en la evolución de las redes sociales fue el lanzamiento de Twitter en 2006. Según un artículo de The Guardian, "Twitter revolucionó la forma en que nos comunicamos al permitirnos compartir mensajes cortos y concisos con seguidores".

En los últimos años, han surgido otras redes sociales populares como Instagram (2010) y Snapchat (2011), cada una con su propio enfoque único y características distintivas. Cada una tenía su propia propuesta única: Twitter permitía a los usuarios compartir mensajes cortos llamados "tweets", Instagram se centraba en compartir fotos y Snapchat ofrecía la opción de enviar mensajes que desaparecían después de ser vistos. Este entorno variado y altamente conectado facilita nuevas oportunidades para la interacción, pero también ha abierto puertas a riesgos y amenazas en el ámbito de la ciberseguridad.

En este contexto, los ciberdelincuentes aprovechan la amplia difusión y popularidad de estas plataformas para emplear tácticas fraudulentas como el phishing. Según la investigación de Azeez y otros (2020) sobre identificación de ataques de phishing en redes de comunicación manifiestan que el phishing se refiere a una táctica fraudulenta empleada por ciberdelincuentes para engañar al público objetivo mediante mensajes de texto, llamadas telefónicas o correos electrónicos, haciéndose pasar por agentes legítimos y solicitando información confidencial y sensible. Un ataque de phishing exitoso puede llevar a pérdidas financieras y robo de identidad. Es crucial identificar las características forenses de estos ataques para detectarlos y desalentar a los perpetradores, así como implementar medidas defensivas. Con el fin de proteger a los usuarios de Internet de los ataques de phishing, se han propuesto diversos modelos antiphishing. Sin embargo, las técnicas actuales para abordar este desafío no han sido suficientes ni lo bastante efectivas.

Azeez y Fadhal (2023) han investigado el creciente fenómeno de las plataformas de redes sociales en Internet, las cuales han ganado una gran popularidad al permitir que diversos usuarios se mantengan conectados con sus amigos y familiares sin importar su ubicación y en cualquier momento. Sin embargo, este aumento en la popularidad también ha traído consigo un incremento significativo en el crimen virtual desde que estas plataformas se iniciaron hasta la actualidad. El crimen virtual en las redes sociales se manifiesta en diversas formas, donde los delincuentes aprovechan estas plataformas para cometer diversos tipos de crímenes.

Una modalidad delictiva muy común en las redes sociales es el acoso cibernético o cyberbullying. Esta forma de violencia se caracteriza por el hostigamiento constante a través de mensajes ofensivos, amenazantes o difamatorios hacia una persona. El anonimato que proporcionan las redes sociales facilita este tipo de comportamiento agresivo, causando un gran impacto emocional en las víctimas.

Otra modalidad delictiva es la suplantación de identidad. Mediante perfiles falsos, los delincuentes pueden hacerse pasar por otra persona para engañar y obtener información personal sensible. Esto puede llevar al robo de identidad, donde los criminales utilizan esta información para realizar estafas financieras u otros actos ilícitos.

Además, las redes sociales también son utilizadas como plataforma para la distribución y consumo de contenido ilegal, como pornografía infantil o material violento. Los delincuentes aprovechan la facilidad con la que se comparten archivos en estas plataformas para difundir este tipo de contenido prohibido.

El grooming es otra práctica delictiva que ha aumentado gracias a las redes sociales. Se trata del proceso mediante el cual un adulto establece contacto con un menor a través de internet con fines sexuales. Los depredadores sexuales utilizan perfiles falsos y técnicas manipuladoras para ganarse la confianza de los menores y luego abusar sexualmente de ellos.

El término happy slapping (traducido como "bofetada feliz") surgió en el Reino Unido en 2005. Este fenómeno implica la grabación de un acto de agresión, que puede ser física, verbal o incluso sexual, con el propósito de difundirlo en línea a través de plataformas digitales, como sitios web, blogs, chats y redes sociales. Es común que este tipo de violencia se comparta mediante redes sociales, y en algunos casos, puede llegar a viralizarse rápidamente (García, 2022).

Por otro lado, las redes sociales también son utilizadas para cometer estafas y fraudes. Los delincuentes aprovechan la ingenuidad de las personas y su confianza en esta plataforma para engañarlas y obtener beneficios económicos ilegítimos. Estos fraudes pueden incluir desde la venta de productos falsificados hasta esquemas piramidales que prometen grandes ganancias.

En su investigación, los autores emplean distintos métodos para abordar este problema. Comparan los clasificadores tradicionales y el aprendizaje conjunto con el objetivo de clasificar el acoso virtual en redes sociales en línea. Para lograrlo, utilizan ambos modelos junto con cuatro conjuntos de datos diferentes, buscando identificar y diferenciar las situaciones de acoso y proteger a los usuarios de estas experiencias negativas.

Sin embargo, el estudio llevado a cabo por Chen, Hao, Ding y otros investigadores (2023) considera el cibercrimen como un fenómeno social y desarrolla un marco teórico que integra diversos aspectos: sociales, económicos, políticos, tecnológicos y factores de ciberseguridad que influyen en el ciberdelito. Para esta investigación, se utiliza la lista negra de FireHOL IP como un nuevo conjunto de datos de ciberseguridad, que permite mapear los delitos cibernéticos a nivel subnacional en todo el mundo. Los investigadores emplean un Modelo Lineal Generalizado (GLM) para identificar los principales factores que influyen en el cibercrimen. Asimismo, utilizan un Modelo de Ecuaciones Estructurales (SEM) para estimar los efectos directos e indirectos de varios factores en el cibercrimen.

Los resultados del GLM indican que, al incluir un amplio conjunto de factores socioeconómicos, se mejora significativamente la capacidad explicativa del modelo. Además, se demuestra que el cibercrimen está estrechamente relacionado con el desarrollo socioeconómico y que sus efectos varían según el nivel de ingresos. Por otro lado, los resultados del SEM revelan aún más la relación causal entre el cibercrimen y numerosos factores contextuales. En particular, se muestra que los factores tecnológicos actúan como mediadores entre las condiciones socioeconómicas y el ciberdelito.

En conjunto, este enfoque más completo y multidimensional del estudio del cibercrimen contribuye a una mejor comprensión de sus causas y consecuencias, proporcionando información valiosa para el diseño de estrategias más efectivas en la lucha contra este creciente problema global.

La influencia de las redes sociales en los índices de criminalidad en Ecuador es un tema complejo que ha generado diversas opiniones. Según el sociólogo ecuatoriano Carlos Vera, "las redes sociales han contribuido a la propagación de delitos como el bullying, la extorsión y el acoso cibernético, lo cual ha aumentado los índices de criminalidad en el país" (Vera, 2018). Esta afirmación indica que el acceso fácil a estas plataformas permite que estos delitos se perpetúen y afecten negativamente a la sociedad.

En un estudio realizado por la Universidad Central del Ecuador, se concluyó que "el uso excesivo de las redes sociales puede generar conductas desviadas en los jóvenes, quienes son más propensos a estar involucrados en actos delictivos" (Universidad Central del Ecuador, 2020). Esto sugiere que la constante exposición a contenidos inapropiados o violentos en estas plataformas puede influir en comportamientos criminales.

Además, otro estudio publicado por el Observatorio Nacional para la Seguridad Ciudadana en 2020 revela que "el acceso fácil y rápido a las redes sociales ha permitido la organización y coordinación de actividades ilegales como robos a domicilios o asaltos a mano armada". Este informe también destaca que "las redes sociales son utilizadas por grupos criminales para reclutar nuevos miembros, planificar acciones delictivas e incluso exhibir sus fechorías".

No obstante, algunos expertos argumentan que "no se puede atribuir únicamente a las redes sociales el aumento de los índices de criminalidad en Ecuador", ya que existen múltiples factores socioeconómicos y culturales involucrados (González, 2017). Es importante considerar otros aspectos como la pobreza, desigualdad social y falta de oportunidades laborales como variables influyentes.

LEGISLACIÓN. Delitos tipificados en el COIP

En Ecuador, varias leyes son aplicables para abordar la delincuencia cometida a través de redes sociales, especialmente aquellas relacionadas con el uso indebido de la tecnología, el acceso no autorizado a sistemas informáticos y la protección de la privacidad de las personas. Algunas de las más relevantes incluyen:

1. Ley de Comunicación (LORE) - Art. 19 y 25

Esta ley regula el uso de los medios de comunicación, incluidos los digitales, y establece disposiciones sobre la privacidad, el acceso a la información y el respeto a los derechos humanos. La violación de estos derechos a través de las redes sociales puede acarrear sanciones.

2. Código Penal Ecuatoriano - Delitos informáticos

Art. 234 (Acceso no autorizado a sistemas de información): Penaliza el acceso no autorizado a sistemas informáticos o de telecomunicaciones, lo que incluye hackeos o invasión a cuentas personales o de instituciones a través de las redes sociales.

Art. 230.3 (Diseminación de programas informáticos para realizar Phishing y Pharming): Relacionado con el fraude cibernético, incluyendo el uso de las redes sociales para engañar a personas y obtener información confidencial de forma fraudulenta.

Art. 234.1 (Falsificación informática): Trata sobre el uso de medios electrónicos para falsificar información, que es un delito frecuente en las redes sociales (por ejemplo, crear perfiles falsos o difundir noticias falsas).

3. Código Orgánico Integral Penal (COIP)

Tabla 1

Normas jurídicas que establece los delitos y las penas por el COIP

Delitos informáticos y delitos relacionados con las computadoras	Artículo	Conducta	Pena

Pornografía Infantil	103		13 a 10 años
Posesión de Pornografía Infantil	104		13 a 10 años
Grooming	173		3 a 5 años
Oferta de servicios sexuales a través de medios electrónicos	174		7 a 10 años
Hostigamiento	154.2	Hostigue a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra persona	6 meses a 1 año y 1 a 3 años, si son menores de edad
Ciberacoso Sexual	166	Solicitar actos de naturaleza sexual prevaliéndose de su situación de autoridad o jerarquía, para los cuales utiliza cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales.	1 a 5 años.
Happy slapping	160	Se grabe o transmita un abuso sexual o violación con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, o se agreda físicamente a la víctima, y dicha agresión también sea grabada o transmitida.	3 a 5 años; 7 a 10 años (Abuso sexual) 19 a 23 años (Violación)
Violación del Derecho a la Intimidad, Mensajes de datos Vídeos Datos Personales	178	No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley	de 1 a 3 años
Revelación de secreto o información personal de terceros	179,2	Revele o divulgue a terceros contenidos digitales, mensajes, correos, imágenes, audios o vídeos, o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.	de 1 a 3 años
Intercambio, comercialización o compra de información de equipos terminales móviles	192		de 1 a 3 años
Actos Lesivos a los Derechos de Autor	208.B	Vulnere a sabiendas los derechos de autor o derechos conexos.	6 meses a 1 año, con comiso y multa de 8 hasta 300 salarios básicos unificados del trabajador en general.

Suspensión, alteración o suposición de la identidad y estado civil por medios electrónicos	221		1 a 3 años
Revelación ilegal de información de bases de datos	229		3 a 5 años
Pharming y Phishing	230.1 230.2 230.3	Diseminación, posesión o introducción de programas informáticos, mensajes de datos y todo contenido digital para realizar Pharming y Phishing	3 a 5 años
Duplicación de información de tarjetas de débito y crédito	230.4 230.5		3 a 5 años
Fraude Informático	231		3 a 5 años
Mulas del fraude informático	231.2		3 a 5 años
Ataque a la integridad de sistemas informáticos	232	Diseño, venta, distribución de malware Destrucción de infraestructura física Destrucción de bienes informáticos para la prestación de servicios informáticos Prestación de un servicio público o vinculado con la seguridad ciudadana	3 a 5 años
Acceso no autorizado a sistemas de información	234	La persona que, sin autorización, acceda en todo o en parte a un sistema informático, sistema telemático o de telecomunicaciones	3 a 5 años
Explota ilegítimamente el acceso logrado			3 a 5 años
Modificar un portal web			3 a 5 años
Desvía o redirecciona el tráfico de datos o voz		Ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos	3 a 5 años
Falsificación Informática	234.1	Provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produciendo datos o documentos no genuinos.	3 a 5 años
		La persona que utilice el mensaje de datos o contenido digital falsificado.	3 a 5 años
Terrorismo	366.1	La persona que, respecto de un transporte terrestre, una nave o aeronave, plataformas fijas marinas, se apodere de ella, ejerza control sobre la misma por medios tecnológicos	10 a 13 años.

Nota. COIP, Normas jurídicas que establece los delitos y las penas relacionadas a ciberdelitos.

4. Ley Orgánica de Prevención y Erradicación de la Violencia Contra las Mujeres (2018)

La ley busca prevenir y sancionar diversas formas de violencia, incluida la que se da a través de las redes sociales (como el ciberacoso, la difusión no consensuada de imágenes

íntimas, etc.). Esta ley establece que la violencia digital contra las mujeres puede tener repercusiones legales severas.

5. Ley de Protección de Datos Personales (en trámite)

Aunque aún está en proceso de desarrollo, esta ley tiene como objetivo regular el uso de datos personales, proteger la privacidad de los ciudadanos y sancionar el uso indebido de esta información en plataformas digitales, incluidas las redes sociales. El robo de información personal o la exposición no consentida de datos personales se considera un delito.

6. Ley de Delitos Informáticos y Ciberseguridad (propuesta)

Ecuador ha estado trabajando en una ley de delitos informáticos que podría fortalecer la legislación actual para abordar de manera más precisa y efectiva los delitos cometidos a través de las tecnologías digitales y redes sociales, como el acceso no autorizado a datos, el fraude digital, y la distribución de contenido ilícito.

Ecuavisa analiza: tres tipos de ciberdelitos son los más frecuentes en Ecuador

Los jóvenes son más vulnerables debido a su exceso de confianza con la tecnología Más del 80 % de la población usa Internet para realizar actividades de entretenimiento y finanzas, como por ejemplo compartir fotografías en tiempo real hasta el uso de sus cuentas bancarias. Esto da oportunidad al ciberdelito.

Las cifras son alarmantes.

Apropiación fraudulenta por medios electrónicos, 562 casos de investigación o delegaciones en 2022. En el año 2023, 371. Y en lo que va del 2024, 291

Violación a la intimidad, en el 2022 presentó 120 casos. En el 2023, 98. En el 2024, 54

Pornografía infantil, en el 2022 presentó 42 casos. En el 2023, 45. En lo que va del 2024, 30

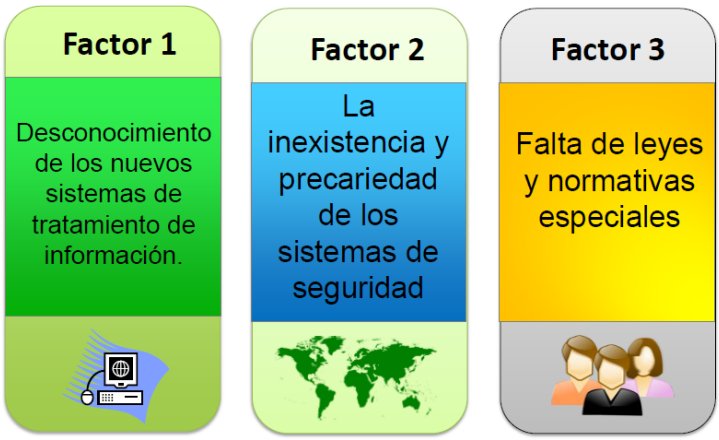
Para Gonzalo García, jefe de la Unidad Nacional de Ciberdelitos, estas cifras varían. "No hay una tendencia a la baja. Siempre estos delitos van perfeccionándose, existen nuevas modalidades. Entonces la tendencia siempre es un poco al alza", explica García.

Asegura además que los jóvenes son más vulnerables debido a su exceso de confianza con la tecnología. "Los jóvenes postean muchas fotografías de los lugares en los que se encuentran o cuando se reúnen con familiares o amigos".

Para Santiago Acurio del Pino (2020) explica por qué la proliferación de este fenómeno delictivo:

Figura 1

Por qué la proliferación de los delitos informáticos



Nota. Tomado de Delitos informáticos en el código orgánico integral penal COIP por Santiago Acurio, 2020. Derechos de autor.

Para Fidel Velásquez la legislación sobre ciberdelitos ha comenzado a ser cada vez más relevante, aunque aún existen retos significativos en su implementación y aplicación efectiva. Las leyes ecuatorianas, como el Código Orgánico Integral Penal (COIP), incluyen sanciones para delitos informáticos, pero la falta de recursos y capacidades en ciberseguridad sigue siendo un obstáculo importante para su aplicación efectiva. Aunque se han promulgado leyes, como el reciente proyecto de ley sobre ciberseguridad, que busca prevenir y mitigar las amenazas cibernéticas, la implementación de estas normativas enfrenta dificultades debido a la falta de infraestructura adecuada y la limitada preparación de los sectores públicos y privados.

El 80% de los delitos cibernéticos en Ecuador no son denunciados, lo que refleja no solo un subregistro, sino también la desconfianza o desconocimiento de los ciudadanos sobre cómo abordar este tipo de delitos (DataGuidance, 2021)

Además, los ataques recientes, como el de Anonymous en 2019, y la fuga de datos masiva en 2019, evidencian la vulnerabilidad del país a los ciberdelitos y la falta de una respuesta rápida y eficiente frente a los mismos.

Estos incidentes destacan la necesidad urgente de una mayor capacitación, tanto a nivel gubernamental como empresarial, para prevenir futuros ataques.

El país también está en proceso de desarrollar un marco legal más robusto, como lo demuestra el Proyecto de Ley sobre Ciberseguridad, que busca establecer un sistema de seguridad digital nacional. Este sistema incluiría subsistemas y políticas públicas que coordinen las acciones del gobierno para mitigar los riesgos cibernéticos (Fidel Velásquez, 2019).

Sin embargo, el desafío persiste debido a que Ecuador aún ocupa posiciones bajas en los índices globales de ciberseguridad, lo que indica que el país aún no está completamente preparado para enfrentar las amenazas de la era digital

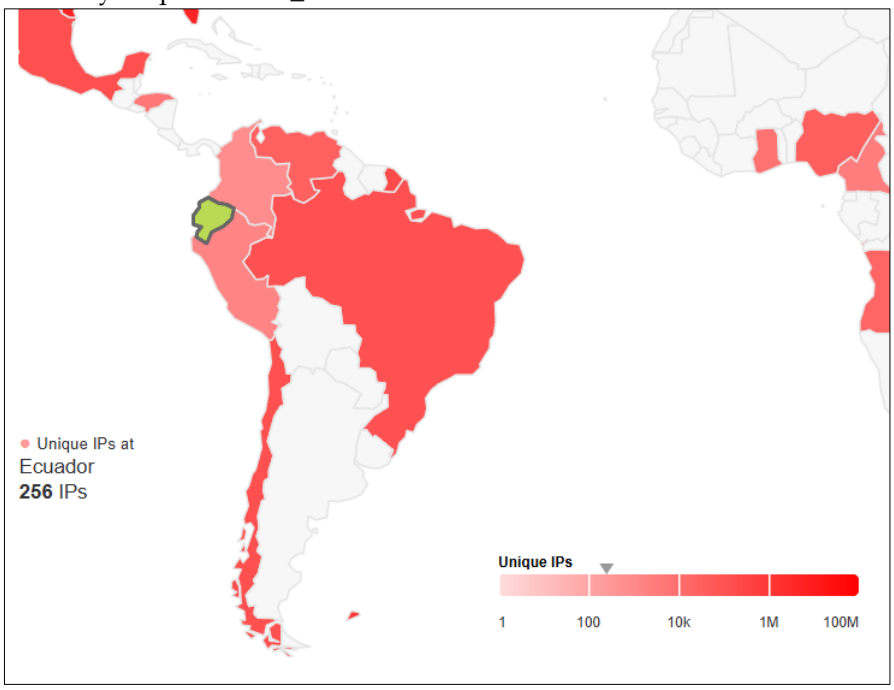
Aunque Ecuador está tomando pasos importantes para mejorar su marco legal en ciberseguridad, los avances son lentos, y la falta de una infraestructura robusta y la limitada denuncia de delitos complican la lucha contra el ciberdelito. Es necesario un esfuerzo conjunto entre el gobierno, el sector privado y la sociedad para fortalecer la ciberseguridad y garantizar que la legislación sea efectiva en la protección de los ciudadanos y sus datos

DISCUSIÓN

Por el uso de las redes sociales se dan varios tipos de delitos, el cibercrimen está generando importantes repercusiones en la economía mundial, la seguridad nacional, la estabilidad social y los intereses individuales. Los esfuerzos actuales para enfrentar las amenazas del ciberdelito se enfocan principalmente en medidas técnicas.

De acuerdo con la lista negra de FireHOL IP sitio que analiza todas las fuentes de IP de seguridad disponibles, principalmente relacionadas con ataques en línea, abuso de servicios en línea, malware, botnets, servidores de comando y control y otras actividades de ciberdelito.

Figura 2
Country Map of firehol_level1. IPIP.Net



Nota. información de FireHOL IP

El análisis de FireHOL IP, particularmente del mapa de países firehol_level1, nos proporciona una visión de los países donde se detectan direcciones IP potencialmente maliciosas o abusivas. La herramienta evalúa y compara las IPs reportadas en diferentes bases de datos de ubicación, como MaxMind GeoLite2, IPDeny.com, IP2Location.com Lite e IPIP.net. Esta combinación ayuda a identificar las IPs por país y permite a los usuarios de FireHOL decidir si desean bloquear o monitorear el tráfico entrante y saliente hacia ciertas direcciones IP.

El mapa indica que Ecuador tiene actualmente 256 direcciones IP incluidas en la lista negra de FireHOL. Esto es significativo porque:

1. Indicador de Riesgo en la Región: La presencia de 256 IPs en Ecuador en esta lista sugiere que el país está siendo notado como una fuente de posibles ciberamenazas o actividades de abuso. Puede deberse tanto a usuarios finales comprometidos en redes de bots como a servidores comprometidos utilizados para actividades maliciosas, como ataques de denegación de servicio, envío de spam o propagación de malware.
2. Impacto para Usuarios Ecuatorianos: Al aplicar esta lista en un firewall, las 256 IPs identificadas en Ecuador podrían bloquear el acceso de usuarios legítimos si estas direcciones pertenecen a clientes no involucrados en actividades maliciosas, ya que las listas de bloqueo no son completamente infalibles. Esto plantea un desafío para empresas y proveedores de servicios en Ecuador, quienes podrían ver restricciones en el tráfico hacia sus clientes y potenciales interrupciones de servicio.
3. Reputación de Direcciones IP en Ecuador: Las direcciones IP ecuatorianas incluidas en la lista de FireHOL podrían afectar la reputación de los proveedores de servicios de internet (ISP) en Ecuador, quienes deben estar atentos a la seguridad de sus redes y, si es posible, tomar medidas para investigar y mitigar la causa de estas inclusiones.
4. Estrategias de Mitigación: Los administradores de redes en Ecuador deben evaluar cuidadosamente la inclusión de FireHOL como una lista de bloqueo directa, dado el potencial de falsos positivos y el impacto en los clientes locales. FireHOL recomienda analizar primero

las IPs incluidas y posiblemente emplear estrategias de monitoreo en lugar de un bloqueo directo de todo el rango.

La inclusión de 256 IPs ecuatorianas en el mapa de FireHOL Level1 refleja una necesidad urgente de fortalecer las medidas de seguridad en redes y sistemas dentro de Ecuador. Si bien esta lista puede ser útil para identificar comportamientos sospechosos, es esencial que los administradores de red en Ecuador adopten un enfoque equilibrado, implementando medidas como el monitoreo y la revisión activa antes de aplicar bloqueos generalizados. Este enfoque preventivo no solo minimizará el riesgo de interrumpir las operaciones legítimas, sino que también permitirá una respuesta más específica y eficiente ante ciberamenazas reales, contribuyendo a la protección de infraestructuras críticas.

Sin embargo, incluso con herramientas como FireHOL y otras listas de bloqueo, la lucha contra los delitos informáticos, especialmente las estafas cibernéticas, enfrenta grandes obstáculos. Uno de los principales desafíos es la dificultad inherente en la sanción de estos delitos, debido a su naturaleza transnacional y al anonimato que otorgan las tecnologías de ocultación utilizadas por los ciberdelincuentes. Este anonimato y las diferencias legislativas entre países complican la identificación y persecución de los atacantes, lo que pone en evidencia la necesidad de fortalecer no solo las medidas de seguridad en las redes, sino también los marcos legales y la cooperación internacional para abordar eficazmente las amenazas cibernéticas. A pesar de los avances tecnológicos y la implementación de legislaciones específicas, la naturaleza transnacional de las redes sociales y el ciberespacio hace que la identificación y persecución de los infractores sea extremadamente compleja. Los ciberdelincuentes a menudo operan desde países con legislaciones más laxas o con un marco regulatorio débil, lo que dificulta la colaboración internacional entre autoridades judiciales. Además, los delitos informáticos suelen implicar una gran cantidad de anonimato para los atacantes, quienes emplean diversas herramientas de ocultación, como VPNs, proxies y criptomonedas, para proteger su identidad y localización, lo que incrementa aún más las dificultades para su localización y captura.

Las estafas cibernéticas, por ejemplo, son comunes en plataformas como redes sociales y sitios de comercio electrónico. Los estafadores utilizan métodos sofisticados para engañar a las víctimas, como la creación de perfiles falsos, la manipulación de sistemas de pago en línea y el phishing, entre otros. Estos delitos no solo afectan económicamente a las personas, sino que también socavan la confianza de los usuarios en las plataformas digitales, lo que puede tener repercusiones negativas a largo plazo en el desarrollo y uso de tecnologías emergentes. Una de las razones por las que la sanción efectiva se vuelve casi imposible es la falta de una normativa internacional uniforme. Las legislaciones sobre delitos informáticos varían considerablemente entre países, y muchos de ellos no cuentan con la infraestructura necesaria para hacer frente a la criminalidad digital de manera eficaz. Esto genera un vacío legal donde los ciberdelincuentes pueden actuar con impunidad, al menos temporalmente. En este sentido, es urgente que se fortalezcan los marcos regulatorios internacionales para facilitar la cooperación entre gobiernos y el intercambio de información, además de invertir en la capacitación de autoridades locales para mejorar su capacidad de respuesta frente a estos delitos.

En la discusión sobre la relevancia de este tema, también es fundamental abordar el impacto social de los delitos informáticos. Aunque la legislación es importante, igualmente lo es la educación y la prevención. La concientización pública sobre los riesgos de las estafas cibernéticas y la importancia de la seguridad en línea debe ser una prioridad, no solo para evitar daños financieros a las víctimas, sino también para fomentar una cultura digital más segura y responsable. Los usuarios deben estar informados sobre cómo identificar ataques de

phishing, el manejo adecuado de la privacidad en línea, y las mejores prácticas para protegerse en el ciberespacio.

De acuerdo con Ecuavisa en Ecuador El reto para combatir los ciberdelitos. La Policía Nacional ejecuta trabajos conjuntos para combatir esta amenaza y cuenta con el respaldo del convenio de Budapest, un acuerdo internacional integrado por 100 países para frenar los delitos en línea (Aguilar 2021). El reto para combatir los ciberdelitos sigue siendo un desafío, pero con la correcta prevención más ciudadanos pueden evitar ser víctimas.

La sanción efectiva de los delitos informáticos y las estafas sigue siendo una tarea monumental debido a la falta de uniformidad legal, el anonimato de los atacantes y la carencia de recursos en muchas regiones. Sin embargo, la cooperación internacional, el fortalecimiento de las normativas, la educación y la concientización pública son pasos clave para reducir la incidencia de estos delitos y garantizar un entorno digital más seguro para todos.

REFERENCIAS BIBLIOGRÁFICAS

Acurio, S. (2020). Delitos informáticos en el código orgánico integral penal (COIP). https://acortar.link/EYrSD6

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios internacionales (Santiago), 53(198), 169-197. http://dx.doi.org/10.5354/0719-3769.2021.57067

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal - Título IV Delitos contra la inviolabilidad del domicilio y la tranquilidad individual - Capítulo II De los atentados contra la vida privada - Sección I Violación al derecho a la intimidad.

Azeez, N. A., & Fadhal, E. (2023). Classification of virtual harassment on social networks using ensemble learning techniques. Applied Sciences (Switzerland), 13(7) doi:10.3390/app13074570

Azeez, N. A., Salaudeen, B. B., Misra, S., Damasevicius, R., & Maskeliunas, R. (2020). Identifying phishing attacks in communication networks using URL consistency features. International Journal of Electronic Security and Digital Forensics, 12(2), 200-213. doi:10.1504/IJESDF.2020.106318

Boyd, D. M., y Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., . . . Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1) doi:10.1057/s41599-023-01560-x

DataGuidance. (2021, diciembre 13). Ecuador: Cybersecurity Bill overview. https://acortar.link/TyycJh

De, L. 0. R. O. S. 180. (s/f). Código orgánico integral penal, COIP. Gob.ec. Recuperado el 13 de julio de 2024, de https://acortar.link/el9Tdb

De, L. 0. R. O. S. 22. (s/f). Ley organica de comunicacion. Gob.ec. Recuperado el 17 de agosto de 2024, de https://acortar.link/FLYST2

De, Ley 0. Registro Oficial Suplemento 175. (s/f). Ley para prevenir y erradicar la violencia contra las mujeres. Gob.ec. Recuperado el 18 de agosto de 2024, de https://acortar.link/hMRWa

El Universo. (2019). Delincuentes extorsionan a través de Facebook y WhatsApp en Ecuador. Recuperado de: https://acortar.link/pJiYjY

García Andrés A., Giusti Minotre F. y Jimenez Mata S. (2022). Adolescencia y violencia de género en línea: revisión comparativa entre Costa Rica, México y España. Sociedad e Infancias, 6(2), 165-177. https://doi.org/10.5209/soci.83596

González, L. (2017). Delincuencia en el siglo XXI: ¿nuevos desafíos o viejos problemas? Revista Criminológica, 55(2), 89-109.

Kaplan, A. M., y Haenlein, M. (2010). Users of the world unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68.

Ministerio del Interior de Ecuador. (2020). Estudio Nacional sobre Violencia Digital en Adolescentes, 2019. Recuperado de: https://acortar.link/JOPjbe

Televistazo. (2024, octubre 15). Tres tipos de ciberdelitos son los más frecuentes en Ecuador. Ecuavisa. https://acortar.link/BMSkiy

Tsaousis, C. (s/f). FireHOL IP lists. FireHOL IP Lists. Recuperado el 15 de septiembre de 2024, de https://iplists.firehol.org/

Universidad Central del Ecuador. (2020). Influencia de las redes sociales en la conducta delictiva juvenil.

Velasquez, F. (2019, octubre 9). Cybercrime in Ecuador: An asymmetrical threat — the security distillery. The Security Distillery. https://acortar.link/WEytpc

Vera, C. (2018). Redes sociales y delincuencia: una relación compleja. Diálogos Andinos, 56(1), 105-119.