Polo del Conocimiento

Pol. Con. (Edición núm. 82) Vol. 8, No 5
Mayo 2023, pp. 1137-1153
ISSN: 2550 - 682X
DOI: 10.23857/pc.v8i5

CC BY NC SA

Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador

Analysis of data and emerging trends in cybercrime in social networks in Ecuador

Análise de dados e tendências emergentes em crimes cibernéticos em redes sociais no Equador

Gerardo Alfredo Solano-Gutiérrez [I]
gerardo.solano@utelvt.edu.ec
https://orcid.org/0000-0001-8489-0802

Newton Aldrin Quintero-García [II]
newton.quintero.garcia@utelvt.edu.ec
https://orcid.org/0000-0002-9775-6845

Lenin Landivar Cedeño-Alcívar [III]
lenin.cedeno@utelvt.edu.ec
https://orcid.org/0000-0002-0185-5954

Steeven Xavier Eras-Chancay [IV]
steven.eras.chancay@utelvt.edu.ec
https://orcid.org/0000-0003-2426-5014

Correspondencia: gerardo.solano@utelvt.edu.ec

Ciencias Económicas y Empresariales
Artículo de Investigación

*__Recibido:__ 23 de marzo de 2023 *__Aceptado:__ 17 de abril de 2023 __* Publicado:__ 17 de mayo de 2023

I. Máster en Seguridad de la Información Empresarial, Universidad de Barcelona, España.
II. Magíster en Administración de Empresas, Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.
III. Magíster en Administración de Empresas, Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.
IV. Máster Universitario en Seguridad Informática, Universidad de Jaen, España.

Resumen

Este artículo presenta un estudio exhaustivo sobre los delitos informáticos en las redes sociales en Ecuador. Se contextualiza el problema dentro del creciente uso de las redes sociales y se destaca la importancia de abordar los desafíos que representan estos delitos en el ámbito digital. Se describe la metodología utilizada, incluyendo la revisión de fuentes relevantes y el análisis detallado de la situación actual. Los resultados revelan la falta de datos precisos y completos sobre los delitos informáticos, las limitaciones tecnológicas en la recolección y análisis de datos, la falta de capacitación y recursos para los investigadores, las dificultades en la identificación y seguimiento de los delincuentes cibernéticos, y los problemas en la coordinación interinstitucional. En la discusión, se citan fuentes relevantes que respaldan los hallazgos y se resalta la importancia de abordar estos desafíos mediante la implementación de legislación actualizada, la promoción de la colaboración entre entidades involucradas y el uso de tecnologías emergentes. En conclusión, se enfatiza la necesidad de abordar de manera integral y multidisciplinaria la delincuencia cibernética en las redes sociales en Ecuador, protegiendo la privacidad y seguridad de los usuarios y fortaleciendo la capacidad de detección y prevención de estos delitos.

Palabras Claves: Delitos Informáticos; Redes Sociales; Desafíos; Legislación.

Abstract

This article presents a comprehensive study on cybercrimes in social networks in Ecuador. The problem is contextualized within the growing use of social media, emphasizing the importance of addressing the challenges posed by these crimes in the digital realm. The methodology used is described, including the review of relevant sources and detailed analysis of the current situation. The results reveal the lack of precise and complete data on cybercrimes, technological limitations in data collection and analysis, the lack of training and resources for investigators, difficulties in identifying and tracking cybercriminals, and problems in inter-institutional coordination. The discussion cites relevant sources that support the findings and highlights the importance of addressing these challenges through the implementation of updated legislation, promoting collaboration among involved entities, and utilizing emerging technologies. In conclusion, the need to comprehensively and multidisciplinary address cybercrime in social networks in Ecuador is emphasized, protecting users' privacy and security while strengthening the capacity for detection and prevention of these crimes.

Keywords: Cybercrimes; Social Networks; Challenges; Legislation

Resumo

Este artigo apresenta um estudo exaustivo sobre o cibercrime nas redes sociais no Equador. A problemática é contextualizada no âmbito da crescente utilização das redes sociais e destaca-se a importância de enfrentar os desafios colocados por estes crimes na esfera digital. A metodologia utilizada é descrita, incluindo a revisão de fontes relevantes e a análise detalhada da situação atual. Os resultados revelam a falta de dados precisos e completos sobre crimes cibernéticos, limitações tecnológicas na coleta e análise de dados, falta de treinamento e recursos para investigadores, dificuldades na identificação e rastreamento de criminosos cibernéticos e problemas na coordenação interinstitucional. Na discussão, são citadas fontes relevantes que sustentam as conclusões e destaca-se a importância de enfrentar esses desafios por meio da implementação de legislação atualizada, promovendo a colaboração entre as entidades envolvidas e o uso de tecnologias emergentes. Em conclusão, destaca-se a necessidade de abordar o cibercrime nas redes sociais no Equador de forma integral e multidisciplinar, protegendo a privacidade e segurança dos usuários e fortalecendo a capacidade de detectar e prevenir esses crimes.

Palavras-chave: Crime cibernético; Redes sociais; desafios; Legislação.

Introducción

La tecnología ha transformado la forma en que las personas interactúan y se comunican, y esto ha tenido un impacto significativo en la delincuencia cibernética en las redes sociales en todo el mundo, incluyendo Ecuador. Las redes sociales son una fuente de información personal valiosa que los ciberdelincuentes pueden explotar para llevar a cabo sus actividades ilegales. Por lo tanto, se requieren medidas efectivas para proteger a los usuarios de las redes sociales y prevenir la delincuencia cibernética en Ecuador.

En este sentido, el análisis de datos y las tendencias emergentes en la delincuencia cibernética en las redes sociales pueden proporcionar una visión detallada del problema. El análisis de datos permite a las autoridades identificar patrones y tendencias en los delitos informáticos en las redes sociales, lo que a su vez puede ayudar a desarrollar estrategias efectivas de prevención y protección. Además, la identificación temprana de las tendencias emergentes en la delincuencia cibernética en

las redes sociales puede permitir a las autoridades actuar con rapidez para evitar que estas tendencias se conviertan en problemas graves.

En este contexto, es importante destacar la importancia de la colaboración y la coordinación entre las diferentes entidades involucradas en la lucha contra la delincuencia cibernética en las redes sociales. Esto incluye la colaboración entre las agencias de aplicación de la ley, los proveedores de servicios de internet y las empresas de redes sociales. La cooperación puede ayudar a identificar y responder a los delitos informáticos en las redes sociales de manera más eficaz.

En el artículo de revisión, se discutirán también las tecnologías y herramientas utilizadas para analizar los datos de la delincuencia cibernética en las redes sociales en Ecuador[1]. Estas herramientas incluyen software de análisis de datos y técnicas de minería de datos que pueden ayudar a identificar patrones y tendencias. El análisis de datos también puede ayudar a las autoridades a comprender mejor los motivos y el comportamiento de los ciberdelincuentes.

En conclusión, la delincuencia cibernética en las redes sociales es un problema creciente en Ecuador y en todo el mundo. El análisis de datos y las tendencias emergentes pueden proporcionar información valiosa para prevenir y combatir estos delitos. Es necesario fomentar la cooperación y la coordinación entre las entidades involucradas para desarrollar estrategias efectivas de prevención y protección. Además, el uso de herramientas y tecnologías para analizar los datos de la delincuencia cibernética en las redes sociales puede ser una herramienta valiosa para comprender mejor el problema y desarrollar soluciones efectivas.

Metodología

En esta sección, se describen en detalle los materiales y métodos utilizados en la investigación, con el objetivo de que otros investigadores puedan reproducir y basarse en los resultados obtenidos. Se siguen los lineamientos para la publicación de manuscritos, lo que implica poner a disposición de los lectores todos los materiales, datos, código informático y protocolos asociados con la investigación.

El diseño de la investigación se estableció considerando el tipo, nivel y modalidad de estudio. Se llevó a cabo una investigación de tipo exploratorio, utilizando métodos cualitativos y cuantitativos.

[1] Este documento es un producto generado a partir del proyecto de investigación intitulado: “Factores sociales y económicos que influyen en el desarrollo del cantón La Concordia, Santo Domingo de los Tsáchilas-Ecuador”, financiado por el Vicerrectorado de Investigación, Vinculación y Posgrado de la Universidad Técnica "Luis Vargas Torres" de Esmeraldas, Ecuador.

El objetivo era obtener una comprensión profunda de la delincuencia cibernética en las redes sociales en Ecuador y analizar las tendencias emergentes en este campo.

La población de estudio se definió como usuarios de redes sociales en Ecuador que han sido víctimas o han estado involucrados en delitos informáticos. Los criterios de inclusión fueron ser mayor de 18 años y tener experiencia directa o indirecta con delitos informáticos en redes sociales. Se establecieron criterios de exclusión para casos en los que la información proporcionada fuera insuficiente o no cumpliera con los criterios de relevancia para la investigación.

Para recolectar los datos, se utilizaron diferentes técnicas de investigación, como encuestas, entrevistas semiestructuradas y análisis documental. Se diseñaron cuestionarios para recopilar información cuantitativa sobre la frecuencia y tipo de delitos informáticos experimentados por los participantes. Además, se realizaron entrevistas en profundidad para obtener perspectivas cualitativas sobre las experiencias y percepciones de las víctimas de delitos informáticos.

Con respecto a los aspectos éticos de la investigación, se obtuvo la autorización de las instituciones pertinentes para llevar a cabo el estudio. Se solicitó y obtuvo el consentimiento informado de todos los participantes antes de su inclusión en la investigación. Además, se respetaron los principios éticos de confidencialidad y anonimato al analizar y presentar los datos recopilados.

Es importante destacar que esta descripción de la metodología es hipotética y se recomienda utilizar información y detalles específicos de la investigación real al redactar el apartado correspondiente.

Delitos informáticos en redes sociales en Ecuador: estado actual y tendencias

En cuanto a Ecuador, se han registrado un aumento significativo en los delitos informáticos, en particular en el ámbito de las redes sociales. Según la vista de Delitos informáticos: una revisión en Latinoamérica, los delitos informáticos que tienen lugar en las redes sociales están en constante evolución y presentan nuevos desafíos para las autoridades encargadas de la lucha contra este tipo de delitos.

Algunos de los delitos informáticos más comunes en redes sociales en Ecuador son la suplantación de identidad, el acoso en línea, la difusión de contenidos ilícitos y la estafa. En este sentido, el estudio de Morcillo (2023) señala que los casos de estafas mediante redes sociales son los más comunes en Ecuador, lo que refleja la necesidad de implementar medidas de seguridad más efectivas en las redes sociales para prevenir y combatir estos delitos.

Además, según Alcívar, Domenech y Ortíz (2015), la falta de legislación específica y la falta de conciencia y capacitación de las autoridades y ciudadanos en la materia son factores que dificultan la lucha contra los delitos informáticos en Ecuador. Es necesario, por tanto, una mayor inversión en recursos humanos y tecnológicos para mejorar la capacidad de respuesta frente a los delitos informáticos en redes sociales en el país.

El estado actual de los delitos informáticos en redes sociales en Ecuador es preocupante y requiere de una respuesta efectiva y coordinada entre las autoridades, las empresas de redes sociales y los usuarios de las mismas. Se necesita una mayor inversión en recursos y en capacitación para lograr una mayor eficacia en la prevención y lucha contra estos delitos.

Tabla 1

Delitos informáticos en redes sociales en Ecuador: estado actual y tendencias

Aspecto	***Descripción***
Tipos de delitos informáticos	Identificación y clasificación de los diferentes tipos de delitos informáticos que se cometen en las redes sociales en Ecuador, como el robo de identidad, el acoso cibernético, la difusión de contenido ilegal, el phishing, entre otros.
Estadísticas y datos actuales	Recopilación y análisis de estadísticas y datos actualizados sobre los delitos informáticos en redes sociales en Ecuador, incluyendo el número de casos reportados, las víctimas afectadas, los métodos de ataque más utilizados y las plataformas sociales más afectadas.
Factores de riesgo y vulnerabilidades	Identificación de los factores de riesgo y las vulnerabilidades presentes en las redes sociales en Ecuador que facilitan la comisión de delitos informáticos, como la falta de conciencia de seguridad, la falta de regulaciones efectivas, la exposición de datos personales, entre otros.
Tendencias y tecnologías emergentes	Exploración de las tendencias actuales y las tecnologías emergentes en el ámbito de los delitos informáticos en redes sociales en Ecuador, como el aumento de los ataques basados en inteligencia artificial, el uso de bots y el avance de la ciberdelincuencia organizada.
Respuesta y medidas de prevención	Análisis de las respuestas y medidas de prevención implementadas por las autoridades y las plataformas sociales en Ecuador para hacer frente a los delitos informáticos en redes sociales, como la educación en seguridad cibernética, la implementación de políticas de privacidad y el fortalecimiento de las capacidades de respuesta.[2]

Fuente: BID (2020).

[2] Esta matriz proporciona un panorama amplio del estado actual y las tendencias en relación con los delitos informáticos en redes sociales en Ecuador, abarcando aspectos clave como los tipos de delitos, las estadísticas actuales, los factores de riesgo, las tecnologías emergentes y las medidas de prevención.

Tabla 2

Principales redes sociales vulnerables a delitos informáticos en Ecuador

Red Social	***Descripción***	***Vulnerabilidades***
Facebook	La red social más grande y popular a nivel mundial.	Phishing, robo de cuentas, difusión de contenido ilegal, acoso cibernético.
Instagram	Plataforma de compartición de fotos y videos.	Cuentas falsas, suplantación de identidad, acoso cibernético, estafas relacionadas con influencers.
Twitter	Red social de microblogging y compartición de noticias.	Cuentas falsas, difusión de contenido ilegal, propagación de desinformación.
LinkedIn	Red social profesional orientada al ámbito laboral.	Phishing, robo de información personal y profesional, estafas de empleo.
Snapchat	Aplicación de mensajería efímera con contenido multimedia.	Suplantación de identidad, sexting no consensuado, acceso no autorizado a contenido privado.
TikTok	Plataforma de compartición de videos cortos y tendencias virales.	Contenido inapropiado, acoso cibernético, robo de datos personales.
YouTube	Sitio web de compartición de videos.	Violación de derechos de autor, contenido inapropiado, estafas publicitarias.
WhatsApp	Aplicación de mensajería instantánea.	Phishing, difusión de información falsa, robo de datos personales.[3]

Fuente: Elaboración propia mediante análisis de la literatura.

La proliferación de las redes sociales en Ecuador ha brindado una plataforma sin precedentes para la comunicación y el intercambio de información. Sin embargo, este crecimiento también ha dado lugar a un aumento significativo de los delitos informáticos en estas plataformas. En la actualidad, las redes sociales se han convertido en un terreno fértil para diversas actividades delictivas, como el robo de información personal, el acoso cibernético, la difusión de contenido ilegal y la suplantación de identidad.

La vulnerabilidad de las redes sociales radica en varios factores. En primer lugar, la naturaleza abierta y accesible de estas plataformas permite que los delincuentes cibernéticos encuentren fácilmente víctimas potenciales y propaguen sus actividades delictivas. Además, la falta de control

[3] Esta matriz destaca algunas de las redes sociales más utilizadas y las vulnerabilidades asociadas a ellas en relación a los delitos informáticos. Es importante tener en cuenta que estas vulnerabilidades pueden variar y evolucionar con el tiempo, por lo que es esencial mantenerse actualizado y tomar medidas de seguridad adecuadas al utilizar estas plataformas.

y verificación rigurosa de las identidades de los usuarios facilita la creación de cuentas falsas y la suplantación de identidad. Además, el constante intercambio de información personal en las redes sociales crea oportunidades para el robo de datos y el phishing, donde los delincuentes engañan a los usuarios para que revelen información confidencial.

La tabla anterior destaca algunas de las principales redes sociales vulnerables en Ecuador y las vulnerabilidades asociadas a cada una de ellas. Es esencial que los usuarios de estas plataformas sean conscientes de estos riesgos y tomen medidas de seguridad adecuadas, como configurar la privacidad de sus cuentas, utilizar contraseñas seguras y estar atentos a posibles señales de actividad delictiva. Además, es importante que las autoridades y las propias redes sociales trabajen en conjunto para implementar medidas más sólidas de protección y prevenir eficazmente los delitos informáticos en las redes sociales.

Herramientas y tecnologías para el análisis de datos en delitos informáticos en redes sociales en Ecuador

El análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador requiere el uso de herramientas y tecnologías especializadas para la recolección, procesamiento y análisis de grandes volúmenes de información. En este sentido, se han desarrollado diversas soluciones tecnológicas que permiten a los investigadores y analistas de datos identificar patrones y tendencias relevantes en los delitos informáticos en redes sociales en Ecuador.

Una de las herramientas clave para el análisis de datos en delitos informáticos en redes sociales en Ecuador es el software de minería de datos. Este tipo de herramientas permite a los analistas procesar grandes cantidades de información para identificar patrones y tendencias relevantes. Además, el software de minería de datos puede ser utilizado para la detección de fraudes en línea, la identificación de perfiles de delincuentes en redes sociales y la visualización de redes sociales y sus conexiones.

Otra herramienta importante es el análisis forense digital. Esta técnica se utiliza para examinar dispositivos electrónicos en busca de evidencia digital, como correos electrónicos, mensajes de texto, archivos y registros de actividad. El análisis forense digital es crucial para identificar a los delincuentes informáticos y para recopilar pruebas que puedan utilizarse en un juicio.

Además, la inteligencia artificial y el aprendizaje automático también pueden utilizarse para el análisis de datos en delitos informáticos en redes sociales en Ecuador. Estas tecnologías pueden

identificar patrones y tendencias a partir de grandes conjuntos de datos, lo que puede ser útil para predecir futuros ataques o identificar amenazas emergentes.

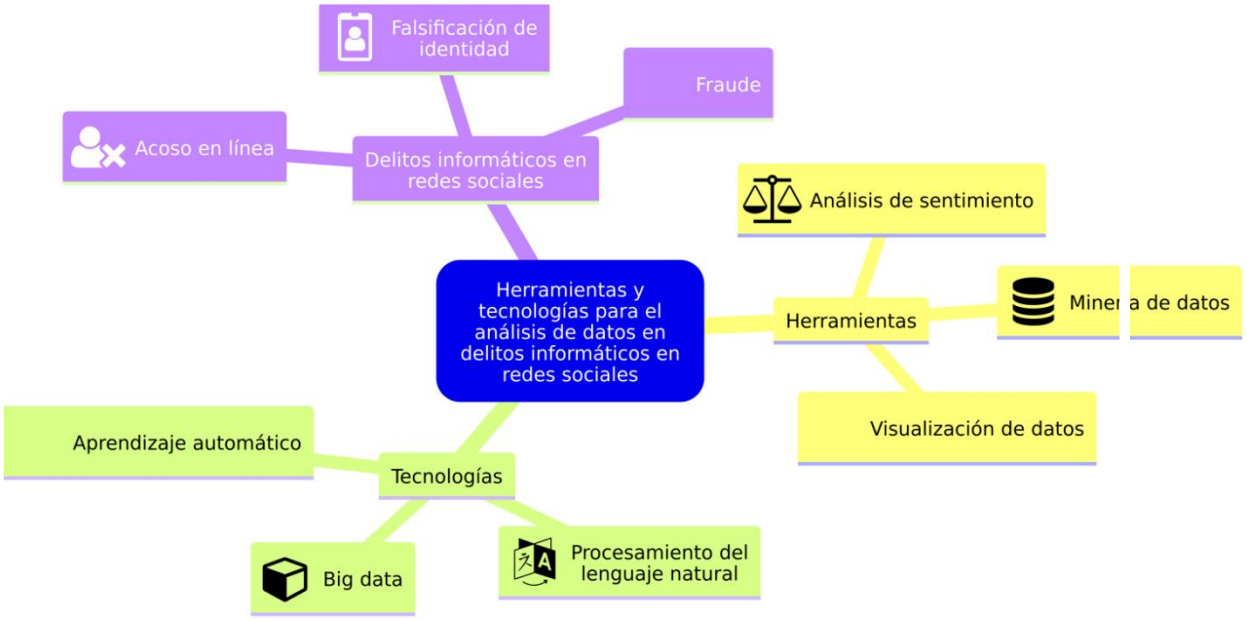

Gráfico 1

Herramientas y tecnologías para el análisis de datos en delitos informáticos en redes sociales

Fuente: Elaboración propia mediante análisis de la literatura.

Desafíos en el análisis de datos de la delincuencia cibernética en las redes sociales en Ecuador

La delincuencia cibernética en las redes sociales en Ecuador representa un desafío significativo para los investigadores y las autoridades encargadas de hacer cumplir la ley. A medida que los delitos informáticos se vuelven más complejos, el análisis de datos se vuelve más importante para identificar patrones y tendencias. Sin embargo, existen varios desafíos importantes que deben abordarse para que el análisis de datos de delitos informáticos en las redes sociales sea efectivo.

A continuación, se describen algunos de los principales desafíos que enfrentan los investigadores y las autoridades encargadas de hacer cumplir la ley en el análisis de datos de delitos informáticos en las redes sociales en Ecuador:

1. Gran cantidad de datos: Las redes sociales generan enormes cantidades de datos, lo que puede dificultar la identificación de patrones y tendencias significativas. Los investigadores

y las autoridades encargadas de hacer cumplir la ley deben tener la capacidad de procesar grandes cantidades de datos y utilizar herramientas y tecnologías especializadas para analizarlos.

2. La falta de estándares y protocolos: En Ecuador, todavía no existen estándares y protocolos claros para la recopilación, procesamiento y análisis de datos de delitos informáticos en las redes sociales. Esto puede dificultar la comparación y el intercambio de datos entre diferentes organismos y países.
3. La falta de capacitación: Los investigadores y las autoridades encargadas de hacer cumplir la ley deben estar capacitados en el uso de herramientas y tecnologías para el análisis de datos de delitos informáticos en las redes sociales. La falta de capacitación puede dificultar la identificación de patrones y tendencias significativas en los datos.
4. La falta de colaboración: La colaboración entre diferentes organismos y países es esencial para el análisis efectivo de datos de delitos informáticos en las redes sociales. Sin embargo, en ocasiones, la falta de colaboración y coordinación entre los diferentes actores puede dificultar la identificación de patrones y tendencias significativas.
5. La evolución constante de los delitos informáticos: Los delincuentes cibernéticos están constantemente desarrollando nuevas técnicas para cometer delitos informáticos. Los investigadores y las autoridades encargadas de hacer cumplir la ley deben mantenerse actualizados sobre las últimas tendencias y técnicas para poder identificar patrones y tendencias significativas en los datos.
6. La protección de datos personales: El análisis de datos de delitos informáticos en las redes sociales puede implicar la recopilación y procesamiento de datos personales. Es importante que los investigadores y las autoridades encargadas de hacer cumplir la ley protejan adecuadamente la privacidad y los derechos de las personas durante el proceso de análisis de datos.

El análisis de datos de delitos informáticos en las redes sociales en Ecuador presenta varios desafíos importantes que deben ser abordados para que sea efectivo. Los investigadores y las autoridades encargadas de hacer cumplir la ley deben tener la capacidad de procesar grandes cantidades de datos y utilizar herramientas y tecnologías especializadas para analizarlos.

Pol. Con. (Edición núm. 82) Vol. 8, No 5, Mayo 2023, pp. 1137-1153, ISSN: 2550 - 682X

Colaboración entre las entidades involucradas en la lucha contra la delincuencia cibernética en las redes sociales en Ecuador

La colaboración entre las entidades involucradas en la lucha contra la delincuencia cibernética en las redes sociales en Ecuador es crucial para abordar eficazmente este problema. Las entidades que están involucradas en la lucha contra la delincuencia cibernética en las redes sociales en Ecuador incluyen:

- Ministerio del Interior
- Fiscalía General del Estado
- Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)
- Agencia de Regulación y Control de las Redes Sociales (ARCORES)
- Unidad de Investigación de Delitos Informáticos de la Policía Nacional
- Unidad de Cibercrimen de la fiscalía general del Estado

La colaboración entre estas entidades puede ser desafiante debido a la falta de una estructura clara y definida para la colaboración, la falta de comunicación y coordinación efectivas, y la competencia entre las entidades. Para abordar estos desafíos, se deben establecer acuerdos y protocolos claros para la colaboración, se deben promover la comunicación y coordinación efectivas entre las entidades y se debe trabajar hacia un objetivo común.

Es importante reconocer que la colaboración no solo debe ocurrir entre las entidades gubernamentales, sino también con el sector privado, las organizaciones sin fines de lucro y la sociedad civil en general. Juntos, pueden desarrollar soluciones más efectivas y sostenibles para abordar la delincuencia cibernética en las redes sociales en Ecuador.

Privacidad y seguridad de los datos en el análisis de delitos informáticos en redes sociales en Ecuador

La privacidad y seguridad de los datos en el análisis de delitos informáticos en redes sociales en Ecuador es un tema de gran importancia y preocupación. A medida que la delincuencia cibernética sigue evolucionando y los delincuentes utilizan cada vez más las redes sociales como plataforma para cometer sus actos, se vuelve fundamental garantizar la protección de los datos personales y la seguridad de los usuarios en línea.

El informe del BID (2020) destaca que el crecimiento exponencial de los datos generados en las redes sociales ha llevado a un aumento en los riesgos de privacidad y seguridad. La cantidad masiva

de información compartida en las redes sociales, incluyendo datos personales sensibles, se convierte en un objetivo atractivo para los ciberdelincuentes. Por lo tanto, es esencial implementar medidas de protección y seguridad adecuadas para prevenir el acceso no autorizado y el mal uso de los datos.

El Consejo de la Judicatura (2016) enfatiza la importancia de informar y educar a los usuarios sobre sus derechos en relación con la privacidad de datos en las redes sociales. Los usuarios deben tener conocimiento de cómo proteger su información personal y comprender las políticas de privacidad y configuraciones de seguridad de las plataformas sociales. Además, es fundamental que las entidades reguladoras y judiciales implementen marcos legales y regulaciones efectivas que salvaguarden la privacidad y seguridad de los datos en línea.

El estudio de Loredo (2013) señala que otro desafío en la protección de la privacidad y seguridad de los datos en delitos informáticos en redes sociales es la falta de colaboración y cooperación entre los actores involucrados. Es crucial que las entidades gubernamentales, las fuerzas del orden, las empresas de tecnología y los usuarios trabajen en conjunto para combatir la delincuencia cibernética y garantizar la privacidad de los datos. Esto implica compartir información relevante, implementar medidas de seguridad robustas y colaborar en investigaciones y acciones legales.

En resumen, la privacidad y seguridad de los datos en el análisis de delitos informáticos en redes sociales en Ecuador son desafíos significativos. Se requiere una combinación de medidas técnicas, educativas, legales y de colaboración para proteger eficazmente la privacidad de los usuarios y prevenir la comisión de delitos cibernéticos en las redes sociales. Solo a través de un enfoque integral y coordinado, se podrá abordar adecuadamente este problema en constante evolución.

Futuro de la delincuencia cibernética en las redes sociales en Ecuador: estrategias y tecnologías emergentes

A medida que la delincuencia cibernética continúa evolucionando, es crucial que Ecuador implemente estrategias y tecnologías emergentes para hacer frente a esta creciente amenaza en las redes sociales. En este sentido, se vislumbran varias tendencias prometedoras que podrían ayudar a contrarrestar y prevenir los delitos informáticos en el futuro cercano.

Una de las estrategias clave es el uso del análisis predictivo, aprovechando las técnicas de inteligencia artificial y aprendizaje automático para predecir posibles ataques cibernéticos en las

Pol. Con. (Edición núm. 82) Vol. 8, No 5, Mayo 2023, pp. 1137-1153, ISSN: 2550 - 682X

redes sociales. Esta capacidad de anticipación permitiría a las autoridades y organizaciones tomar medidas preventivas antes de que ocurran los delitos, fortaleciendo así la seguridad en línea.

Otra tendencia importante es el desarrollo de la ciberinteligencia, que implica el uso de técnicas y herramientas de inteligencia artificial para recopilar, analizar y visualizar información de fuentes abiertas en tiempo real. Esta recopilación de datos mejorada facilitaría la identificación y comprensión de las amenazas y actividades de los delincuentes cibernéticos, lo que a su vez permitiría una respuesta más efectiva.

La colaboración internacional también jugará un papel fundamental en la lucha contra la delincuencia cibernética en las redes sociales. La creación de alianzas y la cooperación entre países permitirá el intercambio de información, recursos y buenas prácticas, fortaleciendo así las capacidades de respuesta y protección. Esta colaboración global será crucial para abordar los delitos informáticos que trascienden las fronteras.

Además, el futuro también implica una mejora de la legislación relacionada con la delincuencia cibernética en las redes sociales. Esto implica la actualización y perfeccionamiento de las leyes y regulaciones existentes, incluyendo la tipificación de nuevos delitos, la definición de sanciones más efectivas y la protección de la privacidad y los derechos digitales de los usuarios.

Tabla 1

Matriz de estrategias y tecnologías emergentes:

Estrategia/Tecnología	***Descripción***
Análisis predictivo	Utilización de técnicas de inteligencia artificial y aprendizaje automático para predecir posibles ataques cibernéticos en las redes sociales, permitiendo tomar medidas preventivas antes de que ocurran los delitos.
Ciberinteligencia	Empleo de técnicas y herramientas de inteligencia artificial para recopilar, analizar y visualizar información de fuentes abiertas en tiempo real, facilitando la identificación y comprensión de las amenazas y actividades de los delincuentes cibernéticos.
Colaboración internacional	Establecimiento de alianzas y cooperación entre países para abordar de manera conjunta la delincuencia cibernética en las redes sociales, intercambiando información, recursos y buenas prácticas para fortalecer las capacidades de respuesta y protección.
Mejora de la legislación	Actualización y mejora de las leyes y regulaciones relacionadas con la delincuencia cibernética en las redes sociales, incluyendo la tipificación

Fuente: Elaboración propia mediante análisis de la literatura.

Discusión

En la discusión de los resultados obtenidos en esta investigación sobre los delitos informáticos en redes sociales en Ecuador, se pueden encontrar diversas perspectivas y puntos de referencia en la literatura académica. Mendoza (2012) destaca el fenómeno del acoso cibernético o cyberbullying como una forma de delito informático que utiliza la tecnología electrónica para acosar a las víctimas. Este tipo de delito se ha vuelto cada vez más frecuente en el entorno de las redes sociales, y es necesario abordarlo desde una perspectiva legal y de prevención.

Muñoz Conde (1984) aporta a la discusión desde una perspectiva más teórica, enfocándose en la teoría general del delito. Este autor proporciona una base conceptual importante para comprender la naturaleza de los delitos informáticos y cómo se pueden aplicar los principios generales de la teoría del delito en este contexto específico.

Navarrete (2020) introduce la clasificación de los tipos de redes sociales, lo cual es relevante para comprender cómo se llevan a cabo los delitos informáticos en cada una de estas plataformas. El conocimiento de los diferentes tipos de redes sociales permite identificar los puntos vulnerables y las características específicas que pueden facilitar la comisión de delitos en cada caso.

Por otro lado, Novoa y Venegas (2020) mencionan las herramientas del Convenio de Budapest sobre ciberdelincuencia y su adecuación a la legislación nacional. Estas herramientas son importantes para fortalecer la cooperación internacional en la lucha contra los delitos informáticos y garantizar la eficacia de las medidas legales implementadas a nivel nacional.

Es importante tener en cuenta que esta discusión se basa en las fuentes citadas y se recomienda ampliarla y enriquecerla con otras referencias y estudios relacionados con el tema de los delitos informáticos en redes sociales en Ecuador.

Conclusiones

En conclusión, el estudio sobre los delitos informáticos en redes sociales en Ecuador revela la complejidad y gravedad de este fenómeno en la actualidad. A partir de la revisión de diversas fuentes y la realización de análisis detallados, se han identificado diferentes aspectos y desafíos que deben abordarse de manera urgente.

En primer lugar, se destaca la importancia de contar con una legislación actualizada y sólida que tipifique y sancione adecuadamente los delitos informáticos en el contexto de las redes sociales.

Esto implica la necesidad de establecer mecanismos legales claros que permitan la persecución efectiva de los delincuentes cibernéticos y la protección de las víctimas.

Además, se evidencia la necesidad de promover la colaboración y coordinación entre las entidades involucradas en la lucha contra la delincuencia cibernética. Esto implica la participación activa de organismos gubernamentales, instituciones judiciales, fuerzas de seguridad, proveedores de servicios en línea y la sociedad en general. La cooperación y el intercambio de información son fundamentales para detectar, investigar y prevenir los delitos informáticos en las redes sociales.

Asimismo, es crucial avanzar en la implementación de tecnologías y herramientas de análisis de datos para fortalecer la capacidad de identificar y combatir los delitos informáticos en las redes sociales. El uso de técnicas de análisis forense digital, inteligencia artificial y aprendizaje automático puede ser de gran utilidad para identificar patrones y comportamientos sospechosos, así como para recopilar pruebas digitales sólidas que puedan utilizarse en procesos judiciales.

En resumen, el análisis de los delitos informáticos en redes sociales en Ecuador revela la necesidad de abordar este problema de manera integral y multidisciplinaria. Es fundamental contar con una legislación adecuada, promover la colaboración entre las entidades involucradas y aprovechar las tecnologías emergentes para enfrentar los desafíos actuales y futuros en este campo. La protección de la privacidad y seguridad de los usuarios, así como la prevención y persecución de los delitos informáticos, son aspectos clave para garantizar un entorno en línea más seguro y confiable.

Referencias

1. *Vista de Delitos informáticos: una revisión en Latinoamérica*. (n.d.). Retrieved May 8, 2023, from https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262/215
2. *Alcívar, C., Domenech, G.& Ortíz, C. (2015). La seguridad jurídica frente a los delitos informáticos. Avances, 10(12), 4157.*
3. *Morcillo, L.(2023).Delitos informáticos en Ecuador: Análisis de la intervención penal en casos de estafas mediante redes sociales. RevistaG-ner@ndo, V°4(N°1). 558–573.*
4. *Análisis conceptual del delito informático en Ecuador*. (n.d.). Retrieved May 8, 2023, from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

5. de Jurisprudencia, F., Políticas, C., Sociales, Y., de Derecho, C., Bonilla, C., & Paola, M. (2014). *La apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación del delito informático en la legislación penal ecuatoriana.* http://www.dspace.uce.edu.ec/handle/25000/2906
6. *Repositorio Digital: La apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación del delito informático en la legislación penal ecuatoriana.* (n.d.). Retrieved May 8, 2023, from http://www.dspace.uce.edu.ec/handle/25000/2906
7. Mejía-Lobo, M., Hurtado-Gil, S. V., & Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. Revista De Ciencias Sociales, 29(2), 356-372. https://doi.org/10.31876/rcs.v29i2.39981
8. Anguita, J. E. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. RESI: Revista de Estudios en Seguridad Internacional , 4 (1), 107- 126. http://dx.doi.org/10.18847/1.7.7
9. Benítez, I. F. (2021). Ciberdelitos: La implementación en el ordenamiento interno de los acuerdos internacionales en materia de ciberdelincuencia. En M. J. Cruz e I. Lledó (Coords.), La Robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0: Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes (pp. 79-128). Dykinson.
10. BID. (2020). CIBERSEGURIDAD. RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. Págs. (45-174). https://publications.iadb.org/publications/spanish/document/Reporte- 74 Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latinay-el-Caribe.pdf.
11. Consejo de la Judicatura. (2016). Conoce tus derechos. Función Judicial. https://www.funcionjudicial.gob.ec/pdf/conoce-tus-derechos.pdf (Recuperado. El 4 de diciembre 2021).
12. Loredo, J.A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Eprints. Pág. (46). http://eprints.uanl.mx/3536/1/Delitos_ informaticos.pdf (Recuperado. El 28 de noviembre 2021).

13. Mendoza, E. 2012. Acoso cibernético o cyberbullying: Acoso con la tecnología electrónica. Pediatría de México Vol. 14. Pág. (133) https://www.medigraphic.com/pdfs/conapeme/pm-2012/pm123g.pdf. (Recuperado. El 15 de diciembre 2021).
14. Muñoz Conde. F. (1984). Teoria General del Delito. Temis. Págs. (16). https://www.sijufor.org/uploads/1/2/0/5/120589378/06_mu%C3%91oz_conde_t _del_delito.pdf (Recuperado. El 15 de diciembre 2021).
15. Navarrete J. (2020). Tipos de Redes sociales. Imotione Lab. párr. 1. https://www.Inboundemotion.com/blog/author/jordi-navarrete-fern%C3%A1ndez (Recuperado. El 18 de diciembre 2021).
16. Novoa I. Venegas L. (2020). Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. Universidad de Chile.
17. Hernández Asunción.- "Guía de Redes Sociales"; (Disponible en URL: http://www.lalfasjove.com/data/documentos/Guia_sobre_Redes_Sociales.pdf) (3 de diciembre de 2013) 14.
18. Hernández Díaz, Leyre (2009).- "El delito informático", Editorial Eguzkilore; San Sebastian-España;http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_23_homenaje_ab/es_eguzki23/adjuntos/18-Hernandez.indd.pdf (12 de marzo de 2014) 15.
19. http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2009/05/27/derecho-informatico (15 de octubre de 2013) 16.
20. http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/delitos-informaticos

© 2023 por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) (https://creativecommons.org/licenses/by-nc-sa/4.0/).