EL IMPACTO DE LA UTILIZACION DE MEDIOS INFORMATICOS EN EL TIPO PENAL DE ESTAFA Y LA RESPUESTA DEL SISTEMA PENAL EN SU INVESTIGACION Y JUZGAMIENTO EN COLOMBIA

José Fernando Salazar Osorio

Lisbeth Dayana Rendón Ramírez

Universidad de Manizales

Facultad de ciencias jurídicas y derecho

Manizales 2024

Dedicatorias

Dedicatoria Lisbeth Dayana Rendón Ramírez.

Quiero agradecer primero a Dios por darme la paciencia y sabiduría para enfrentar estos años de aprendizaje y la fuerza para culminar esta etapa. A mis padres, Luis Carlos Rendón y Paula Ramírez, por su guía, motivación y acompañamiento frente a todas las dificultades, y a mi hermana Mariana, por ser un impulso constante; desde la distancia sé lo orgullosos que están. A mi tío y padrino, Jorge Enrique Ramírez, por confiar en mis capacidades y ser un apoyo tanto emocional como económico, pues sin él no habría logrado tanto. A mi compañero de tesis, José Fernando, por compartir la pasión por nuestra profesión y trabajar incansablemente para lograr este maravilloso resultado. Agradezco también a mis abuelos y a Sebastián, mi compañero de vida, por ser un sostén fundamental, aportando palabras de aliento, apoyo y motivación constante. Especial mención al Dr. Jorge Eduardo Missas, nuestro director de tesis, y a la Universidad de Manizales, por los aprendizajes y el apoyo durante más de cinco años, que contribuyeron a mi formación profesional, ética y crecimiento personal. Finalmente, gracias al destino por ponerme en este camino y a todos los que, aunque no mencionados, fueron parte de este logro; este triunfo es por y para todos.

Dedicatoria José Fernando Salazar Osorio.

Este trabajo es el resultado de años de esfuerzo, dedicación y sacrificio, así como del amor, compañía y apoyo incondicional de quienes han estado conmigo en cada paso de este camino. A mis padres, Nelson y Liliana, no existen palabras suficientes para agradecerles por su amor infinito, su fe en mí y su constante aliento; su apoyo y enseñanzas sobre el esfuerzo y la perseverancia han sido mi mayor inspiración. A mi hermano, Juan Felipe, gracias por ser un compañero incondicional, por sus palabras de ánimo y su disposición para escucharme, su compañía fue esencial en este proceso. A mis amigos, gracias por su alegría y por estar presentes en los momentos difíciles, haciendo este camino más llevadero y celebrando cada logro conmigo. A mi compañera de tesis, Dayana, gracias por compartir conmigo no solo largas jornadas de estudio, sino también la pasión por el derecho, su compromiso y complicidad han sido fundamentales en este proyecto. A la Universidad de Manizales y a la Facultad de Derecho, gracias por brindarme el espacio para crecer como persona y profesional, ya que este logro no solo es personal, sino también fruto de la formación integral recibida. A todos ustedes, de corazón, gracias por ser parte de este viaje; este triunfo también es suyo.

Contenido

Resumen:

El ciberdelito en Colombia ha cobrado relevancia con la expansión del internet, generando modalidades delictivas como el phishing, que compromete la seguridad de la información personal y económica a través de suplantación de identidad y manipulación psicológica. A pesar de avances legislativos como la Ley 2011 de 2019, que fortalece la recolección de pruebas digitales y aumenta las sanciones, persisten vacíos en la tipificación del phishing y otros delitos cibernéticos, dificultando su persecución. La sofisticación tecnológica, como el uso de inteligencia artificial, redes anónimas y blockchain, presenta constantes retos para las autoridades, que además enfrentan dificultades para identificar y capturar a los responsables. El Convenio de Budapest, ratificado en 2018, establece directrices internacionales para combatir el ciberdelito y promover la cooperación transnacional. No obstante, la legislación actual en Colombia sigue siendo insuficiente para abordar de manera efectiva estas prácticas, lo que resalta la necesidad de actualizar el marco normativo y reforzar la educación digital para prevenir delitos informáticos y mejorar la seguridad cibernética en el país.

Palabras Clave: Medios informáticos, ciberdelito, estafa, sistema penal

Abstract

Cybercrime in Colombia has gained relevance with the expansion of the internet, leading to criminal activities such as phishing, which compromise the security of personal and financial information through identity theft and psychological manipulation. Despite legislative advances like Law 2011 of 2019, which strengthens the collection of digital evidence and increases penalties, there are still gaps in the classification of phishing and other cybercrimes, making their prosecution difficult. Technological sophistication, including the use of artificial intelligence, anonymous networks, and blockchain, poses constant challenges for authorities, who also face difficulties in identifying and apprehending perpetrators. The Budapest Convention, ratified in 2018, establishes international guidelines to combat cybercrime and promote transnational cooperation. Nonetheless, the current legislation in Colombia remains insufficient to effectively address these practices, highlighting the need to update the legal framework and strengthen digital education to prevent cybercrimes and improve cybersecurity in the country.

Keywords: Computer media, cybercrime, fraud, criminal justice system

1. Introducción

El auge de la era digital ha transformado radicalmente la manera en que las personas interactúan, trabaja y realizan transacciones comerciales. Sin embargo, este avance también ha dado lugar a una serie de desafíos en el ámbito de la ciberseguridad, entre los cuales se destaca el phishing, una técnica de ingeniería social utilizada para obtener información sensible de manera fraudulenta, se ha convertido en una de las amenazas más prevalentes y peligrosas en el mundo digital. En Colombia, el crecimiento exponencial del acceso a internet y el uso de dispositivos electrónicos ha expuesto a una parte significativa de la población a los riesgos asociados con esta práctica delictiva.

Esta tesis tiene como objetivo principal analizar el fenómeno del phishing en Colombia, evaluando su evolución, impacto y las estrategias implementadas por las autoridades judiciales para investigar los delitos de estafa por medio del phishing. a través de un enfoque jurídico, se explorarán los factores que contribuyen a la vulnerabilidad de los usuarios. Además, se investigan las políticas y marcos regulatorios establecidos por el gobierno colombiano y las iniciativas privadas dirigidas a fortalecer la ciberseguridad y proteger a los ciudadanos de estas amenazas.

La relevancia de este estudio radica en la necesidad de comprender a fondo el panorama del phishing en Colombia y validar las soluciones efectivas y adaptadas al contexto nacional que se hayan desarrollado. Al identificar las técnicas actuales y los desafíos específicos del país, se estudiarán las medidas preventivas y correctivas que se hayan generado que no solo beneficien a los individuos, sino que también fortalezcan la seguridad de las organizaciones y del entorno digital en su conjunto. En última instancia, esta investigación busca contribuir al desarrollo de una cultura de ciberseguridad más robusta en Colombia, promoviendo una utilización más segura y consciente de las tecnologías de la información.

2. Planteamiento Del Problema

El ciberdelito es una actividad delictiva que emplea medios electrónicos para acceder a la información de usuarios de plataformas digitales, con fines como la extracción de datos valiosos o el impacto negativo en la economía de los afectados. Este delito, comúnmente conocido como "hackeo", no discrimina por edad; tanto niños con videojuegos como adultos en plataformas de

suscripción pueden convertirse en víctimas. Las modalidades de estafa han proliferado debido al avance tecnológico, facilitando el acceso a nuevas víctimas y métodos de engaño. El ciberdelito de estafa abarca desde fraudes financieros hasta suplantación de identidad y engaños sentimentales. En Colombia, el auge de los dispositivos digitales y la conectividad ha incrementado tanto el alcance como la sofisticación de estas actividades. La falta de conciencia y educación digital ha hecho especialmente vulnerables a ciertas poblaciones, como los adultos mayores, que pueden no poseer los conocimientos necesarios para identificar y evitar estafas en línea, situación que se agrava por la escasa regulación y la aplicación ineficaz de la ley en el ámbito digital.

Una de las investigaciones más destacadas sobre este tema en Colombia es el estudio de Esteban Torres, titulado "Tendencias actuales en la estafa cibernética en Colombia: Un estudio de caso de phishing y fraude en redes sociales". Este trabajo analiza los métodos utilizados por los ciberdelincuentes y su impacto en las víctimas mediante entrevistas, informes de seguridad de empresas tecnológicas y casos legales documentados. Además, la investigación "Impacto de las estafas en línea en las pequeñas y medianas empresas en Colombia" Ruiz (2022), revela la vulnerabilidad de las PYMEs frente a los delitos cibernéticos debido a la falta de capacitación y personal especializado en ciberseguridad. Las estafas mediante phishing, correos electrónicos fraudulentos y otras tácticas de ingeniería social son comunes y tienen graves repercusiones financieras. La obra "Aspectos Jurídicos del Ciberdelito en Colombia: Enfoque en Estafas y Fraudes", de Laura Gómez, ofrece recomendaciones para mejorar la legislación actual, incluyendo la necesidad de reformas legales y el fortalecimiento de la capacitación de jueces, fiscales y fuerzas del orden en ciberseguridad.

La economía de Colombia también ha sido impactada por el ciberdelito, con consecuencias socioeconómicas evidentes. Según Bortnik (2011), en su libro "Ciberdelincuencia: Impacto y Estrategias de Mitigación en América Latina", la expansión de la tecnología en la región ha aumentado tanto la frecuencia como la sofisticación de los delitos cibernéticos. Entre los costos más notables se incluyen los gastos directos asociados a la recuperación de datos y reparaciones de sistemas, así como los costos indirectos que afectan la productividad y la reputación empresarial. El sector financiero y el comercio electrónico son los más perjudicados, ya que los ataques pueden tener efectos devastadores en la estabilidad y las operaciones cotidianas. Datos recientes de Caracol Radio (2021) revelan un aumento del 17% en los delitos cibernéticos

reportados en Colombia, con más de 33,000 casos solo en ese año. La pandemia de COVID-19 y la acelerada digitalización que esta propició expusieron vulnerabilidades que han sido aprovechadas por los ciberdelincuentes para perpetrar fraudes relacionados con tratamientos médicos falsos y ayudas gubernamentales fraudulentas.

A lo largo de las décadas, la evolución del ciberdelito en Colombia ha seguido el desarrollo de la conectividad digital. Desde los años 90, con el advenimiento de Internet y los primeros fraudes financieros a través de correos electrónicos, hasta los años 2000, cuando el acceso masivo a Internet facilitó el phishing y la suplantación de identidad en banca en línea. En los años 2010, con el auge de las redes sociales, surgieron nuevas formas de estafas de ingeniería social. Entre 2015 y 2018, el aumento de ransomware y fraudes relacionados con criptomonedas se hizo evidente, mientras que en 2019 y 2020, se intensificaron los esfuerzos para combatir estos delitos mediante la creación de unidades especializadas. Sin embargo, el avance del ciberdelito no se ha detenido. Con la pandemia, el trabajo remoto y la educación en línea se convirtieron en factores que facilitaron nuevas estafas, lo que demuestra que el ciberdelito es un reto dinámico que requiere estrategias adaptativas para su prevención y control.

Para afrontar el ciberdelito en Colombia, se necesita un enfoque integral que combine prevención, aplicación de la ley y concienciación pública. Es esencial implementar programas de educación digital para que tanto jóvenes como adultos aprendan a reconocer las amenazas en línea y naveguen con seguridad. La colaboración entre el gobierno, el sector privado y la sociedad civil es crucial para desarrollar y aplicar políticas efectivas que protejan a los ciudadanos. Las campañas de información pueden ayudar a que los ciudadanos comprendan los riesgos y denuncien actividades sospechosas, promoviendo una cultura de precaución en línea. La legislación debe actualizarse constantemente para abordar las nuevas amenazas, y es imprescindible invertir en la capacitación de jueces, fiscales y fuerzas del orden en temas relacionados con la ciberseguridad, así como en la investigación y el desarrollo de tecnologías que permitan una mejor protección.

El ciberdelito de estafa plantea desafíos específicos en Colombia, como la necesidad de aumentar la concienciación pública sobre los riesgos digitales, mejorar la inclusión digital y desarrollar las capacidades de las instituciones para responder eficazmente a estos delitos. La brecha digital significa que algunos sectores son más vulnerables y carecen de los recursos para defenderse. Por ello, es fundamental promover la formación en ciberseguridad y la investigación continua para adaptarse a las nuevas tácticas de los delincuentes. Además, es esencial examinar la

aplicabilidad de la legislación y enfocar los esfuerzos en reducir las brechas en la protección legal para combatir el ciberdelito de manera efectiva, reconociendo que su impacto va más allá de la violencia física, afectando significativamente tanto la integridad económica como la información personal de las víctimas.

3. Pregunta de investigación:

¿Cuáles son los impactos de la utilización de medios informáticos en el tipo penal de estafa y la respuesta del sistema penal en su investigación y juzgamiento en Colombia?

4. Hipótesis

La percepción de impunidad y la ausencia de consecuencias severas para los cibercriminales en Colombia fomentan la comisión de estafas en línea. Esta afirmación se sustenta en la teoría de la disuasión, que sostiene que la probabilidad de ser castigado influye en la decisión de delinquir. La proliferación de dispositivos conectados a Internet y la digitalización de los servicios financieros en el país han generado un aumento en las oportunidades para que los delincuentes lleven a cabo estas estafas. Esta situación sugiere que la facilidad de acceso y la falta de medidas de seguridad adecuadas incrementan la incidencia de delitos cibernéticos. Los estafadores en línea están adaptando sus tácticas en respuesta a nuevas medidas de seguridad implementadas por empresas y el gobierno, lo que crea una competencia constante entre los ciberdelincuentes y las entidades dedicadas a la seguridad. Además, la falta de educación digital y la escasa conciencia sobre la seguridad cibernética entre los usuarios colombianos los hacen más vulnerables a ser víctimas de estafas en línea. Esta hipótesis plantea que los ciberdelincuentes se aprovechan de la inexperiencia y la falta de conocimientos técnicos de los usuarios, lo que facilita la realización de sus delitos.

5. Objetivos

5.1 Objetivo general:

Analizar las modalidades del delito de estafa a través de la utilización de medios informáticos y los retos para la investigación y juzgamiento por parte de las autoridades judiciales.

5.2 Objetivos específicos:

- Determinar cuáles son los criterios jurídico penales para la configuración del delito de estafa en Colombia.
- Identificar las modalidades del delito de estafa con la utilización de medios informáticoscomo el phishing.
- Describir las estrategias implementadas por las autoridades judiciales para investigar y juzgar el delito de estafa a través de la modalidad del phishing.

6. Justificación

La presente investigación se enfocará en el fenómeno del phishing en Colombia, una modalidad de cibercrimen que ha adquirido una relevancia creciente en los últimos años debido al aumento significativo del uso de las tecnologías de la información y la comunicación en el país, los cuales siguen y seguirán evolucionando, lo que conlleva a que se presenten drásticos cambios en lasociedad y en el uso correcto o incorrecto que las personas en general le den y esta problemática hallevado a que los gobiernos desde sus poderes legislativo, ejecutivo y judicial, interpongan leyes y grupos para el seguimiento y la judicialización de quienes las usan con fines delictivos.

El phishing que consiste en el intento fraudulento de obtener información sensible como contraseñas, datos de tarjetas de crédito y otra información personal mediante la suplantación de una entidad confiable, representa una amenaza crítica para la seguridad digital de individuos y organizaciones. Hablando un poco de historia, el primer ataque de Phishing se detectó en el año 1990 por una empresa estadounidense donde el estafador enviaba un correo electrónico solicitando información sobre la facturación de la compañía, entre la que se encontraban los números de las tarjetas de crédito empleadas para pagar por el servicio, proceso que fue evolucionando a través de los años y que se presenta en la actualidad con la frecuencia ya mencionada.

Es de gran importancia analizar el delito del phishing en Colombia, resaltando que en la actualidad la mayoría de ciberdelitos se presentan por medio de esta modalidad y de la misma manera validar como se está actuando o qué medidas se están ejecutando para controlar y buscar erradicar de manera definitiva este tipo de actos. En Colombia la regulación y las medidas para

combatir el phishing se han centrado en la legislación, la cooperación interinstitucional y las campañas de concientización pública, a través de la ley 1273 de 2009 por medio de la cual se crearon nuevos tipos penales y modificó el código penal colombiano para incluir delitos relacionados con el uso indebido de la tecnología de la información y las comunicaciones, también a través de diversas maneras se han incluido disposiciones específicas para combatir el fraude informático y el acceso abusivo a sistemas informáticos, proporcionando herramientas legales para procesar y condenar a los perpetradores el phishing. Es de resaltar que las medidas mencionadas las cuales fueron aplicadas

en Colombia han surtido efectos y se refleja en varios casos donde se ha logrado desmantelar redes de phishing y llevar a los responsables ante la justicia y podemos decir que en la actualidad Colombia ha adoptado un enfoque multifacético para regular y combatir el phishing y estas acciones han fortalecido la capacidad del país para proteger a sus ciudadanos y sancionar a los responsables de estos delitos, sin dejar a un lado de falta mucho sobre la marcha para en algún momento decir que el modelo de estafa está radicado y las personas se encuentran tranquilas de en algún momento ser víctimas directas del delito que aquí trabajaremos.

Todo lo que ya se mencionó lleva al estado colombiano y a la población del mundo en general a mirar de una manera los delitos que se presentan a través de las tecnologías de la información, teniendo en cuenta que en la actualidad la tecnología cada día está creciendo y avanzando un poco más, para los estafadores se está convirtiendo mucho más fácil desarrollar estas prácticas delictivas, por esta razón, buscar un método efectivo y que genere cambios reales es un reto para los entes gubernamentales, la inteligencia artificial, misma que para las presentes calendas está en un auge superior debe tener de alguna y otra manera un control efectivo y sistemático el cual en todo momento le proporcione a sus consumidores una seguridad clara y efectiva ante cualquier intento de estada, de delito como el Phishing o cualquiera relacionado.

A través del desarrollo del presente trabajo nos detendremos en la práctica del phishing desde las cárceles en Colombia que claramente es un fenómeno muy preocupante donde los internos utilizan teléfonos móviles y acceso a internet, los cuales claramente obtienen de manera ilícita, para llevar a cabo este tipo de estafas. Estas actividades delictivas pueden incluir tanto phishing como otros tipos de fraudes cibernéticos. Los estafadores en las cárceles utilizan técnicas de ingeniería social para obtener información personal y financiera de las víctimas. Esto puede incluir llamadas telefónicas fraudulentas, mensajes de texto y correos electrónicos, una de las técnicas que utilizan

es hacerse pasar por entidades bancarias instituciones gubernamentales o empresas para engañar a las víctimas y obtener sus datos confidenciales, en algunos casos los estafadores obtienen también información comprometedora y luego extorsionan a las personas para obtener dinero a cambio de no divulgar dicha información. Claramente los centros penitenciarios en el país han adoptado ciertas medidas (no del todo efectivas) para contrarrestar este delito, tales como, la implementación de bloqueadores de señal para impedir el uso de teléfonos móviles no autorizados, operativos periódicos para confiscar dispositivos electrónicos ilegales, supervisión y control de las comunicaciones de los reclusos para detectar y prevenir actividades ilícitas, coordinación entre las autoridades penitenciarias, la policía y las entidades financieras para rastrear y desmantelar redes de fraude operadas desde las cárceles y el endurecimiento de las sanciones para los reclusos y el personal implicado, teniendo en cuenta que en algunas ocasiones hasta los mismos custodios hacen parte de la práctica ilícita.

Es muy importante dentro de la presente investigación analizar las prácticas seguras que la población en general debe tener en cuenta para no ser en algún momento víctima del presente delito, las personas deben ser conscientes de las técnicas de phishing y mantenerse escépticas ante las solicitudes inesperadas de información personal y tomar acciones preventivas como no compartir información personal por teléfono o correo electrónico, verificar la identidad del remitente o interlocutor a través de canales oficiales, utilizar medidas de seguridad adicionales como la autenticación en dos pasos y reportar cualquier intento de estafa a las autoridades correspondientes, de esta manera podemos identificar que combatir el phishing en general es una tarea compleja, pero que se debe desarrollar de manera conjunta, y que con la combinación de medidas tecnologías, operativas y educativas se puede mitigar de alguna manera esta problemática y proteger a la población de estas actividades delictivas.

Hablando de la inteligencia artificial podemos validar cómo impacta de manera significativa su uso para cometer ciberdelitos como por ejemplo en la creación de correos electrónicos utilizados para el phishing y cómo se desarrollan de manera personalizada, la IA también le permite a los estafadores analizar perfiles en redes sociales y otras fuentes de datos para crear mensajes altamente personalizados que sean más efectivos para engañar a las víctimas, también puede optimizar ataques de fuerza bruta, haciendo que sean más rápidos y eficientes al predecir y generar posibles combinaciones de contraseñas. Además, es posible por medio de la IA crear videos, audios e imágenes falsos que imitan a personas reales, facilitando fraudes y estafas que dependen de la

suplantación de identidad.

En conclusión, podemos determinar que desarrollamos la presente investigación, primero conel fin de validar las acciones que en la actualidad se toman por parte de los entes gubernamentales para mitigar el desarrollo de esta práctica ilícita, también de qué manera se desarrolla y cómo las personas pueden caer en una estafa como esta, cómo puede ser tan sencillo para los actores desarrollar y llevar hasta un fin exitoso la estafa, como las personas deben estar conscientes y de qué manera deben proteger absolutamente todos sus datos personales, denunciar por ejemplo debe ser el inicio de la cadena de investigación para que todas las autoridades del país desarrollen sus estrategias de protección y para ello se debe tener en cuenta, como ya lo mencionamos, la evolución que a la fecha las tecnologías de la información han tenido, no es lo mismo investigar un delito informático de hace 20 años y confrontarlo con uno que se presenta en las calendas actuales, teniendo en cuenta por ejemplo a inteligencia artificial o las diversas formas que los estafadores tienen fácilmente a sus manos para desarrollar de manera efectiva su delito.

Este estudio pone de manifiesto la necesidad de un enfoque multifacético que combine la educación del usuario, la implementación de tecnologías avanzadas de detección y respuesta, y la cooperación interinstitucional para combatir el Phishing de manera integral. Al explorar las diversas formas en que se manifiesta el phishing y las medidas actuales para enfrentarlo, esta tesis justifica la urgencia de fortalecer nuestras defensas cibernéticas y las herramientas que gubernamentalmente se nos proporciona para cuidarnos ante cualquier ataque o fraude que personas inescrupulosas intentan efectuar en nuestra contra con el único fin de poner en riesgo nuestra información o nuestro dinero.

La justificación de esta tesis radica en su contribución a la actual problemática que Colombia atraviesa respecto al phishing y claramente proporcionará una base sólida para futuras investigaciones y desarrollos en el campo de la ciberseguridad y de qué manera las personas pueden blindarse ante cualquier ataque cibernético que intenten en contra de ellos. Al abordar el phishing desde múltiples perspectivas, se espera que este trabajo sirva como un recurso valioso para académicos profesionales de la seguridad informática y legisladores ayudando de alguna u otra manera a construir un entorno digital más seguro, resiliente y claramente que funcione como una guía para que las personas sean más precavidas al momento se proporcionar información por los diversos medios tecnológicos que a la fecha existen.

7. Marco de Referencias

7.1 Marco Teórico

Con el avance de la tecnología se debe tener claridad que por desgracia la delincuencia ha tomado provecho de esto para realizar estafa por medio de aparatos electrónicos y/o aplicativos que se usan a diario, se aprovechan de las necesidades diarias que tiene cada persona hasta la inocentada de un niño en su videojuego. Según datos de la fiscalía general de la Nación de Colombia, el ciber delito de estafa ha experimentado un aumento significativo en los últimos años. De acuerdo con el fiscal general Francisco Barbosa, "El ciberdelito de estafa se ha convertido en una de las modalidades delictivas más frecuentes en Colombia, afectando a miles de ciudadanos cada año" (El Tiempo, 2023).

De acuerdo a lo anterior, el delito informático entonces es aquel que se vale de medios informáticos para vulnerar algún bien jurídico tutelado, pudiendo hacerlo mediante: Acciones que inciden sobre el software y hardware de un dispositivo. Acciones en que es usado como instrumento para perpetrar un delito. Acciones en que se utiliza hardware o software sin autorización debida.

En medio de la investigación de este delito podemos evidenciar que, aunque hay normatividad para combatirlo no ha sido muy eficiente la norma en cuanto a la captura de los delincuentes pues la tecnología suele ser tan avanzada que algunos no dejan rastro de como se hizo o quien realizó dicho delito, es por esto según un informe de la Superintendencia de Sociedades, "La falta de regulación efectiva en el ámbito digital y la creciente sofisticación de los perpetradores son factores clave que facilitan la comisión de delitos cibernéticos en el país" (Superintendencia de Sociedades, 2022).

Varios factores contribuyen al riesgo de ciber delito de estafa en Colombia. Entre ellos se incluyen la falta de conciencia sobre seguridad cibernética entre la población, la falta de regulación efectiva en el ámbito digital, la disponibilidad de herramientas y servicios en línea que facilitan la comisión de delitos, y la presencia de grupos delictivos organizados que se dedican a actividades ilícitas en la web oscura. Además, la rápida adopción de tecnologías emergentes, como las criptomonedas y la inteligencia artificial, también introduce nuevos desafíos en la lucha contra el ciberdelito de estafa.

Las consecuencias del ciber delito de estafa en Colombia son significativas tanto a nivel

individual como institucional. Según un estudio realizado por la Universidad Nacional de Colombia, "Las víctimas de ciber delito de estafa experimentan pérdidas financieras, estrés emocional y daño a su reputación, lo que puede tener un impacto duradero en sus vidas" (Universidad Nacional de Colombia, 2021).

Julio Téllez Valdez en su investigación divide los delitos informáticos en los siguientes grandes grupos a modo de clasificación: Falsificaciones Informáticas: Manipulando información arrojada por una operación de consulta en una base de datos. Manipulación de los datos de salida: Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo. Fraude efectuado por manipulación informática: Accediendo a los programas establecidos en un sistema de información y manipulándolos para obtener una ganancia monetaria Delitos financieros en línea: Incluye actividades como el robo de información financiera, la manipulación de transacciones en línea o el fraude bancario. Fraude en línea: Engaños o estafas llevadas a cabo a través de Internet, como el phishing, donde los delincuentes se hacen pasar por entidades legítimas para obtener información confidencial.

Estos son solo algunos ejemplos y la lista no es exhaustiva. Los delitos informáticos pueden variar ampliamente en su naturaleza y complejidad, y su definición y clasificación pueden cambiar con el tiempo debido al desarrollo tecnológico y las nuevas formas de delincuencia en línea. En el mundo criminológico existen dos teorías y/o factores que podemos ver a continuación: Teoría de la Oportunidad: Sostiene que el ciberdelito ocurre cuando los delincuentes perciben una alta oportunidad y un bajo riesgo de ser atrapados. Según esta teoría, la disponibilidad de oportunidades delictivas es crucial. El acceso a la tecnología y la falta de controles efectivos pueden facilitar la comisión de cibercrímenes. En Colombia, la rápida adopción de la tecnología puede ofrecer oportunidades para cometer estafas en línea. (Cloward – Ohlin).

Teoría de las Rutinas Cotidianas: Sugiere que el ciberdelito ocurre cuando hay una convergencia de un delincuente motivado, una víctima adecuada y la ausencia de un guardián capaz. En el caso del cibercrimen, la creciente actividad en línea y la falta de medidas de seguridad adecuadas hacen que las estafas sean más comunes. (Cohen y Felson)

En Colombia, varios criminólogos y académicos han abordado el tema del ciberdelito, en particular la modalidad de estafa. A continuación, se presentan algunas citas y opiniones destacadas

de criminólogos colombianos sobre este fenómeno: Sánchez (2019) argumenta que el crecimiento del comercio electrónico y las transacciones en línea ha creado un ambiente propicio

para las estafas cibernéticas, donde los delincuentes explotan las vulnerabilidades tecnológicas y la confianza de los usuarios.

González observa que "la educación digital es clave para prevenir el ciberdelito. Muchos usuarios caen en estafas debido a la falta de conocimientos sobre cómo identificar y evitar fraudes en línea" (González, 2022). Bonilla Sebá, en su investigación sobre ciberdelitos en Colombia, destaca que "las estafas en línea representan uno de los tipos más comunes de cibercrimen, impulsadas por la rápida adopción de tecnologías y la falta de educación en seguridad digital entre los usuarios" (Bonilla Sebá, 2018).

Los criminólogos tratan de encajar a las personas delictivas en un grupo determinado, pero se les ha hecho difícil porque estas personas no tienen características comunes, por lo que es más preocupante para el entorno social pues cualquier persona puede llegar a cometer este tipo de delito teniendo conocimientos informáticos.

7.2 Marco Legal

La Ley 1298 de 2018 aprueba el convenio sobre la ciberdelincuencia y establece la definición y categorización de los delitos informáticos dentro del código penal. Esta ley busca adaptar la legislación colombiana a los desafíos que presenta la ciberdelincuencia en un mundo cada vez más digital, garantizando una respuesta legal adecuada a las nuevas formas de delito.

El Código Penal Colombiano, en su Artículo 269G, establece que la persona que, con un objeto ilícito y sin estar facultado, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses, además de una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (smlmv), siempre que esta conducta no constituya un delito sancionado con una pena más grave.

Por su parte, la Ley 1273 de 2019 modifica el código penal y crea un nuevo bien jurídico tutelado, denominado “De la protección de la información y de los datos.” Esta ley busca preservar integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones, garantizando una mayor protección frente a los delitos informáticos.

La Constitución Política de Colombia, en su Artículo 15, establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, siendo obligación del estado

respetarlos y hacerlos respetar. Este derecho es fundamental en el contexto digital, donde la privacidad puede verse comprometida por diversas actividades en línea.

El Convenio de Budapest es un acuerdo internacional que busca enfrentar los delitos informáticos y en internet. Este convenio establece una cooperación entre los países firmantes para mejorar la eficacia de las leyes y la capacidad de respuesta ante la ciberdelincuencia, promoviendo un marco legal adecuado para la colaboración internacional.

La Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales en Colombia. Esta ley es un paso crucial en la regulación del manejo de datos en el país, buscando garantizar la privacidad y la protección de la información personal de los ciudadanos.

Finalmente, la Policía Nacional de Colombia, a través de su unidad especializada en cibercrimen (CNP-CU), trabaja para prevenir, investigar y combatir las actividades delictivas en línea. Esta unidad desempeña un papel vital en la lucha contra la ciberdelincuencia, colaborando con diferentes entidades para fortalecer la seguridad cibernética en el país.

8. Diseño Metodológico

Tipo de investigación: La investigación tendrá una naturaleza cualitativa, lo que permite comprender en profundidad el tema en estudio, incluyendo motivaciones, percepciones, comportamientos y proyecciones. Esto facilitará una comprensión integral de los fenómenos que intervienen en el análisis. El método empleado será inductivo-deductivo, con un tratamiento de datos que incorpora un enfoque cuantitativo. El enfoque elegido será descriptivo-interpretativo, centrándose en los datos, pero con la intención de trascenderlos al sujeto social, lo que permitirá una mejor comprensión del tema en investigación.

Técnicas de recolección de información: Se utilizará la encuesta como técnica principal para recopilar información de la muestra de estudio, que consistirá en personas expertas, como policías con experiencia en el combate de este delito, con el fin de identificar las razones detrás de la ocurrencia de estafas en Colombia. Adicionalmente, se realizarán entrevistas a profundidad con expertos en ciberdelitos y ciberseguridad, así como con la policía departamental, para obtener información más detallada sobre las tácticas de estafa y prevención. El diseño del cuestionario para la entrevista incluirá preguntas claras y concisas, una variedad de tipos de preguntas (opción

múltiple, escala de Likert y abiertas), así como preguntas demográficas (edad, género, nivel educativo, etc.) para facilitar el análisis. También se llevará a cabo un análisis de contenido y comparación cruzada de estudios de caso. Finalmente, se preparará un informe que resuma los hallazgos, utilizando gráficos y tablas para ilustrar los resultados, describiendo las implicaciones de los datos y proporcionando las recomendaciones pertinentes.

Capítulo I

Determinación De Los Criterios Jurídico Penales Para La Configuración Del Delito De Estafa En Colombia.

En Colombia, es fundamental reconocer que el delito de estafa está tipificado en nuestro código penal. Cuando este delito ocurre de manera digital o mediante métodos electrónicos, se considera un ciberdelito. La estafa se clasifica como tal cuando el engaño o el fraude se realizan a través de plataformas digitales, redes sociales, correos electrónicos, páginas web falsas y comercio electrónico, entre otros. Investigaciones previas han identificado los elementos esenciales de la estafa, lo que permite determinar si se trata de un delito tipificado. Entre estos elementos destacan el engaño, donde el ciberdelincuente induce a la víctima a cometer un error mediante promesas falsas o suplantación de identidad. Los ciberdelincuentes suelen presentar una apariencia legítima, replicando información de manera convincente y utilizando imágenes casi idénticas a las de empresas e instituciones legítimas, lo que dificulta la identificación del fraude.

Otro aspecto relevante es la urgencia o presión que ejercen los ciberdelincuentes sobre sus víctimas, quienes reciben mensajes que incluyen amenazas de bloqueo y plazos cortos para actuar, sin cuestionar la veracidad del mensaje. Además, estos delincuentes suelen apelar a las emociones de las víctimas, utilizando el miedo, la compasión o incluso el amor para manipularlas y obtener lo que desean. El aprovechamiento del error implica inducir a la víctima a cometer equivocaciones, haciéndola creer que está actuando de manera correcta cuando, en realidad, está siendo manipulada. Un ejemplo común de esto en Colombia son los fraudes bancarios y las ofertas de empleo falsas. El detrimento o perjuicio económico se presenta cuando las víctimas, inducidas por el engaño, pierden dinero o bienes a través de transacciones fraudulentas, entregando información sensible o realizando acciones que resultan en pérdidas financieras.

El marco legal colombiano busca proteger a los ciudadanos y sus bienes de los delitos informáticos y electrónicos que se cometen diariamente. Las normas establecen mecanismos de sanción para los ciberdelincuentes, así como para la investigación y judicialización de estos delitos. El artículo 246 del código penal colombiano tipifica las conductas asociadas a este tipo de delitos, imponiendo penas de 2.6 a 12 años de prisión, además de multas que oscilan entre 66.6 y 1.500 salarios mínimos legales vigentes. Con la Ley 1273 de 2009, se modificó el código penal,

añadiendo un nuevo capítulo titulado "La protección de la información y de los datos", que tipifica varios delitos relacionados con los ciberdelitos, incluidos aquellos que afectan la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Antes de esta ley, Colombia carecía de legislación específica para combatir los delitos informáticos, lo que dejaba un vacío frente a crímenes como el hackeo, la suplantación de identidad digital y el fraude electrónico.

Entre los principales aspectos de la Ley 1273 de 2009 se encuentran el acceso abusivo a un sistema informático (Artículo 269A), que penaliza a quien acceda sin autorización a un sistema protegido, y que conlleva penas de 48 a 96 meses de prisión y multas. La obstaculización ilegítima de sistemas informáticos o redes de telecomunicación (Artículo 269B) castiga la interferencia en el funcionamiento de sistemas o redes, con sanciones similares. El uso de software malicioso (Artículo 269H) se penaliza al igual que el hurto por medios informáticos (Artículo 269I), que penaliza el apoderamiento de bienes ajenos mediante el uso de medios electrónicos. Asimismo, la suplantación de sitios web (Artículo 269F) castiga la creación de sitios falsos para captar datos personales, afectando principalmente a bancos y usuarios de servicios financieros. A pesar de que esta ley representa un avance legislativo, algunos expertos consideran que su implementación enfrenta barreras significativas, como la falta de recursos tecnológicos y capacitación en las fuerzas del orden y el sistema judicial.

La Ley 1581 de 2012, aunque no se refiere directamente al ciberdelito de estafa, es relevante porque establece el régimen general de protección de datos personales en Colombia. El mal manejo de los datos o la no aplicación de esta ley puede llevar al robo de identidad y al uso indebido de información personal. Esta ley garantiza el habeas data, el derecho de las personas a conocer, actualizar y rectificar la información que se ha recopilado sobre ellas. En casos de estafa o ciberdelito donde se utiliza información personal robada, las empresas y plataformas digitales tienen la responsabilidad de proteger adecuadamente los datos y notificar a los usuarios en caso de violaciones de seguridad. Los principios de seguridad y confidencialidad son fundamentales, pero muchas empresas no los aplican adecuadamente, lo que pone en riesgo la información sensible de los usuarios. Las entidades que manejan datos personales están obligadas a implementar medidas técnicas y administrativas para proteger esos datos contra riesgos como el acceso no autorizado, la pérdida o la destrucción.

A pesar de las obligaciones establecidas, muchas empresas no cumplen con los requisitos de la Ley 1581, lo que puede acarrear sanciones y multas por un mal manejo de los datos personales.

Estas sanciones son aplicables tanto a personas naturales como jurídicas. La falta de cumplimiento de estas normativas no solo expone a los usuarios a riesgos de estafas y ciberdelitos, sino que también debilita la confianza en el sistema legal y en las plataformas digitales. Por lo tanto, es esencial que tanto el sector público como el privado se comprometan a mejorar la protección de datos y a garantizar la seguridad de la información para prevenir la comisión de delitos informáticos y proteger a los ciudadanos de los peligros que representan los ciberdelitos en el entorno digital.

Sanciones por incumplimiento de la Ley 1581 de 2012

El incumplimiento de la ley en el ámbito del tratamiento de datos puede acarrear sanciones severas que afectan tanto a las empresas como a los individuos. La Superintendencia de Industria y Comercio (SIC) tiene la potestad de imponer multas que pueden alcanzar hasta 2.000 salarios mínimos legales mensuales vigentes (SMLMV), lo que representa una carga financiera significativa para quienes no cumplan con las normativas establecidas. Además, la SIC puede suspender las actividades de tratamiento de datos por un período de hasta seis meses, lo que podría interrumpir gravemente las operaciones comerciales y afectar la confianza de los usuarios. En casos de violaciones graves de los derechos de los titulares de los datos, la ley también permite la clausura definitiva de las operaciones relacionadas con el tratamiento de estos datos, e incluso puede ordenar la eliminación de las bases de datos implicadas. Estas sanciones severas reflejan la creciente preocupación por la protección de datos personales en el contexto digital actual.

Ante la necesidad urgente de fortalecer las capacidades del Estado para combatir el cibercrimen en Colombia, se promulgó la Ley 2011 de 2019. Aunque existía legislación previa, como la Ley 1273 de 2009, que regulaba y sancionaba los delitos informáticos, las instituciones responsables de investigar estos delitos carecían de herramientas adecuadas para realizar investigaciones efectivas y colaborar en el ámbito internacional. El auge del comercio electrónico y la creciente dependencia de plataformas digitales han hecho que las personas sean más vulnerables a diversos tipos de ciberataques y fraudes. Por ello, se hacía indispensable dotar a las autoridades de instrumentos jurídicos y técnicas adecuadas para enfrentar estas amenazas de manera efectiva. La Ley 2011 de 2019 no solo mejora la legislación existente, sino que también introduce medidas novedosas que buscan adaptarse a la evolución del cibercrimen.

Uno de los aspectos más significativos de la Ley 2011 de 2019 es la ampliación de las facultades de las autoridades para investigar delitos informáticos. Esta legislación otorga a las autoridades judiciales y policiales capacidades especiales para intervenir y obtener pruebas en el

contexto de delitos que utilizan las tecnologías de la información y las comunicaciones (TIC). Esto incluye la interceptación de comunicaciones electrónicas, que solo se permite bajo autorización judicial y en el marco de investigaciones sobre delitos graves. Este tipo de intervención es crucial, ya que muchos delitos cibernéticos son planificados y ejecutados mediante plataformas digitales. Además, la ley permite el acceso a datos cifrados, lo cual es fundamental para desentrañar la complejidad de los delitos informáticos, ya que muchos delincuentes emplean técnicas criptográficas para ocultar sus actividades. La colaboración internacional es otro aspecto esencial contemplado en la Ley 2011 de 2019. Reconociendo que muchos delitos informáticos tienen un carácter transnacional, la ley busca establecer un marco de cooperación más eficaz entre las autoridades colombianas y organismos internacionales. Esto incluye medidas para facilitar la colaboración con entidades como Interpol y otros cuerpos de ciberseguridad globales. Tal cooperación es vital para el intercambio rápido y fluido de información durante las investigaciones y los juicios, especialmente cuando se trata de ciberdelincuentes que operan desde diferentes jurisdicciones. La firma de tratados como la Convención de Budapest sobre Ciberdelincuencia también es un paso importante hacia la consolidación de un marco legal que facilite la extradición y el proceso judicial en casos transnacionales.

La creación de unidades especializadas en delitos informáticos, como el Centro Cibernético Policial (CCP), es otra de las innovaciones clave introducidas por la Ley 2011 de 2019. Estas unidades están compuestas por expertos en ciberseguridad, análisis forense digital y tecnologías de la información, lo que les permite enfrentar de manera efectiva los delitos cibernéticos. Por ejemplo, el CAI Virtual de la Policía Nacional proporciona a los ciudadanos un canal directo para reportar delitos como el fraude informático y el robo de identidad. Este enfoque coordinado es esencial para detectar y prevenir amenazas digitales, así como para perseguir a los delincuentes en el ámbito cibernético. La existencia de estas unidades también contribuye a la formación continua de los profesionales encargados de la seguridad digital, lo que es fundamental en un campo que evoluciona rápidamente.

La Ley 2011 de 2019 también establece mejoras significativas en la recolección y manejo de pruebas digitales. La capacidad de las autoridades para recolectar, examinar y presentar evidencias digitales en procesos judiciales ha sido fortalecida, introduciendo métodos que aseguran que la obtención de dicha evidencia se realice respetando principios de legalidad, transparencia y debido proceso. Esto es esencial para que las pruebas obtenidas durante las investigaciones sean

consideradas válidas y utilizables en los tribunales. La legislación actual incluye disposiciones específicas que aseguran la preservación y presentación adecuada de registros digitales, como comunicaciones y transacciones electrónicas, lo cual es crucial para investigar delitos cibernéticos.

Por último, las obligaciones impuestas a los Proveedores de Servicios de Internet (ISP) por la Ley 2011 de 2019 son fundamentales para combatir los delitos cibernéticos. Se exige a los ISP que colaboren activamente con las fuerzas del orden para prevenir y detectar actividades criminales en línea, lo que incluye la retención de ciertos datos de tráfico por un periodo específico. Esta medida es esencial para facilitar las investigaciones de delitos cibernéticos y garantizar que la información esté disponible cuando se solicite a través de una orden judicial. La ley también asegura que el acceso a los datos por parte de las autoridades se realice con las debidas autorizaciones legales, manteniendo así un equilibrio entre la lucha contra el cibercrimen y la protección de los derechos fundamentales de los individuos.

La reciente legislación, la Ley 2011 de 2019, intensifica considerablemente las sanciones aplicables a los delincuentes informáticos, sobre todo cuando los ataques afectan a infraestructuras esenciales como los sistemas financieros o las redes de telecomunicaciones. Esta ley establece sanciones claras para aquellos que se dedican a actividades delictivas en el ciberespacio, buscando no solo castigar a los infractores, sino también prevenir futuros delitos. Entre las sanciones más destacadas se encuentra la imposición de penas de prisión de hasta 10 años para quienes cometan delitos informáticos graves. Estas infracciones incluyen el acceso no autorizado a sistemas informáticos, así como la modificación de datos personales con fines lucrativos. Además, la ley contempla la posibilidad de imponer multas sustanciales, diseñadas para desalentar la utilización de medios electrónicos en la perpetración de actos delictivos. Otro aspecto importante de esta legislación es la prohibición de ocupar cargos públicos o ejercer profesiones en ámbitos que involucren el manejo de información sensible, lo que se aplica a funcionarios o individuos que, aprovechando su acceso privilegiado, cometan este tipo de delitos. Con estas medidas, se busca proteger la integridad de los sistemas críticos que son esenciales para el funcionamiento de la sociedad y garantizar la seguridad de la información de todos los ciudadanos.

Las autoridades enfrentan un desafío constante debido al rápido avance de las tecnologías y el surgimiento de nuevas modalidades de cibercrimen. La creciente sofisticación de los ataques informáticos y el uso de herramientas avanzadas como la inteligencia artificial, redes anónimas (como TOR) y tecnologías de blockchain dificultan la identificación y captura de los delincuentes.

La inteligencia artificial se ha convertido en una herramienta poderosa para los ciberdelincuentes, permitiéndoles cometer delitos de manera más eficiente y difícil de detectar. Por ejemplo, la automatización de ataques a gran escala les permite operar de manera rápida y efectiva, ya que las herramientas impulsadas por IA tienen la capacidad de analizar en tiempo real grandes volúmenes de datos y redes para detectar vulnerabilidades. Una vez identificadas estas vulnerabilidades, los delincuentes pueden aprovecharlas a través de malware o ataques específicos, con muy poca participación humana. Este enfoque automatizado no solo hace que los ataques sean más rápidos, sino que también complica la tarea de las autoridades para prevenir y responder a estos delitos en evolución.

Los delincuentes también han comenzado a utilizar deepfakes, que son contenidos falsos generados por inteligencia artificial, como imágenes, videos y audios, para llevar a cabo fraudes de identidad o suplantación de personas. Estos avances tecnológicos permiten crear imágenes o videos altamente realistas que pueden ser utilizados para la creación de contenido falso con el fin de amenazar y difamar a personas o empresas en Colombia. En pocas palabras, la inteligencia artificial desempeña un doble papel en el campo de los ciberdelitos en el país. Aunque proporciona soluciones avanzadas para proteger a las empresas y ciudadanos, también se ha convertido en una potente herramienta en manos de los ciberdelincuentes, que utilizan la tecnología para llevar a cabo ataques más sofisticados, automatizados y eficientes. Este aumento en el uso de IA por parte de delincuentes representa un desafío significativo para las autoridades, quienes deben encontrar formas de responder adecuadamente desde el punto de vista tecnológico y legal. La rapidez con la que estas herramientas evolucionan exige que las leyes y regulaciones se mantengan al día con los avances tecnológicos para asegurar la protección de la ciudadanía.

Otra modalidad que ha cobrado relevancia en el ámbito del cibercrimen son las redes anónimas, como TOR (The Onion Router), que permiten a los criminales ocultar su identidad y actividades en línea. Estas redes, concebidas originalmente para aumentar la privacidad y salvaguardar la libertad de expresión en situaciones represivas, son lamentablemente utilizadas por personas malintencionadas para perpetrar delitos en el ámbito virtual. Su funcionamiento se basa en anonimizar la actividad en línea a través de una serie de servidores distribuidos, lo que dificulta enormemente rastrear la ubicación o identidad del usuario, dado que se oculta su dirección IP. A través de TOR, los ciberdelincuentes tienen acceso al darknet (mercado oscuro), donde pueden vender bases de datos robadas que contienen información confidencial sobre colombianos, como

números de tarjetas de crédito, cuentas bancarias y credenciales para acceder a sistemas. Algunos de ellos utilizan esta información para realizar fraudes financieros, mientras que otros la venden a terceras personas para su uso en otros tipos de delitos. La facilidad de acceso y la percepción de impunidad que ofrece el anonimato en estas redes hacen que sean una herramienta atractiva para quienes buscan el lucro a través de actividades ilegales en el ciberespacio.

Finalmente, la tecnología blockchain, a menudo asociada con criptomonedas, también se ha convertido en un terreno fértil para el cibercrimen. Los delincuentes pueden realizar transacciones de grandes cantidades de dinero sin dejar un rastro claro, lo que genera oportunidades para el lavado de dinero, estafas y financiamiento de actividades ilícitas. En Colombia, se han reportado numerosos incidentes de hackeo de plataformas de intercambio locales o billeteras personales, donde los delincuentes roban fondos y los distribuyen en múltiples billeteras para dificultar el rastreo. Este fenómeno ha llevado a que la blockchain sea vista como una herramienta tanto de innovación como de riesgo. La descentralización y el anonimato que ofrece la tecnología han permitido a los delincuentes operar con un mayor grado de impunidad, lo que ha puesto en jaque a las autoridades y exige una respuesta integral para proteger la economía digital del país. La creciente adopción de criptomonedas y la falta de regulación adecuada han intensificado la necesidad de que las instituciones colombianas fortalezcan sus capacidades para detectar y prevenir delitos relacionados con esta tecnología.

Colombia se enfrenta a una amenaza cibernética que se agrava cada día, y ha reconocido la importancia de la cooperación internacional para abordar esta problemática. Existen diversas leyes y acuerdos internacionales que han sido fundamentales para mejorar la capacidad del país en el combate del ciberdelito. Uno de estos acuerdos es el Convenio de Budapest, que fue el primer tratado internacional que aborda los delitos informáticos y establece normas para combatir el cibercrimen a nivel mundial. Colombia firmó este convenio en el año 2018, convirtiéndose en uno de los primeros países latinoamericanos en adoptar medidas globales para enfrentar los delitos informáticos. Mediante la ratificación de este acuerdo, el país se compromete formalmente a realizar cambios legislativos efectivos en su ordenamiento interno sobre la materia, de manera que se adecúe a las exigencias de las normas internacionales. Esto implica no solo la modificación de las leyes existentes, sino también la creación de nuevas disposiciones que refuercen la lucha contra el cibercrimen, asegurando así una respuesta más efectiva ante los desafíos que plantea el entorno digital.

El Convenio de Budapest también requiere que Colombia establezca procedimientos eficaces para la investigación de delitos cibernéticos, que abarcan desde el fraude en línea hasta el acceso no autorizado a sistemas. Este aspecto es crucial, ya que permite a las autoridades contar con herramientas y protocolos claros para abordar la creciente complejidad de los delitos informáticos. Asimismo, se busca facilitar la colaboración con otros estados para la persecución y el enjuiciamiento de delitos cibernéticos transfronterizos, lo que incluye la facilitación del intercambio de información y la asistencia recíproca. Este enfoque multilateral es esencial para enfrentar la naturaleza global del cibercrimen, ya que muchas de las actividades ilegales trascienden fronteras y requieren una respuesta coordinada de diversos países. El Convenio de Budapest abarca múltiples áreas de interés particular para Colombia en relación con la lucha contra el ciberdelito, lo que incluye la necesidad de establecer normas claras para poder perseguir el acceso ilegal a los sistemas informáticos, la interferencia en los datos y los sistemas, así como la interceptación de las comunicaciones en el país.

Se establecen normas en Colombia para combatir la difusión de contenidos ilegales, como el material de explotación sexual infantil, que constituye una de las prioridades del país, dada la gravedad de los problemas que han derivado de estos contenidos en el ciberespacio. La estafa cibernética ha emergido como un delito registrado en Colombia, especialmente con el auge de las compras en línea y las transacciones digitales. El Convenio de Budapest fija pautas específicas para perseguir el fraude cibernético y la falsificación informática, formas delictivas muy presentes en el país. Uno de los elementos más significativos del Convenio es la cooperación internacional, fundamental para Colombia, ya que muchos delitos informáticos provienen de delincuentes que operan desde el exterior, permitiendo que el país solicite asistencia en investigaciones transnacionales, lo cual es crucial para rastrear a ciberdelincuentes que operan desde redes internacionales y utilizan técnicas avanzadas de anonimato, como redes TOR. Además, el Convenio ofrece directrices claras para el manejo y la obtención de pruebas electrónicas, un aspecto clave en la lucha contra el ciberdelito, y Colombia ha trabajado para mejorar los procedimientos de recolección, preservación y análisis de pruebas digitales en investigaciones penales. A pesar de la alta impunidad histórica en delitos cibernéticos, leyes y convenios han ayudado a reducirla al mejorar la capacidad investigadora y el intercambio internacional de información. Finalmente, el seguimiento de las transacciones financieras ilegales, especialmente las relacionadas con criptomonedas, ha mejorado gracias a la cooperación mantenida con agencias internacionales y la

aplicación de marcos legales que permiten investigar estos delitos de manera más eficaz.

Capítulo II

Identificación De Las Modalidades Del Delito De Estafa Con La Utilización De Medios Informáticos Como El Phishing.

El phishing es una modalidad delictiva que se caracteriza por la obtención fraudulenta de información confidencial de los usuarios, como nombres de usuario, contraseñas y datos

financieros, mediante la suplantación de identidad. Este delito se ejecuta a través de la manipulación psicológica (ingeniería social), donde los delincuentes se presentan como entidades confiables a través de correos electrónicos, mensajes de texto, llamadas telefónicas, o sitios web falsos. La clasificación de phishing como un delito informático se basa en la utilización de medios digitales para perpetrar la estafa, afectando la seguridad de la información y el patrimonio económico de las víctimas.

En el contexto colombiano, el phishing ha cobrado relevancia como una forma sofisticada de estafa que se ha adaptado rápidamente a los avances tecnológicos. El crecimiento del uso de dispositivos conectados y el acceso masivo a internet han facilitado la expansión de este delito, haciendo que tanto personas naturales como jurídicas sean susceptibles a estas prácticas fraudulentas. Según la Ley 1273 de 2009, que modifica el Código Penal Colombiano, este tipo de conductas son tipificadas bajo los delitos contra la confidencialidad, la integridad y la disponibilidad de la información y los datos.

La relevancia de estudiar el phishing en Colombia radica en el impacto significativo que tiene en la economía y la confianza de los usuarios en los sistemas digitales. Colombia, siendo un país en desarrollo con un creciente índice de digitalización, ha sido testigo de un incremento en los casos de phishing, afectando no solo a individuos, sino también a empresas y entidades públicas. La falta de educación digital, combinada con el acceso masivo a plataformas en línea, crea un entorno propicio para que los delincuentes exploten la vulnerabilidad de los usuarios.

El presente capítulo tiene como objetivo identificar las diversas modalidades de estafa mediante phishing, analizando su impacto en la legislación colombiana y comparando con normativas internacionales. Se examinarán casos de estudio específicos para ilustrar cómo estas modalidades operan en la práctica y se evaluará la respuesta del sistema penal frente a estos desafíos.

Modalidades de Estafa mediante Phishing: Phishing tradicional: Suplantación de identidad mediante correos electrónicos fraudulentos

El phishing tradicional es la forma más común y reconocida de este delito. En esta modalidad, los delincuentes envían correos electrónicos que aparentan provenir de fuentes legítimas, como bancos, plataformas de pago o instituciones gubernamentales, solicitando a los usuarios que ingresen sus credenciales o información personal en un sitio web falsificado. Este tipo de estafa se

caracteriza por su alta capacidad de masificación y bajo costo operativo, lo que facilita su repetición en grandes volúmenes, afectando a miles de personas simultáneamente.

Spear phishing: Ataques dirigidos y personalizados a individuos o instituciones específicas

A diferencia del phishing tradicional, el Spear phishing se enfoca en objetivos específicos, utilizando información personalizada para ganar la confianza de la víctima. Estos ataques suelen estar dirigidos a ejecutivos de alto nivel, empleados de empresas con acceso a información crítica o instituciones con datos sensibles. Los correos electrónicos y mensajes utilizados en Spear phishing suelen contener datos personales del objetivo, obtenidos a través de redes sociales o bases de datos filtradas, lo que incrementa su efectividad.

Smishing y Vishing: Phishing a través de mensajes SMS y llamadas telefónicas: El Smishing (phishing mediante SMS) y el Vishing (phishing mediante llamadas de voz) son variantes del phishing que utilizan dispositivos móviles para ejecutar la estafa. En el Smishing, los delincuentes envían mensajes de texto que simulan ser de empresas conocidas, solicitando a los usuarios que ingresen sus datos en un enlace adjunto. El Vishing, por otro lado, implica llamadas telefónicas en las que los estafadores se hacen pasar por representantes de entidades financieras u otras organizaciones para obtener información sensible. Pharming: Redirección de usuarios a sitios web fraudulentos mediante la manipulación del DNS: El Pharming es una modalidad más avanzada de phishing que no requiere interacción directa del usuario para ser efectiva. A través de la manipulación del Sistema de Nombres de Dominio (DNS), los delincuentes redirigen a los usuarios a sitios web falsos incluso cuando estos ingresan la URL correcta de una página legítima. Esta técnica es particularmente peligrosa, ya que es difícil de detectar por el usuario promedio y puede afectar a un gran número de personas sin que estas sospechen de la manipulación.

Cada una de estas modalidades tiene ejemplos documentados en Colombia y a nivel global. En los últimos años, se han registrado numerosos incidentes en los que tanto ciudadanos como empresas han sido víctimas de correos electrónicos fraudulentos y ataques dirigidos que comprometen datos sensibles. A modo de ilustración, en 2022, una entidad bancaria colombiana reportó un aumento significativo en los intentos de Spear phishing dirigidos a sus empleados, evidenciando la evolución y adaptación de los delincuentes a medidas de seguridad más robustas Análisis Normativo y Legislación Colombiana Revisión de la normativa vigente en Colombia sobre delitos informáticos.

La legislación colombiana ha evolucionado para hacer frente a los desafíos que presentan los

delitos informáticos, incluyendo el phishing. La Ley 1273 de 2009 es una de las normas más relevantes en este ámbito, ya que establece un marco jurídico para la protección de la información y los datos en Colombia, tipificando conductas como el acceso abusivo a un sistema informático, la interceptación de datos y la utilización indebida de software malicioso. Sin embargo, a pesar de los avances, el phishing y sus modalidades no se encuentran tipificadas de manera explícita, lo que complica su persecución y juzgamiento. En el contexto del phishing, se considera que este delito puede ser subsumido en tipos penales como la suplantación de identidad, la estafa agravada y el acceso abusivo a sistemas informáticos. No obstante, la falta de especificidad y la constante evolución de las técnicas utilizadas por los delincuentes plantean retos significativos para los operadores judiciales. Esta situación resalta la necesidad de actualizar y adecuar la legislación para cubrir de manera efectiva todas las formas de phishing y fortalecer la capacidad de respuesta del sistema de justicia.

Análisis de la adecuación de las normas frente a las modalidades de phishing identificadas: La normativa vigente en Colombia, aunque cubre aspectos generales de los delitos informáticos, presenta vacíos importantes cuando se enfrenta a la complejidad y especificidad del phishing. Por ejemplo, las sanciones establecidas para la estafa mediante medios informáticos no siempre son proporcionales al daño causado, especialmente en casos de Spear phishing que pueden comprometer información crítica de empresas y entidades gubernamentales.

Además, el uso de técnicas como el Pharming, que manipulan sistemas informáticos sin que el usuario esté consciente, muestra la insuficiencia de las disposiciones actuales, que están principalmente enfocadas en conductas directas y evidentes de suplantación. Estos desafíos normativos evidencian la necesidad de una actualización legislativa que contemple de manera detallada las diversas modalidades de phishing, suplantando la tipificación genérica de delitos informáticos por definiciones más precisas y ajustadas a la realidad tecnológica actual.

Comparativa con la legislación de otros países para evaluar si la normativa colombiana está alineada con estándares internacionales. En comparación con la legislación internacional, Colombia presenta avances, pero también carencias significativas. Países como Estados Unidos y Reino Unido cuentan con marcos regulatorios más robustos, donde el phishing es tratado con una especificidad que permite la persecución efectiva de sus modalidades. Por ejemplo, en Estados

Unidos, leyes como el Computer Fraud and Abuse Act (CFAA) y el Identity Theft Penalty Enhancement Act han establecido bases legales claras para castigar a los perpetradores de phishing con penas severas y medidas de reparación para las víctimas.

En contraste, en Colombia, la falta de una definición específica y las dificultades en la identificación y persecución de los delitos de phishing reflejan una brecha que debe ser abordada. La cooperación internacional y la adopción de mejores prácticas globales pueden servir como guía para la implementación de políticas más efectivas en la lucha contra el phishing.

Ahora bien, se hace una presentación de casos emblemáticos de phishing ocurridos en Colombia Los casos de phishing en Colombia han demostrado ser variados en su modalidad y alcance, afectando tanto a usuarios individuales como a instituciones. Uno de los casos más emblemáticos es el del fraude a través de correos electrónicos bancarios falsos que afectó a cientos de usuarios de una reconocida entidad financiera en 2021. Los delincuentes lograron obtener información confidencial de los clientes, lo cual resultó en pérdidas económicas significativas y una crisis de confianza en los sistemas de seguridad de la entidad.

Otro caso destacado involucra un ataque de Spear phishing dirigido a una empresa de telecomunicaciones en 2022, donde los atacantes lograron acceder a información corporativa crítica mediante la suplantación del CEO de la empresa. Este incidente no solo comprometió datos internos, sino que también puso en riesgo la reputación de la compañía, evidenciando la sofisticación de las modalidades de phishing que están enfocadas en objetivos específicos y de alto perfil.

El análisis del impacto en las víctimas y las sanciones impuestas a los perpetradores: el impacto del phishing en Colombia va más allá de las pérdidas económicas; también afecta la confianza de los usuarios en los sistemas digitales. Las víctimas a menudo enfrentan no solo la pérdida de dinero, sino también daños emocionales y reputacionales, especialmente en casos de phishing dirigido o Spear phishing. En términos de sanciones, aunque se han logrado algunas condenas, los castigos impuestos en muchos casos no son proporcionales al daño causado, y la baja tasa de judicialización refleja las dificultades del sistema penal para enfrentar estos delitos.

Evaluación de la efectividad de las estrategias de prevención y judicialización: Las estrategias de prevención implementadas por instituciones financieras y otras organizaciones incluyen campañas de educación digital, autenticación de dos factores y mejoras en la seguridad de los sistemas informáticos. Sin embargo, la efectividad de estas medidas se ve limitada por la rápida

evolución de las técnicas de phishing y la falta de una cultura de ciberseguridad entre los usuarios. En términos de judicialización, los desafíos en la recolección de pruebas digitales y la necesidad de cooperación internacional para perseguir a los autores, que a menudo operan desde fuera del país, siguen siendo obstáculos críticos.

El análisis Comparativo con Legislación Internacional Comparación de la legislación colombiana con la de países como Estados Unidos, España y Brasil: en Estados Unidos, la legislación contra el phishing es amplia y bien definida, con penas severas para los infractores y un enfoque en la protección de los datos personales y la integridad de los sistemas informáticos. En España, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales y el Código Penal tipifican claramente las conductas de phishing y proporcionan herramientas legales para su persecución. Brasil, por su parte, ha avanzado con la Ley General de Protección de Datos (LGPD) y el Código Penal revisado, que incluyen disposiciones específicas para los delitos cibernéticos, incluido el phishing.

Identificación de fortalezas y debilidades en la normativa colombiana: comparando estos marcos legales con el colombiano, se evidencian varias áreas de mejora. Mientras que la normativa colombiana ha dado pasos hacia la protección contra delitos informáticos, aún carece de una especificidad y claridad que faciliten la persecución del phishing y sus modalidades. La introducción de políticas más detalladas y sanciones más severas podría mejorar significativamente la capacidad de respuesta del sistema penal colombiano.

La revisión de iniciativas internacionales en la lucha contra el phishing y su aplicabilidad en el contexto colombiano: La adopción de iniciativas como las alianzas público-privadas para la educación y prevención del phishing, y la implementación de sistemas avanzados de monitoreo y reporte de fraudes, podrían ser altamente beneficiosas para Colombia. La cooperación internacional y la participación en redes de intercambio de información son estrategias clave que han demostrado ser efectivas en otros países y que podrían ser replicadas en Colombia.

Los desafíos en la Investigación y Juzgamiento del Phishing, identificación de los principales desafíos que enfrenta la justicia colombiana en la investigación y procesamiento de casos de phishing: el procesamiento judicial del phishing en Colombia enfrenta múltiples desafíos que dificultan su efectividad. Uno de los principales problemas es la identificación de los autores de estos delitos, dado que muchos de los ataques se realizan de manera anónima o desde ubicaciones internacionales, lo que complica la cooperación y coordinación judicial entre países. La falta de

recursos especializados en ciberseguridad dentro de las instituciones judiciales también limita la capacidad de rastrear y recolectar evidencia digital, la cual es volátil y susceptible a la alteración o destrucción.

Además, las técnicas de phishing se desarrollan rápidamente, lo que significa que los delincuentes siempre están un paso adelante de las normativas y procedimientos tradicionales. Los sistemas de justicia a menudo no cuentan con las herramientas tecnológicas ni con el conocimiento actualizado necesario para seguir el ritmo de las innovaciones delictivas, lo que afecta la efectividad de las investigaciones.

Dificultades en la obtención de pruebas, cooperación internacional y limitaciones tecnológicas: la obtención de pruebas en los casos de phishing presenta retos significativos debido a la naturaleza transfronteriza del delito. Las evidencias digitales, como registros de IP, metadatos de correos electrónicos y otros datos de tráfico, pueden estar alojadas en servidores de otros países, lo que requiere cooperación internacional para acceder a dicha información. Sin embargo, los procesos legales para obtener estos datos suelen ser lentos y complejos, y la falta de acuerdos internacionales eficaces en algunos casos impide una respuesta rápida.

Por otro lado, las limitaciones tecnológicas dentro del sistema judicial colombiano, como la falta de software especializado y la escasez de personal capacitado en ciberseguridad, dificultan la recolección y el análisis de pruebas. Estas carencias afectan no solo la fase de investigación, sino también el juicio, ya que los fiscales y jueces a menudo no tienen la formación técnica necesaria para comprender plenamente la naturaleza del phishing y su impacto.

Impacto de la formación y la actualización constante en los operadores judiciales: la formación continua de los operadores judiciales es crucial para enfrentar el phishing de manera efectiva. Sin embargo, los programas de capacitación en delitos informáticos aún son insuficientes en Colombia, y muchos fiscales y jueces no están familiarizados con las nuevas modalidades de cibercrimen. La implementación de programas de formación especializados y la creación de unidades de cibercrimen dentro de las fiscalías podría mejorar significativamente la capacidad del sistema judicial para manejar casos de phishing. Presentación de estadísticas sobre la prevalencia del phishing en Colombia

El phishing es uno de los delitos informáticos más reportados en Colombia, con un aumento constante en los últimos años debido a la mayor penetración de internet y el uso masivo de dispositivos móviles. Según un informe de la Policía Nacional de Colombia (2023) se registraron

más de 10,000 denuncias relacionadas con fraudes electrónicos, de las cuales un alto porcentaje correspondió a casos de phishing. Los datos muestran que el phishing afecta principalmente a usuarios de banca en línea y comercio electrónico, siendo las entidades financieras las más afectadas. Gráficos recientes indican un crecimiento exponencial de los casos de Smishing (phishing mediante SMS), en particular durante eventos masivos de compras como el Black Friday, donde los delincuentes aprovechan el aumento en las transacciones en línea para ejecutar sus fraudes.

Análisis de tendencias y patrones detectados a partir de los datos: El análisis de los datos revela que las tendencias de phishing en Colombia se alinean con las observadas a nivel global, donde se observa un incremento en los ataques dirigidos (spear phishing) y en las técnicas que utilizan la ingeniería social para manipular a las víctimas. También se destaca un patrón de estacionalidad, con picos en los reportes durante festividades y eventos comerciales, lo que sugiere que los delincuentes aprovechan momentos de alta actividad económica y menor atención por parte de los usuarios.

En conclusión, El phishing, como una de las modalidades más prevalentes del cibercrimen, presenta un desafío significativo para la legislación y el sistema penal colombiano. Las modalidades de phishing, incluyendo Spear phishing, Smishing, Vishing y Pharming, han demostrado ser altamente adaptables y efectivas en su objetivo de engañar a los usuarios para obtener información confidencial. A pesar de los esfuerzos normativos, la respuesta legal aún no es completamente efectiva debido a la falta de especificidad en la tipificación de estos delitos y a las dificultades inherentes a la naturaleza transfronteriza del phishing.

Los casos de estudio revisados evidencian que tanto individuos como corporaciones son vulnerables a este tipo de estafa, y que la respuesta del sistema penal a menudo no está a la altura del impacto causado. Los esfuerzos de prevención y educación digital han avanzado, pero se requiere un enfoque más integral y una actualización de las leyes para enfrentar adecuadamente este delito. Según todo lo anteriormente narrado, e importante brindar recomendaciones al aparato judicial colombiano, para que de alguna u otra manera la regularización de este delito mejore en el país y lo realizamos de la siguiente manera: Actualización Legislativa: Es necesario reformar la normativa vigente para incluir disposiciones específicas sobre el phishing y sus modalidades, asegurando que las sanciones sean proporcionales al daño causado y que se incluyan medidas de reparación para las víctimas. Capacitación de Operadores Judiciales: Implementar programas de

formación especializada en cibercrimen para fiscales, jueces y policías, con un enfoque en la identificación, recolección y preservación de pruebas digitales. Fomento de la Cooperación Internacional: Fortalecer los acuerdos de cooperación con otros países para facilitar la obtención de pruebas y la persecución de delincuentes que operan desde el extranjero. Educación y Concientización: Ampliar las campañas de educación digital para la ciudadanía, enfocadas en la prevención del phishing y la ciberseguridad personal, para reducir la vulnerabilidad de los usuarios.

Capítulo III

Estrategias Implementadas Por Las Autoridades Judiciales Para Investigar Y Juzgar El Delito De Estafa A Través De La Modalidad Del Phishing.

El avance acelerado de las tecnologías de la información y la comunicación ha facilitado la proliferación de nuevas modalidades delictivas, entre las cuales se destaca la estafa a través de medios informáticos, con el phishing como una de sus formas más comunes y perjudiciales. El phishing se caracteriza por el uso de técnicas fraudulentas para obtener información confidencial de las víctimas, tales como contraseñas o datos bancarios, a través de correos electrónicos, sitios web falsos u otros medios electrónicos que simulan ser legítimos. Ante este panorama, las autoridades judiciales en Colombia se han visto en la necesidad de desarrollar e implementar estrategias adecuadas para investigar y juzgar este delito, enfrentando el desafío de adaptarse a una modalidad delictiva que constantemente evoluciona. El presente trabajo tiene como objetivo describir dichas estrategias, desde el marco normativo hasta los procedimientos judiciales, resaltando también los retos y desafíos en su aplicación y la manera en la que en la actualidad el sistema judicial colombiano a confrontado y combatido esta práctica, no llegando hasta su total desaparición, situación que es técnicamente imposible en cualquier tipo de delito y claramente sumando la facilidad con la que los delitos cibernéticos aumentan, pero si tratando y buscando la manera de elaborar planes de contingencia y de precaución para contrarrestar la practica del mismo.

En Colombia, el Código Penal regula el delito de estafa en su modalidad tradicional bajo el artículo 246, el cual reza de la siguiente manera: "*el que obtenga provecho ilícito para si o para un tercero, induciendo o manteniendo a otro en error por medio de artificios o engaños…"*, pero la estafa a través de medios informáticos, incluida la modalidad de phishing, se encuentra principalmente regulada por la Ley 1273 de 2009, que introduce el delito de violación de datos personales y otros crímenes relacionados con el uso indebido de tecnologías de la información. Esta ley fue promulgada con el propósito de fortalecer la protección de los datos personales y sancionar el uso indebido de herramientas informáticas, aumentando de manera significativa la regulación y la pena de este delito que actualmente se presenta en el país con gran afluencia.

En cuanto a la tipificación del phishing, aunque no se menciona específicamente por nombre

en la legislación colombiana, este se enmarca dentro de los delitos cibernéticos relacionados con la suplantación de identidad, la interceptación de datos y el acceso fraudulento a sistemas informáticos, todos ellos cubiertos en la Ley 1273. La legislación establece penas que pueden variar según el daño causado y la cantidad de víctimas afectadas. Además, se prevé la responsabilidad agravada cuando los hechos delictivos se cometen en masa, lo cual es común en casos de phishing, y teniendo en cuenta esto, es de gran importancia que para futuras modificaciones de la ley se tipifique de manera taxativa el delito, con todo lo que conlleva, sus modalidades, técnicas y demás conductos que lleven al perpetuador a cometerlo, adicional, como ya lo hemos mencionado en varios apartados de este documento, la concientización a la comunidad en general es de vital importancia, más allá de la ley, estas técnicas ayudarían a disminuir su práctica, teniendo en cuenta que las personas estarían mucho mas consientes y precavidas al momento de proporcionar sus datos y demás información de carácter sensible.

Por otro lado, Colombia ha ratificado acuerdos internacionales como el Convenio de Budapest sobre Ciberdelincuencia, lo que ha permitido adoptar estrategias investigativas comunes entre países para enfrentar la criminalidad transnacional vinculada al phishing y otros delitos cibernéticos y queremos hacer hincapié en este convenio de la siguiente manera:

Colombia ratificó el Convenio de Budapest mediante la Ley 1928 de 2018, promulgada el 24 de julio de 2018. Esto representó un paso significativo en la lucha contra la ciberdelincuencia en el país, ya que permitió:

Modernizar el marco legal: El convenio ofrece un marco para actualizar las leyes nacionales relativas a delitos informáticos, tipificando diversas conductas delictivas como el acceso no autorizado a sistemas, la interferencia en los datos, el abuso de dispositivos y la distribución de material relacionado con delitos cibernéticos.

Cooperación internacional: Facilita la cooperación judicial entre los países miembros del convenio, permitiendo a Colombia acceder a herramientas internacionales para el intercambio de información y la asistencia en investigaciones transfronterizas de ciberdelitos.

Estandarización de procedimientos: Introdujo directrices sobre cómo recolectar y preservar evidencia digital, la cual es crucial en la investigación de delitos como el phishing, el fraude electrónico, la pornografía infantil, entre otros.

Protección de derechos humanos: El convenio establece medidas de seguridad para garantizar que los derechos fundamentales, como la privacidad y la protección de datos, no sean vulnerados

en el marco de la investigación de ciberdelitos.

La ratificación del Convenio de Budapest ha permitido a Colombia fortalecer su respuesta judicial y policial ante delitos cibernéticos, promoviendo una mayor colaboración con otros países y mejorando sus capacidades para el combate contra amenazas globales como el fraude electrónico, la suplantación de identidad (phishing), la pornografía infantil y el robo de información.

A pesar de los avances, Colombia aún enfrenta desafíos en la implementación plena del convenio, tales como la falta de personal especializado y la necesidad de mayor inversión en tecnologías para la lucha contra delitos cibernéticos. Sin embargo, la adhesión al convenio ha sido un paso clave para mejorar la legislación y cooperación en la lucha contra la ciberdelincuencia.

La investigación de delitos de phishing requiere la utilización de técnicas forenses digitales avanzadas. En este sentido, las autoridades judiciales colombianas han desarrollado capacidades que permiten rastrear la actividad en línea de los sospechosos a través del análisis de la red, los dispositivos electrónicos y las comunicaciones interceptadas, siempre dentro de los límites que permite la ley en cuanto a la protección de la privacidad y los derechos fundamentales.

Entre las herramientas más utilizadas para investigar el phishing se encuentran las intervenciones tecnológicas autorizadas por los jueces competentes, como el monitoreo de las transacciones bancarias electrónicas y el análisis de las direcciones IP de los correos o páginas web utilizados para el fraude. El Centro Cibernético Policial, que depende de la Policía Nacional de Colombia, juega un papel clave en estas investigaciones. Este centro utiliza técnicas de inteligencia artificial y análisis de datos para identificar patrones de actividad sospechosa en la web y cooperar con instituciones financieras para bloquear cuentas comprometidas. Es muy importante hacer énfasis en la cooperación que debe tener el país con todas las instituciones financieras y el control que ellas tienen con la información sensible de sus clientes, teniendo en cuenta que se han presentado casos en los que las mismas entidades bancarias proveen a través de sus colaboradores, bases de datos con información no tan precisa pero suficiente para que las personas inescrupulosas y que se quieren lucrar de esto pues puedan hacerlo de manera efectiva, situación que se presenta en sobre manea actualmente en el país a través de llamadas telefónicas por medio de las cuales atraen a las personas a darles la información completa para acceder por ejemplo al manejo de sus tarjetas de crédito o demás.

Otro aspecto importante es el uso de redes internacionales de cooperación para rastrear y detener a los perpetradores de phishing que operan desde fuera de Colombia. Dado que muchos de

estos delitos involucran a criminales que operan en múltiples jurisdicciones, la Interpol y Europol desempeñan un papel esencial en la coordinación de esfuerzos transnacionales y que representa en gran manera el control que a la fecha se le puede dar al delito en el país, logrando obtener información mucho mas precisa de la manera en la que se comete el accionar delictivo.

En la lucha contra el phishing, la colaboración entre diversas instituciones es crucial. A nivel local, la Fiscalía General de la Nación trabaja de manera conjunta con el Centro Cibernético Policial y otras agencias gubernamentales para coordinar las investigaciones. El Grupo de Delitos Informáticos de la Fiscalía es responsable de dirigir las investigaciones y recopilar las pruebas necesarias para la judicialización de los responsables y buscar la manera de desmantelar de manera efectiva a la cadena completa de delincuentes que se encargan de utilizar de manera fraudulenta la información de las personas para su provecho propio o el de una entidad como tal.

Este trabajo interinstitucional es fundamental para abordar los casos que, muchas veces, implican no solo el phishing como delito, sino también otros delitos conexos como el lavado de activos y la asociación para delinquir. La Fiscalía también colabora con bancos, proveedores de servicios de internet y empresas tecnológicas para obtener pruebas y rastrear los fondos robados, a través de solicitudes judiciales formales que permitan el acceso a información sensible, por ende también es tan importante mantener educadas a todas estas entidades respecto a la modalidad en la que se practica este delito, logrando así, que dentro de estas compañías se generen planes de contingencia, implementen métodos de seguridad más efectivos y demás aspectos que de alguna u otra manera cooperen a que disminuya la practica y sea mucho más difícil para las personas acceder a información sensible.

A nivel internacional, la Interpol y otros organismos supranacionales cooperan en la persecución de redes de phishing transnacionales, proporcionando canales rápidos para la extradición de sospechosos y el intercambio de información sobre métodos y técnicas utilizadas por los ciberdelincuentes, método que colabora en sobre manera a la judicialización de estas personas y al objetivo de desmantelar por completo a la red que coopera para la práctica de este delito.

El juzgamiento del phishing en Colombia sigue los mismos principios básicos que los demás delitos, pero se enfrenta a retos únicos debido a la naturaleza intangible de las pruebas. En los juicios, es necesario que el Ministerio Público presente pruebas digitales obtenidas a través de herramientas forenses, demostrando cómo los autores utilizaron correos electrónicos o sitios web

fraudulentos para cometer el delito. Uno de los mayores desafíos para los jueces y fiscales es la identificación de los autores materiales del delito, quienes a menudo utilizan identidades falsas o redes anónimas para ocultar su ubicación y verdadera identidad.

Algunos casos emblemáticos en Colombia han sentado precedentes en cuanto al uso de pruebas digitales para condenar a los responsables de phishing. Un ejemplo significativo es el caso de una red de phishing desmantelada en 2022, el cual se desarrollo de la siguiente manera:

La red de phishing operaba mediante técnicas avanzadas de suplantación de identidad digital para engañar a víctimas y obtener información personal y financiera, como contraseñas, números de tarjetas de crédito, y datos de cuentas bancarias. Utilizaban correos electrónicos fraudulentos, mensajes SMS y sitios web falsificados que imitaban a instituciones financieras legítimas, induciendo a las víctimas a ingresar sus credenciales en páginas controladas por los delincuentes.

La operación de desmantelamiento fue liderada por la Policía Nacional de Colombia, con el apoyo de la Fiscalía General de la Nación y en coordinación con varias entidades bancarias afectadas. La operación incluyó:

Intervención en varias ciudades: Se llevaron a cabo allanamientos en Bogotá, Medellín, Cali, y Bucaramanga, donde se capturaron a más de 15 miembros de la red.

Incautación de equipos: Durante los operativos, se incautaron servidores, computadores, teléfonos móviles y dispositivos de almacenamiento utilizados para ejecutar los ataques.

Colaboración internacional: Se contó con la cooperación de agencias internacionales debido a que los ataques también afectaban a víctimas en otros países.

Este caso subrayó la importancia de la legislación relacionada con los delitos cibernéticos en Colombia, particularmente en el marco del Convenio de Budapest, ratificado por el país en 2018. Las autoridades pudieron utilizar métodos avanzados de investigación forense digital, alineados con las disposiciones del convenio, para rastrear la actividad criminal y recopilar evidencia crucial para procesar a los responsables.

Este caso es un ejemplo claro del creciente desafío que representa el phishing en la era digital, y cómo Colombia ha comenzado a adoptar medidas más robustas para combatir este tipo de ciberdelincuencia.

A pesar de los avances, la lucha contra el phishing enfrenta numerosos retos. Uno de los más grandes es la evolución constante de las técnicas utilizadas por los delincuentes, lo que requiere que las autoridades actualicen continuamente sus herramientas y métodos de investigación. Los

criminales utilizan métodos cada vez más sofisticados, como la suplantación de marcas reconocidas a través de correos electrónicos muy similares a los originales, y el uso de redes de botnets (computadoras manipuladas) para distribuir ataques masivos, además, el anonimato en internet sigue siendo una barrera significativa. Muchos ataques de phishing se realizan desde ubicaciones fuera de Colombia, lo que requiere una cooperación internacional eficaz, pero que a menudo se ve obstaculizada por diferencias en las leyes y procedimientos de los distintos países.

Frente a los desafíos, se proponen varias mejoras. En primer lugar, es crucial que los fiscales y jueces reciban capacitación continua en ciberseguridad y delitos informáticos para comprender mejor la naturaleza del phishing y la evidencia digital que se presenta en los juicios y se deben actualizar las leyes para adaptarse a las nuevas formas que toma este delito, garantizando así una mayor protección a los ciudadanos, adicional, es necesario fortalecer las alianzas internacionales para facilitar la captura de delincuentes fuera de las fronteras colombianas y mejorar la cooperación interinstitucional a nivel global.

También es importante hablar sobre la educación y la concientización en la guerra contra el fraude de phishing y de ciberdelincuencia en Colombia. La inversión en estos campos no solo salva a las personas y a las empresas, sino también la integridad de la sociedad ante las amenazas que plantean los ataques informáticos. El apoyo mutuo entre todos los campos y la propensión dinámica para modificar las tácticas educativas sería esencial para abordar este peligro cambiante.

La mayoría de veces los ciberdelincuentes dependen de la interacción humana, crear conciencia de como funcionan estos ataques y cuáles son las tácticas comunes de estas personas como por ejemplo correos electrónicos falsos, links con virus, mensajes de texto con enlaces maliciosos, etc., es esencial para empoderar a todos los usuarios.

Una de las mejores estrategias para prevenir y/o combatir el phishing en Colombia es la concientización masiva para educar a toda una población o un grupo selecto, pues si bien sabemos y como lo hemos desarrollado durante todo el trabajo las personas más vulnerables son las personas que tienen poco conocimiento de la tecnología, ya que pueden caer en trampas fáciles y pueden ser víctimas más vulnerables.

La inteligencia artificial (IA) puede ser clave en la lucha contra el phishing en Colombia, sobre todo con la mayor digitalización e incremento del uso de plataformas digitales, una herramienta la cual pueden utilizar de manera responsable las autoridades colombianas para la investigación y juzgamiento de dicho delito.

Las soluciones de la inteligencia artificial, basadas en algoritmos de aprendizaje automático, pueden identificar correos electrónicos con alta probabilidad de phishing mediante el reconocimiento de patrones y características típicas de mensajes de este tipo, analizando frases estructuras de correo y enlaces; estas soluciones se apoyan en la clasificación de correos, determinando cuáles de ellos son legítimos y cuáles emiten señales de advertencia, como remitentes desconocidos, enlaces sospechosos, o el hecho de que el mensaje no coincida con nuestro conocido patrón de comportamiento. Si bien miramos la Inteligencia Artificial es de gran ayuda puesto que, es posible escanear en tiempo real las URLs de los correos para su evaluación. Esto implica una evaluación tanto de la estructura del enlace, como la verificación de la existencia de dominios similares a los de instituciones legítimas o la reputación del sitio. A partir de este tipo de algoritmos, también se podrían detectar técnicas de spoofing en las URLs, donde el atacante hace uso de dominios de confianza para engañar a los destinatarios.

Como bien sabemos el gobierno es quien brinda las estrategias para evitar este tipo de delito cibernético, la tecnología lastimosamente evoluciona también para los ciberdelincuentes es por esto que una de las mejores estrategias que se pueden implementar son la MFA (Autenticación multifactor), esta se trata de una técnica fundamental para incrementar la seguridad en línea al requerir la verificación por diferentes métodos para poder validar la identidad de un usuario antes de poder acceder a una plataforma o sistema. La utilización de MFA proporciona una barrera extra que complica a los atacantes el acceso a cuentas comprometidas que hayan conseguido vulnerar las credenciales del usuario.

El phishing está orientado a adquirir las claves del usuario mediante manipulaciones, o, dicho de otra forma, se basa en correos electrónicos falsos que enumeran servicios legítimos. El atacante logra capturar la contraseña que, a su vez, le permite intentar iniciar sesión en la cuenta del usuario. La MFA está, por el contrario, orientada a introducir un segundo nivel de seguridad que se percibe como una última barrera; aun cuando se capture la contraseña, el atacante no podrá posteriormente entrar en la cuenta sin la intervención del segundo factor, que suele estar en el poder del usuario legítimo.

Ventajas del uso de MFA para prevenir el phishing

El uso de la autenticación multifactor (MFA) ofrece múltiples ventajas para prevenir el phishing. En primer lugar, se reduce la probabilidad de riesgo ante credenciales vulneradas, ya que, si las credenciales (usuario y contraseña) son comprometidas tras un ataque de phishing, el atacante

no puede acceder a la cuenta, dado que se requiere un segundo factor que niega el acceso. Además, la implementación de MFA mitiga vectores de ataque, ya que los códigos o tokens generados por aplicaciones de autenticación, como Google Authenticator o Authy, tienen una corta duración. Esto significa que, si una persona no tiene acceso inmediato a estos códigos, no podrá hacer uso de ellos para acceder a la cuenta. Asimismo, la MFA proporciona protección adicional en distintos servicios, aplicándose a plataformas digitales críticas como el correo electrónico, redes sociales y sistemas financieros, lo que garantiza una protección homogénea. Un claro ejemplo en Colombia es el banco Bancolombia, que requiere la introducción de una clave dinámica para realizar compras o transferencias, mientras que otras entidades bancarias confirman la identidad de los titulares a través de llamadas telefónicas.

Pese a los beneficios claros del MFA, existen retos que deben ser superados para que su uso sea generalizado en Colombia. Uno de los principales obstáculos es la resistencia del usuario, quienes a menudo ven el MFA como un paso innecesario que complica el inicio de sesión. La resistencia a la adopción del MFA aumenta si el usuario no comprende el valor añadido de la seguridad que ofrece. Otro reto significativo es el acceso a la tecnología; no todos los usuarios cuentan con un acceso fácil a smartphones o dispositivos para aplicaciones de autenticación, especialmente en zonas rurales o áreas de bajos recursos, lo que puede dificultar la implementación del MFA. Además, los costos de implementación para las empresas, particularmente las pequeñas y medianas empresas (pymes), pueden resultar altos y engorrosos, ya que generalmente requieren la integración de nuevos sistemas tecnológicos y la capacitación del personal.

Las estrategias para implementar el MFA y otros métodos de ciberseguridad en Colombia se ven reforzadas por la labor de los CSIRT (Computer Security Incident Response Team), que coordinan y gestionan incidentes de seguridad cibernética en el país. Este equipo desempeña un papel protagónico en la protección de infraestructuras críticas y en la defensa de los usuarios contra amenazas cibernéticas, incluyendo el phishing. El CSIRT se dedica a prevenir, detectar, responder y recuperarse de incidentes relacionados con el ciberdelito mediante una variedad de estrategias. Entre estas, destaca el monitoreo continuo y la detección anticipada de ataques de phishing, donde el CSIRT ejerce vigilancia en el ciberespacio para identificar señales de ataques contra usuarios y empresas. Utiliza herramientas avanzadas de análisis de tráfico y de inteligencia de amenazas para detectar sitios web o correos electrónicos maliciosos que podrían estar involucrados en estafas de phishing.

Otra estrategia fundamental del CSIRT es la emisión de alertas y avisos de seguridad, que se envían cuando se detecta un aumento en los ataques de phishing. Estas alertas son distribuidas a través de boletines y redes sociales, informando a instituciones públicas, privadas y ciudadanos sobre las amenazas que enfrentan, así como ofreciendo información sobre cómo identificar mensajes fraudulentos y tácticas utilizadas por los atacantes. En caso de un ataque activo, el CSIRT actúa como punto de contacto para coordinar la respuesta, trabajando junto a las instituciones afectadas para mitigar el impacto, identificar a los atacantes y evitar la propagación del ataque. Esto incluye la intervención técnica para bloquear el acceso a sitios fraudulentos y guiar a las víctimas sobre los pasos a seguir para proteger sus datos y cuentas comprometidas. También intercambian información con otros CSIRT a nivel internacional para rastrear campañas de phishing que operan desde otros países, facilitando así la cooperación en la persecución de ciberdelincuentes.

El CSIRT también está comprometido con el fortalecimiento de la infraestructura de ciberseguridad en el país, asegurando que los servidores, redes y sistemas de instituciones públicas y privadas cuenten con medidas de seguridad robustas para prevenir ataques de phishing y otras ciberamenazas. Promueve el uso de tecnologías de autenticación multifactor (MFA) y protocolos de cifrado, lo que disminuye la posibilidad de que los atacantes comprometan cuentas o sistemas mediante técnicas de phishing. En este contexto, el CSIRT Colombia aporta un valor significativo en la protección contra las amenazas de phishing, implementando un enfoque integral que abarca desde la prevención y la detección temprana hasta la educación y la rápida respuesta a incidentes. A pesar de los múltiples retos que enfrenta, como la falta de denuncia de incidentes y el rápido avance de las tácticas delictivas, las estrategias del CSIRT Colombia son fundamentales para reducir el impacto del phishing y mejorar la ciberseguridad del país.

Conclusiones

El crecimiento exponencial de las tecnologías digitales en Colombia ha incrementado la vulnerabilidad a los delitos cibernéticos, particularmente las estafas y el phishing, estas constituyen las dos modalidades más comunes de delincuencia cibernética. Nos estamos refiriendo al impacto que a nivel individual sufren los individuos y a nivel colectivo, las organizaciones, las entidades

del sistema financiero y la infraestructura crítica del país.

Colombia ha tenido un considerable incremento en la cantidad de casos de delitos cibernéticos, a lo cual ha contribuido intensamente la rápida adopción de servicios digitales y cada vez la dependencia del uso de internet para la realización de actividades económicas, sociales y gubernamentales. Esto le ha conferido al país un atractivo importante para los delincuentes que buscan explotar vulnerabilidades técnicas y humanas.

El phishing se convierte así en una de las modalidades más eficaces de estafa cibernética en Colombia esta consiste precisamente en engañar a las víctimas haciéndose pasar por entidades del entorno, es decir, bancos, empresas de telecomunicaciones o plataformas de comercio electrónico, si bien esta forma delictiva se ha sofisticado con el tiempo hasta llegar a formas más sutiles, como el spear phishing que se compone de mensajes dirigidos, con una personalización de la comunicación más creíble.

La sencillez que presenta el ciberdelincuente a realizar campañas masivas de phishing mediante el envío de correos electrónicos, mensajes de texto (SMS) o por medio de redes sociales, hace que el problema se agrave, ya que la baja concienciación general de la audiencia sobre las tácticas de actuación de los atacantes, así como la falta de sistemas avanzados de seguridad en algunos sectores favorece que los ataques tengan éxito.

Las entidades bancarias y financieras son uno de los sectores más afectados, dado que gran parte de las estafas que se producen tienen que ver con el acceso indebido a las cuentas bancarias. Sin embargo, no sólo este sector sufre ataques, sino que las pymes (pequeñas y medianas empresas) y los comerciantes electrónicos son atacados en sus sistemas de pago, en sus plataformas de venta en la red.

Pese a los grandes avances que se han conseguido en la lucha contra el cibercrimen, aún hay muchos elementos que dificultan la erradicación del phishing y los fraudes del cibercrimen en Colombia. Uno de los puntos más graves es la baja notificación de incidentes. Muchas de las víctimas no dan aviso de los ataques que sufrieron, bien por desconocimiento de los procesos establecidos o bien por vergüenza, y todo ello significa que las autoridades no tienen una visión del problema en su totalidad.

La mayor habilidad profesional de los delincuentes cibernéticos que operan desde fuera de las fronteras nacionales crea la necesidad de una cooperación internacional más efectiva para rastrear y desmantelar redes criminales que se dedican al phishing. El avance de las técnicas de ataque y la

poca conciencia sobre los riesgos de la ingeniería social de los usuarios son otro de los problemas más importantes.

A pesar de que Colombia ha avanzado en la creación de un marco jurídico y técnico para combatir el ciberdelito, le falta un enfoque más dinámico y coordinado de las políticas públicas en su conjunto, y de su perfeccionamiento.

Las políticas públicas deben centrarse en las diversas capacidades para responder a incidentes, así como potenciar la denuncia de las víctimas, planteando para ello un marco jurídico y técnico que se actualice constantemente a medida que avanza el marco jurídico y técnico de la ciberseguridad.

Habrá que hacer frente en un futuro a nuevos retos como el que plantean tecnologías emergentes como la inteligencia artificial o el machine learning, que pueden ser utilizados por los delincuentes para automatizar y perfeccionar ataques, y que pueden ser también empleados por los defensores de la ciberseguridad para detectarlos y mitigarlos.

A lo largo de esta investigación, se ha identificado que el delito de estafa ha encontrado en los medios informáticos un canal propicio para su diversificación, siendo el phishing una de las modalidades más comunes y peligrosas. Este tipo de fraude no solo aprovecha la vulnerabilidad de los usuarios en el entorno digital, sino que también expone la necesidad de una actualización constante en las normativas y herramientas de prevención. En el análisis de casos se ha evidenciado que, a pesar de los esfuerzos por regular este tipo de conductas, persisten vacíos legales y desafíos en la adaptación de las leyes penales tradicionales a los nuevos contextos tecnológicos.

El sistema penal colombiano ha avanzado en la tipificación y el juzgamiento de los delitos informáticos, pero la velocidad con la que se desarrollan nuevas modalidades de estafa, como el phishing, ha superado en muchos casos la capacidad de respuesta del Estado. Las estrategias judiciales implementadas han sido insuficientes en términos de actualización tecnológica y especialización de los operadores judiciales. El análisis normativo muestra que, si bien existen disposiciones en el Código Penal que contemplan el fraude mediante medios informáticos, la falta de claridad en la diferenciación de modalidades y la necesidad de pruebas digitales robustas ralentizan los procesos judiciales, afectando su efectividad.

Las estrategias implementadas por las autoridades judiciales para investigar y juzgar los delitos de phishing han mostrado avances en cuanto a cooperación internacional y uso de herramientas digitales. No obstante, se ha concluido que el principal reto reside en la capacitación continua de

los funcionarios judiciales y la actualización de los procedimientos investigativos. Las autoridades requieren no solo conocimientos técnicos sobre el uso de plataformas informáticas, sino también la capacidad de adaptarse a las nuevas técnicas empleadas por los ciberdelincuentes. La carencia de expertos en ciberseguridad dentro de los equipos investigativos sigue siendo un obstáculo para la eficacia de las investigaciones.

Los resultados de esta investigación subrayan la urgencia de reformas en el marco legal colombiano, tanto para precisar las modalidades del delito de estafa a través de medios informáticos como para establecer penas que se ajusten a la gravedad y alcance de estos delitos. Además, se concluye que, más allá de la creación de normas, es crucial que el sistema de justicia implemente programas de capacitación continua en delitos cibernéticos para jueces, fiscales y defensores. A nivel social, es indispensable fomentar una mayor educación sobre la ciberseguridad entre los ciudadanos, a fin de reducir las posibilidades de ser víctimas de delitos como el phishing.

Uno de los principales desafíos identificados en la investigación es la recopilación de pruebas digitales en casos de phishing y otros delitos informáticos. A pesar de que la legislación colombiana ha avanzado en reconocer la validez de las pruebas electrónicas, en la práctica, la obtención y preservación de dichas pruebas presenta dificultades técnicas y legales. Las limitaciones en la trazabilidad de las transacciones electrónicas y el anonimato de los ciberdelincuentes complican la construcción de un expediente probatorio sólido, afectando la eficacia de los procesos judiciales.

El análisis realizado muestra una desigualdad en la protección de las víctimas de estafa mediante phishing, especialmente entre aquellas con menos recursos tecnológicos o educativos. Mientras que algunos sectores de la población cuentan con conocimientos y herramientas para identificar potenciales fraudes, otros son más vulnerables ante los ataques, lo que refleja una brecha digital que incide en la capacidad de defensa de los derechos de las víctimas. Esta desigualdad plantea la necesidad de fortalecer los mecanismos de denuncia y atención para víctimas de delitos informáticos en todos los estratos sociales.

La investigación también concluye que la lucha contra el phishing y otros delitos informáticos no puede depender únicamente del sistema penal. Existe una responsabilidad compartida entre el Estado y el sector privado, particularmente en el ámbito financiero, que es uno de los más afectados

por estos fraudes. Los bancos y plataformas digitales deben implementar medidas preventivas más estrictas, tales como autenticación multifactorial y sistemas de alerta temprana, para proteger a sus usuarios. El trabajo conjunto entre el sector público y privado es fundamental para reducir la incidencia de estos delitos y mejorar la capacidad de respuesta ante ataques cibernéticos.

Finalmente, la evolución tecnológica ha permitido la expansión del delito de estafa a niveles globales, donde la geografía ya no es un límite para la comisión de estos actos. Esto plantea un desafío tanto para el sistema penal como para las víctimas, ya que muchas veces los delincuentes operan desde jurisdicciones internacionales, dificultando su persecución y enjuiciamiento. En este sentido, es vital que Colombia continúe fortaleciendo los tratados de cooperación judicial internacional para combatir el fraude digital de manera efectiva.

Referencias Bibliográficas

Asúa, L. J. (2011, mayo 12). Pensamiento penal. Obtenido de http://www.pensamientopenal.com.ar/autores/luis-jimenez-asua

Bortnik, S. (2011). Ciberdelincuencia: Impacto y Estrategias de Mitigación en América Latina.

Caracol Radio. (2021). Nota periodística respecto al aumento de los ciberdelitos en Colombia. Obtenido de https://caracol.com.co/radio/2021/11/24/tecnologia/1637765496_602642.html

Carrasquilla, F. (2007, febrero 15). SCIELO. Obtenido de http://www.scielo.org.co/pdf/dere/n42/n42a03.pdf

Congreso de la República de Colombia. (2009). Ley 1273 de 2009.

Duarte, M. A. (2017, mayo 9). Repositorio Unilibre. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/24154/01%20DERECHO%20PENAL%20Y%20CIBERBULLYING%20EN%20J%C3%93VENES%20DE%20COLOMBIA%20-%20FINAL%20-%20NOV.24.2022.pdf?sequence=2

ESET Latinoamérica. (2021). Informe de amenazas 2021: Un enfoque en Colombia. Recuperado de https://www.eset-la.com/informe-amenazas-2021

García, J. (2019). Estafas en línea: Tácticas y prevención en el contexto colombiano. *Revista colombiana de Criminología*, 12(1), 45-67.

Gobierno Digital MinTIC. (s. f.). Estrategias CSIRT Gobierno. Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno

Jiménez, A., & Pérez, S. (2021). La evolución del cibercrimen en Colombia: Retos y estrategias. *Revista de Derecho Penal y Criminología*, 25(2), 123-147.

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, España. Obtenido de https://www.microsoft.com/es-co/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication#:~:text=La%20autenticaci%C3%B3n%20multifactor%20(MFA)%20agrega,que%20reciben%20en%20su%20tel%C3%A9fono.

Lima, M. D. (2008, enero 12). Terra Jurista. Obtenido de https://www.terragnijurista.com.ar/doctrina/informaticos.htm

Ltda, L. C. (2019, noviembre 12). Infolaft. Obtenido de https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2022). Informe anual sobre ciberseguridad en Colombia. Recuperado de https://www.mintic.gov.co/portal/informes/2022/ciberseguridad

Policía Nacional de Colombia. (2023). Informe de cibercrimen: Estadísticas y análisis de delitos informáticos en Colombia.

Reinosa, U. A. (2015, enero 12). UNICEF Organización. Obtenido de https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Ruiz, M. F. (2022). Impacto de las estafas en línea en las pequeñas y medianas empresas en Colombia. Repositorio Universidad Javeriana de Bogotá.

Torres, E. (2023). Tendencias actuales en la estafa cibernética en Colombia: Un estudio de caso de phishing y fraude en redes sociales. Editorial Universidad del Rosario.

United States Department of Justice. (2022). Computer Fraud and Abuse Act (CFAA). Obtenido de https://www.secureit.es/csirt/

Entrust. (s. f.). What is multi-factor authentication (MFA)?. Obtenido de https://www.entrust.com/es/resources/learn/what-is-multi-factor-authentication-mfa