UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

CARRERA DE DERECHO.

INFORME FINAL DEL TRABAJO DE INTEGRACIÓNCURRICULAR

MODALIDAD SEMIPRESENCIAL

TEMA:

´´ LOS DELITOS DE ESTAFA Y APROPIACIÓN FRAUDULENTA POR REDES SOCIALES OCURRIDOS EN LA CIUDAD DE CAYAMBE AÑO 2022 – 2023”

Trabajo de titulación previo a la obtención del título de: Abogado de los Tribunales de la República del Ecuador.

Línea de investigación: Desarrollo social y del comportamiento humano.

Autor:

Reny Fabricio Perez Bonilla

Director:

Mgs. Francisco Xavier Alarcón Torres.

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	230002877-2		
APELLIDOS Y NOMBRES:	PEREZ BONILLA RENY FABRICIO		
DIRECCIÓN:	Cayambe, Pichincha, Ecuador		
EMAIL:	rfperezb@utn.edu.ec		
TELÉFONO FIJO:		**TELF. MOVIL**	0998176283

DATOS DE LA OBRA	
TÍTULO:	"LOS DELITOS DE ESTAFA Y APROPIACIÓN FRAUDULENTA POR REDES SOCIALES OCURRIDOS EN LA CIUDAD DE CAYAMBE AÑO 2022 – 2023´´
AUTOR (ES):	PEREZ BONILLA RENY FABRICIO
FECHA:	09/03/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	ABOGADO DE LOS TRIBUNALES DE LA REPÚBLICA DEL ECUADOR.
ASESOR/DIRECTO:	Mgs. FRANCISCO XAVIER ALARCÓN TORRES.

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 09 del mes de marzo de 2025.

EL AUTOR:

Firma.

Reny Fabricio Perez Bonilla

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Ibarra, 24 de julio del 2024

Msc. Francisco Xavier Alarcón Torres

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que seajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo supresentación para los fines legales pertinentes.

Firmado electrónicamente por:
FRANCISCO XAVIER
ALARCON TORRES

MSC. FRANCISCO XAVIER ALARCÓN TORRES

C.C. 1003694955

APROBACIÓN DEL COMITÉ CALIFICADOR

El comité calificado del trabajo de integración curricular ´´ Los delitos de estafa y apropiación fraudulenta por redes sociales ocurridos en la ciudad de Cayambe año 2022 –2023´´. Elaborado por Reny Fabricio Perez Bonilla, previo a la obtención del título de abogado de los tribunales de la República del Ecuador, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

Firmado electrónicamente por: FRANCISCO XAVIER ALARCON TORRES

MSC. FRANCISCO XAVIER ALARCÓN TORRES

CC: 1003694955

ALEXANDRA CRISTINA PUPIALES PROANO

Firmado digitalmente por ALEXANDRA CRISTINA PUPIALES PROANO
Fecha: 2025.03.05 11:54:45 -05'00'

MSC. ALEXANDRA CRISTINA PUPIALES PROAÑO

CC: 1004418917

DEDICATORIA

A mis padres Esteban Pérez y Ana María Bonilla, por su apoyo inefable ante las adversidades. Personas a las cuales guardo admiración y respeto por su arduo trabajo en la fomentación de valores a mis hermanos como a mi persona, por esa razón y muchas más deseo que este gran logro en mi vida quede guardado y escrito con fuego en lo más profundo de mi corazón, pues son la incognoscible fuerza que me motiva a seguir adelante.

A mis hermanos. Katy Bravo, Alexandra Bonilla, Daniel Pérez, Julio Pérez, Valentín Pérez y Jefferson Pérez que los quiero con toda mi alma, por apoyarme en todo momento que a pesar de muchas veces quise rendirme, pero ellos han me dejaron caer y confiaron en mí, dándome ese impulso para no rendirme, además han guiado mi vida y compartido muchas alegrías.

A mis bellos ángeles que se encuentran en el cielo mis abuelitas Mercedes llaguno, Rosa María Yunga y en especial a mi hermano Edison Bravo Bonilla quien fue mi inspiración para superarme. Este logro va por ustedes, aunque no estén físicamente sé que están en forma espiritual y donde quieran que estén este logro va por ustedes.

AGRADECIMIENTO

Quiero dar gracias a dios por darme vida y salud para poder alcanzar este logro y expresar mi profundo agradecimiento a la UNIVERSIDAD TÉCNICA DEL NORTE, por permitirme formar mi vida profesional en sus aulas, a mi director de tesis Dr. Francisco Alarcón, y a mi asesora Dra. Alexandra Pupiales por su orientación, experiencia, paciencia y motivación constante a lo largo de este proyecto. También quiero agradecer a todos los docentes que de la carrera de derecho por sus valiosas contribuciones y consejos durante mi etapa académica.

Además, agradezco a mis amigos y compañeros de clase Valentina Imba, Dagmar Gualavisí, Santiago Saltos, Héctor Chancosi, Alison Chacón, Yoselin Guerrero y Cristian Vaca por los bellos momentos compartidos y su apoyo en los momentos difíciles.

También quiero agradecer a mis Cuñados; Edwin morales, Cesar Estrella, Orfilia Cevallos y Andrea Cabrera quienes fueron apoyo constante en este proceso y un grato agradecimiento a mi cuñada Jennifer Cevallos por apoyarme y darme aliento para no decaer antes las adversidades que se me presentaron durante esta investigación.

Mi gratitud se extiende a la familia Delgado Perez porque en debido tiempo fuera un gran apoyo para lograr este objetivo y en especial a Dayanara Delgado por apoyarme y darme aliento cuando inicie mi carrera universitaria.

Por último, pero no menos importante, agradezco a todas las personas que participaron en este estudio que generosamente compartieron sus experiencia y tiempo, para llevar a cabo esta investigación. Su colaboración fue fundamental para el éxito de este trabajo

RESUMEN EJECUTIVO

Las redes sociales nos han cambiado la vida, es una herramienta fundamental para la sociedad, nos ha traído grandes beneficios se han vuelto tan populares en la vida cotidiana de las personas, de igual forma, nuevos desafíos al sistema judicial. El art.190 apropiación fraudulenta por medios electrónicos, la estafa art.186 se encuentran tipificado en el código orgánico integral penal. Establece sanciones con pena privativa de treinta días hasta 10 años.

En esta investigación es necesario analizar los dos tipos de denuncia que se realizó principalmente en la fiscalía de la cuidad de Cayambe en los años 2022-2023, estafa y apropiación fraudulenta por medios electrónicos. Los pocos casos investigados en la Fiscalía de Cayambe no han tenido juzgamiento por falta de pruebas y personal capacitado para la investigación de estos delitos.

Para este estudio se solicitó las bases de datos de la fiscalía general del estado sobre los casos denunciado y cuantos tuvieron una sentencia ejecutoriada, realizando entrevista a los profesionales del derecho como Abogados de libre ejercicio, Fiscales, personal de inteligencia de la policía judicial y jueces de Cayambe, de este modo se logró demostrar las dificultades que presenta el sistema justicia y la deficiencia en la investigación de estos delitos.

***Palabras clave*:** *Derecho, redes sociales, ordenamiento, medios electrónicos, delitos informáticos, fraude.*

ABSTRACT

Social networks have changed our lives, it is a fundamental tool for society, it has brought us great benefits, they have become so popular in people's daily lives, as well as new challenges to the judicial system. Article 190 fraudulent appropriation by electronic means, fraud art.186 are typified in the Comprehensive Organic Criminal Code. It establishes penalties with imprisonment of thirty days to 10 years.

In this investigation, it is necessary to analyze the two types of complaints

that were made mainly in the prosecutor's office of the city of Cayambe in the years 2022-2023, fraud and fraudulent appropriation by electronic means. The few cases investigated in the Cayambe Prosecutor's Office have not been tried due to lack of evidence and trained personnel for the investigation of these crimes.

For this study, the databases of the state attorney general's office on the cases reported and those that had an enforceable sentence were requested, conducting interviews with legal professionals such as free practice lawyers, prosecutors, intelligence personnel of the judicial police and judges of Cayambe, in this way it was possible to demonstrate the difficulties presented by the justice system and the deficiency in the investigation of these crimes.

Key words*: Law, social networks, ordering, electronic media, computer crimes, fraud.*

INDICE DE CONTENIDO

INTRODUCCIÓN

Planteamiento del problema

El incremento de los delitos de estafa y apropiación fraudulenta a través de redes sociales en la ciudad de Cayambe durante el período 2022-2023 constituye un fenómeno alarmante que merece una atención académica y jurídica rigurosa. Este tipo de delitos ha evolucionado en paralelo con el desarrollo de las tecnologías de la información, transformándose en una amenaza significativa para la seguridad económica y social de los ciudadanos. La facilidad de acceso a internet y la proliferación de redes sociales han facilitado la comisión de estos delitos, presentando un desafío considerable para el sistema de justicia ecuatoriano.

La jurisprudencia ecuatoriana, en particular las sentencias del Tribunal de lo Penal, han reconocido la complejidad de estos delitos, destacando la necesidad de un enfoque multifacético para su persecución y sanción. La doctrina jurídica ha subrayado que la estafa y la apropiación fraudulenta, definidos en el Código Orgánico Integral Penal, COIP (2021) requieren no solo la identificación del engaño y el abuso de confianza, sino también la prueba del perjuicio económico sufrido por la víctima. Este enfoque integral es esencial para comprender la dinámica de los delitos cometidos a través de plataformas digitales.

En este contexto, el problema de investigación se centra en la identificación de los factores que facilitan la perpetración de estafas y apropiaciones fraudulentas mediante redes sociales en Cayambe, así como en la evaluación de la efectividad de las medidas legales vigentes para combatir este tipo de criminalidad. La falta de un marco regulatorio específico para los delitos cibernéticos en Ecuador añade una capa de complejidad al problema, ya que las herramientas jurídicas tradicionales a menudo resultan insuficientes para abordar las particularidades de estos delitos.

Además, el análisis de casos judiciales recientes en Cayambe revela patrones comunes en la metodología de los delincuentes, quienes aprovechan la falta de conocimiento técnico de las víctimas y la insuficiente educación digital para llevar a cabo sus acciones fraudulentas. Este patrón de comportamiento delictivo subraya la necesidad de implementar estrategias preventivas que incluyan campañas de sensibilización y educación sobre seguridad digital, así

como la capacitación de las autoridades judiciales en el manejo de delitos cibernéticos **(Armijos, 2023)**.

La doctrina jurídica enfatiza la importancia de la cooperación internacional en la lucha contra los delitos cibernéticos, dado que las redes sociales son plataformas globales y los delincuentes pueden operar desde cualquier parte del mundo. En este sentido, la adhesión de Ecuador a tratados internacionales sobre cibercrimen y la colaboración con organismos internacionales resulta crucial para mejorar la capacidad del sistema judicial en la persecución de estos delitos **(Chapi, Chulde, Bracero, & Moreno, 2024)**.

En tanto, el estudio de los delitos de estafa y apropiación fraudulenta por redes sociales en Cayambe durante el período 2022-2023 requiere un abordaje multidimensional que considere tanto la dimensión tecnológica como la jurídica. La actualización de la normativa penal, la capacitación de las autoridades y la educación de la ciudadanía son elementos fundamentales para combatir eficazmente esta problemática, garantizando así la protección de los derechos económicos y la seguridad de los ciudadanos en el entorno digital.

Justificación

La justificación de la investigación realizada en la ciudad de Cayambe durante los años 2022 y 2023 sobre los delitos de estafa y apropiación fraudulenta a través de redes sociales radica en el aumento significativo de estos crímenes y en su repercusión en la estabilidad económica y social de los habitantes. El avance tecnológico y la amplia disponibilidad de plataformas digitales han simplificado la perpetración de estos crímenes, los cuales poseen atributos particulares y de naturaleza compleja. Es fundamental comprender el modus operandi de estos individuos delictivos y familiarizarse con los recursos legales disponibles para combatirlos, con el fin de garantizar la protección efectiva de los ciudadanos.

El examen de la jurisprudencia ecuatoriana indica que las leyes vigentes, como las contempladas en el Código Orgánico Integral Penal, COIP (2021) no resultan siempre adecuadas para enfrentar la complejidad de los delitos informáticos. La doctrina jurídica resalta la importancia de contar con una legislación más detallada y acorde a los avances tecnológicos actuales. El propósito de este estudio es proporcionar pruebas concretas que sustenten la modificación legal requerida para reforzar la lucha contra dichos crímenes y aumentar la salvaguarda de las personas afectadas.

Es fundamental identificar los patrones de comportamiento de los delincuentes y las vulnerabilidades de las víctimas para poder diseñar estrategias de prevención eficaces. La falta de competencias en el ámbito digital y la escasa conciencia acerca de los peligros en internet son elementos que aumentan la vulnerabilidad de los individuos a la manipulación. El estudio en cuestión ofrecerá datos relevantes que podrán ser utilizados en la creación de planes educativos y campañas de sensibilización, dirigidos tanto a la población en general como a las entidades responsables de la aplicación de la normativa.

La investigación se justifica por la importancia de la cooperación internacional y la adhesión a tratados sobre cibercrimen. Los crímenes cibernéticos superan límites territoriales y demandan una acción coordinada a escala internacional. La evidencia recopilada en el estudio puede ser utilizada como fundamento para fomentar la colaboración entre Ecuador y otras naciones en la lucha contra el fraude y la estafa en línea. Esto contribuirá al fortalecimiento del marco jurídico y operativo para abordar eficazmente estos desafíos.

Es fundamental proporcionar formación en técnicas modernas de investigación cibernética a las autoridades judiciales y policiales para mejorar la eficacia en la lucha contra estos crímenes. El estudio permitirá identificar las deficiencias presentes en la formación y propondrá soluciones para mejorar las habilidades de los profesionales del sistema judicial. La implementación de estas mejoras resulta fundamental para garantizar la eficiencia y la adecuación del sistema judicial a las demandas del entorno digital.

La importancia social de este estudio reside en su capacidad para reducir la cantidad de personas afectadas por engaños y fraudes en plataformas digitales. Al contribuir de manera integral a abordar esta problemática, se promoverá la construcción de un entorno digital más seguro y confiable, lo cual resultará en el fomento de la confianza de los usuarios en las tecnologías de la información. En síntesis, el propósito de esta investigación es no solo contribuir al avance del conocimiento académico, sino también impactar de manera positiva en el ámbito jurídico y social de la ciudad de Cayambe y, por consiguiente, del Ecuador.

Impactos de la investigación

El estudio de los delitos de estafa y apropiación fraudulenta a través de plataformas digitales en Cayambe durante el periodo 2022-2023 tendrá repercusiones relevantes en diversos ámbitos. Esta investigación aportará al avance del conocimiento académico y a la formulación de políticas públicas más efectivas. En primer lugar, se ofrecerá un análisis detallado de los

métodos y estrategias empleados por los criminales informáticos, aspecto fundamental para la formulación de estrategias preventivas e intervencionistas. El presente estudio posibilitará la identificación de vulnerabilidades particulares en la población, lo cual favorecerá el diseño de programas educativos y campañas de sensibilización con el fin de disminuir la prevalencia de dichos delitos.

En el contexto jurídico, este estudio proporcionará pruebas empíricas que podrían tener impacto en la modificación del marco legal de Ecuador, específicamente en relación con el Código Orgánico Integral Penal (COIP). La necesidad de ajustar las leyes a las nuevas formas de delitos surgidas a raíz del progreso tecnológico ha sido destacada por la doctrina jurídica. Los resultados de esta investigación pueden ser fundamentales para la elaboración de iniciativas legislativas que refuercen la capacidad del sistema judicial en la lucha efectiva contra los delitos cibernéticos, asegurando de esta manera una protección más sólida para las personas afectadas.

Otro impacto significativo de esta investigación es la capacitación de las autoridades judiciales y policiales en técnicas avanzadas de investigación cibernética, desde una perspectiva operativa. El estudio propiciará la implementación de programas de capacitación específicos con el fin de mejorar la efectividad en la persecución de delitos, al identificar las deficiencias presentes en la formación de los operadores de justicia (Morocho, 2022). El incremento en la competencia técnica de los agentes encargados de hacer cumplir la ley resultará en una respuesta más efectiva frente a la delincuencia cibernética y en una mayor eficacia en la resolución de casos.

La investigación tendrá un impacto positivo en el ámbito social al promover la creación de un entorno digital más seguro y confiable en Cayambe. Esto ayudará a disminuir la percepción de vulnerabilidad que experimentan los usuarios de redes sociales en la zona. El estudio de la dinámica de los delitos de estafa y apropiación fraudulenta, así como la propuesta de soluciones efectivas, contribuirá al fortalecimiento de la confianza en la utilización de tecnologías de la información. El impacto positivo resultante no solo favorecerá a los individuos directamente implicados, sino que también contribuirá al fortalecimiento de la cohesión social al fomentar una cultura de seguridad y responsabilidad digital en el entorno comunitario.

Objetivos

General

- Evaluar el impacto de la normativa vigente en la prevención y sanción de los delitos de estafa y apropiación fraudulenta por redes sociales en la ciudad de Cayambe durante el período 2022-2023, mediante un análisis comparativo de casos y la aplicación efectiva de dichas normativas.

Específicos

- Analizar las bases teóricas, doctrinales y normativas vigentes relacionadas con los delitos de estafa y apropiación fraudulenta por medios electrónicos, enfocándose en su aplicación a través de redes sociales.
- Realizar estudios de casos específicos de estafa y apropiación fraudulenta por redes sociales en Cayambe, utilizando herramientas de investigación como entrevistas y análisis de datos proporcionados por la Fiscalía General del Estado.
- Evaluar la aplicación de sanciones por parte de los jueces en casos de estafa y apropiación fraudulenta, identificando vacíos legales y desafíos en la normativa actual para abordar eficazmente estos delitos cometidos a través de internet.

Capítulo 1: Marco Teórico

1.1.Definición de Estafa y apropiación fraudulenta

1.1.1. Concepto general de Estafa

La estafa se define como un acto delictivo en el cual se emplea el engaño con el propósito de inducir a error a un individuo, obteniendo de esta manera una ganancia ilegítima a expensas de la pérdida económica de la persona afectada. El delito mencionado está tipificado en el Código Orgánico Integral Penal (COIP) de Ecuador. Consiste en la alteración de la percepción de la realidad por parte del perpetrador, quien recurre a estratagemas, promesas falsas o representaciones engañosas con el fin de alcanzar sus objetivos delictivos. La estafa se tipifica como un acto delictivo que atenta contra el patrimonio y la confianza pública, siendo su sanción orientada a resguardar la estabilidad financiera de los individuos (Cisneros & Jiménez, 2021).

En el contexto del derecho en Ecuador, la estafa está definida en el artículo 186 del Código Orgánico Integral Penal (COIP). Según esta disposición, se considera perpetrador de este crimen a aquel individuo que, con la intención de obtener ganancias y a través de engaños o artimañas, logra inducir a error a otra persona, obteniendo de ella un beneficio económico injusto. La penalización por el delito de estafa experimenta variaciones en función del nivel de daño ocasionado, pudiendo intensificarse en caso de la presencia de factores particulares como la reincidencia, la utilización de tecnologías informáticas o el perjuicio a individuos en situación de vulnerabilidad. La jurisprudencia ha establecido criterios para identificar la presencia de los elementos que conforman el engaño y el perjuicio.

Según la doctrina jurídica, el engaño en el delito de estafa debe ser lo bastante efectivo como para inducir a error a un individuo razonable, no siendo suficiente con simples exageraciones o declaraciones imprecisas. El daño económico, por otro lado, debe ser específico y susceptible de ser valorado económicamente. El enfoque doctrinal resalta la importancia de establecer una relación causal directa entre el acto de engaño y la pérdida de patrimonio experimentada por la víctima. En relación a este tema, los tribunales de Ecuador han enfatizado la importancia de demostrar tanto el acto de engaño como las consecuencias económicas derivadas para determinar la responsabilidad penal (Ibarra, 2021).

La evolución de las tecnologías de la información ha dado lugar a nuevas formas de fraude, como los perpetrados en redes sociales y plataformas digitales. En Ecuador, la jurisprudencia ha iniciado el abordaje de estos casos considerando las especificidades del entorno digital. El

potencial delictivo de las estafas se ve amplificado por el anonimato y la facilidad de difusión de información falsa en internet, lo cual demanda una interpretación flexible y actualizada de las normas penales vigentes para su correcta aplicación (Acosta, 2024).

La colaboración internacional es un factor importante en la prevención de fraudes, sobre todo en situaciones en las que los criminales actúan desde el extranjero o emplean recursos transfronterizos. Ecuador ha firmado múltiples acuerdos internacionales que favorecen la cooperación judicial y la entrega de personas acusadas de cometer delitos informáticos. La importancia de estas herramientas legales es destacada por la doctrina, ya que aseguran una respuesta efectiva y coordinada frente a la delincuencia transnacional, lo que a su vez contribuye a fortalecer la seguridad jurídica a nivel mundial.

Es por ello que, el fraude es un crimen complejo que requiere un examen minucioso de los componentes de engaño y daño, ajustándose de manera continua a los avances tecnológicos actuales. Enfrentar este delito en Ecuador se ve respaldado por un marco interpretativo sólido proporcionado por la jurisprudencia y doctrina del país, que pone énfasis en la protección del patrimonio y la integridad económica de los individuos (Velasquez, 2022). La actualización constante de las normativas y la colaboración a nivel internacional son aspectos esenciales para abordar de manera efectiva las múltiples modalidades de fraude que emergen en el entorno digital y globalizado.

1.1.2. Apropiación Fraudulenta

La apropiación fraudulenta es un acto delictivo que consiste en la adquisición indebida de bienes pertenecientes a otra persona con el propósito de obtener una ganancia personal, causando un perjuicio económico al dueño legítimo. En el marco legal de Ecuador, este acto ilícito está definido en el Código Orgánico Integral Penal (COIP), concretamente en el artículo 187. De acuerdo con esta normativa, se impone una sanción a aquella persona que, en base a un contrato o relación de confianza, se apropia de bienes muebles o valores que le han sido confiados para su depósito, administración o custodia, con la intención de apropiárselos de forma indebida.

Según la doctrina jurídica, resulta fundamental que exista una relación de confianza previa entre el autor del delito y la víctima para que se configure el delito de apropiación fraudulenta. La manifestación de esta confianza se observa en situaciones contractuales de depósito, administración o custodia de bienes, en las cuales la persona afectada entrega de manera

voluntaria sus propiedades al responsable. El acto delictivo se centra en la violación de la confianza a través de la apropiación ilegal de los bienes. La confianza traicionada es un elemento subjetivo crucial que distingue la apropiación fraudulenta de otros delitos contra el patrimonio (Montenegro, Gutiérrez, Lugmaña, & Moreno, 2024).

En el ámbito de la jurisprudencia, los tribunales de Ecuador han establecido una serie de criterios para identificar la presencia de apropiación fraudulenta. Dentro de estos parámetros se consideran la validación de la relación de confianza inicial, la prueba de la posesión de los activos y la intención fraudulenta del perpetrador. La importancia de probar la intención de apropiación y el daño económico causado a la víctima ha sido resaltada por los fallos judiciales. Este método garantiza que únicamente se impongan sanciones a aquellos comportamientos que verdaderamente representen una violación seria de la confianza y ocasionen un daño económico importante.

Las sanciones establecidas en el artículo 187 del Código Orgánico Integral Penal (COIP) son proporcionales al daño económico ocasionado. En situaciones en las que el valor de los bienes sustraídos sea significativo o cuando el perpetrador del delito abuse de su posición de confianza, las sanciones pueden ser agravadas. La aplicación de estas sanciones ha sido respaldada por la jurisprudencia en múltiples casos, enfatizando la importancia de una respuesta penal que sea proporcional al perjuicio ocasionado. La proporcionalidad en la imposición de sanciones tiene como objetivo no solo la penalización del transgresor, sino también la prevención de posibles conductas de apropiación fraudulenta en el futuro (Sempértegui, 2022).

El avance de la tecnología y la creciente utilización de plataformas digitales han generado nuevas modalidades de fraude, especialmente en los sectores financiero y empresarial. La doctrina jurídica ecuatoriana ha comenzado a explorar estas nuevas modalidades, reconociendo que la digitalización facilita la comisión de estos delitos al permitir el acceso y control remoto de bienes y valores. En un entorno tecnológico en constante evolución, los tribunales han ajustado sus interpretaciones para abarcar estas nuevas modalidades de apropiación, asegurando de esta manera una protección constante del patrimonio (Aguirre, 2022).

En tanto, la apropiación indebida en el contexto de Ecuador constituye un delito de naturaleza compleja que conlleva la transgresión de la confianza y la adquisición ilegítima de propiedades. La doctrina y la jurisprudencia han establecido un sólido marco para abordar este delito,

garantizando que las sanciones sean proporcionales y eficaces. Es fundamental para preservar la eficacia de la protección jurídica en un entorno digital en constante evolución, que las interpretaciones legales se ajusten continuamente a los avances tecnológicos.

1.1.3. Diferencias y similitudes entre ambos delitos.

Los delitos de estafa y apropiación fraudulenta, a pesar de afectar ambos al patrimonio, muestran divergencias importantes en su comisión y en los elementos que los conforman. La estafa, definida en el artículo 186 del Código Orgánico Integral Penal (COIP) de Ecuador, implica la utilización de la decepción con el propósito de llevar a la víctima a llevar a cabo una acción que afecte su patrimonio. Por el contrario, la apropiación fraudulenta, contemplada en el artículo 187 del Código Orgánico Integral Penal (COIP), se enfoca en el aprovechamiento indebido de la confianza para adueñarse de bienes que han sido confiados al autor en el marco de una relación de fideicomiso (Código Orgánico Integral Penal, COIP, 2021).

Ambos delitos comparten la característica de exigir la presencia de un daño económico para la víctima y de un beneficio ilegítimo para el perpetrador. En la configuración tanto de la estafa como de la apropiación fraudulenta, la intención delictiva del autor juega un papel fundamental. En Ecuador, la jurisprudencia ha resaltado la importancia de demostrar la intención de causar daño patrimonial y el beneficio obtenido a través de prácticas ilícitas en ambos escenarios. Esto conlleva a la necesidad de realizar una prueba rigurosa del elemento subjetivo del dolo.

Una diferencia fundamental entre estos delitos reside en la manera en que se lleva a cabo el acto de engaño o abuso. En el contexto de un acto fraudulento, el autor recurre a artimañas o engaños con el propósito de distorsionar la verdad, induciendo a la víctima a desprenderse de sus bienes de forma voluntaria pero equivocada. En el caso de la apropiación fraudulenta, el individuo adquiere inicialmente los activos de forma legal, para posteriormente traicionar la confianza otorgada al apropiarse de manera indebida de los mismos. El abuso de confianza se destaca como el factor característico de la apropiación fraudulenta (Ortiz & López, 2024).

En la doctrina jurídica se destaca que la relación previa entre el autor del delito y la víctima constituye otro aspecto distintivo. En el caso de una estafa, es posible que no haya existido una relación previa entre las partes involucradas. El contacto entre ellas puede ser breve pero esencial para llevar a cabo el acto de engaño. Por el contrario, el delito de apropiación indebida siempre conlleva una relación de confianza previamente establecida, tal como la que surge de

un contrato de depósito, administración o custodia. La relación fiduciaria es esencial para la comisión del delito de apropiación fraudulenta.

En relación con las sanciones, tanto las dos infracciones pueden resultar en penalizaciones severas, sin embargo, la jurisprudencia ha demostrado que las circunstancias agravantes pueden ser diversas. En el delito de estafa, la utilización de tecnologías de la información puede ser un agravante que resulte en un aumento de la condena. En el delito de apropiación fraudulenta, la cantidad de los activos sustraídos y la utilización abusiva de una posición de confianza suelen constituir elementos agravantes (Chuco, 2023). La adecuación de las sanciones se determina en función de la magnitud del daño económico causado y del grado de intencionalidad probado.

En el campo tecnológico, ambos delitos han experimentado cambios para adecuarse a las nuevas manifestaciones de la delincuencia. La adaptación de la legislación y la interpretación judicial ha sido evidente en la lucha contra la estafa digital y la apropiación fraudulenta de activos electrónicos, dos ejemplos representativos de los desafíos contemporáneos a los que se enfrenta el sistema legal. La doctrina ecuatoriana reconoce la importancia de mantener actualizadas las leyes para abarcar las nuevas formas de delitos, asegurando de esta manera una protección eficaz del patrimonio en el entorno de la sociedad digital contemporánea.

1.2.Importancia del estudio de los delitos en redes sociales

1.2.1. Impacto en la sociedad moderna

El impacto de los delitos de estafa y apropiación fraudulenta en la sociedad contemporánea es significativo y complejo, repercutiendo en tanto en personas individuales como en organizaciones empresariales. En Ecuador, la expansión de estas actividades ilícitas ha suscitado una creciente inquietud en relación con la estabilidad económica y la integridad del sistema financiero. Las acciones delictivas de estafa y apropiación fraudulenta, contempladas en los artículos 186 y 187 del Código Orgánico Integral Penal (COIP) respectivamente, constituyen riesgos relevantes para la credibilidad en las transacciones comerciales y las relaciones de confianza en la sociedad (Código Orgánico Integral Penal, COIP, 2021).

Las personas afectadas por estos crímenes enfrentan frecuentemente serias repercusiones económicas y emocionales a nivel personal. La apropiación fraudulenta o estafa puede ocasionar la pérdida de patrimonio, lo que a su vez puede provocar un menoscabo en la calidad de vida y la estabilidad económica. En Ecuador, la jurisprudencia ha destacado la importancia de imponer castigos severos a fin de desalentar la realización de dichos actos y garantizar la

protección de la ciudadanía. La importancia de la reparación integral del daño causado a las víctimas es destacada por la doctrina jurídica, la cual promueve la restitución y compensación adecuadas.

Las empresas a nivel corporativo también se ven expuestas a riesgos significativos a causa de estos actos delictivos. La apropiación fraudulenta puede minar la confianza en los sistemas de gestión y control interno, en particular. Es necesario que las entidades financieras y comerciales realicen inversiones en medidas de seguridad y auditoría con el fin de evitar la comisión de fraudes internos. En Ecuador, la doctrina académica sugiere reforzar los mecanismos de control y supervisión con el fin de reducir los riesgos vinculados a la malversación de fondos y asegurar la transparencia y la confianza en las actividades comerciales (Roque, 2021).

Otro aspecto relevante es el impacto en la percepción de la seguridad digital. El incremento de las transacciones en línea y la utilización de tecnologías de la información han dado lugar a nuevas modalidades digitales de delitos como la estafa y la apropiación fraudulenta. Esta situación ha generado un aumento en el temor y la desconfianza entre los usuarios de la red. La legislación en Ecuador está en proceso de ajustarse a estas nuevas formas, sin embargo, los avances tecnológicos rápidos presentan desafíos continuos. La doctrina enfatiza la importancia de modificar y reforzar la legislación vigente para enfrentar de manera efectiva los crímenes cibernéticos.

Los delitos mencionados tienen un impacto negativo en la cohesión social y en la confianza que la sociedad deposita en las instituciones tanto públicas como privadas. La percepción de impunidad y la falta de eficacia del sistema judicial en la resolución de estos casos pueden minar la confianza en la justicia y en el estado de derecho. En Ecuador, la jurisprudencia destaca la relevancia de una pronta y eficaz respuesta judicial. Esta no solo debe imponer sanciones a los culpables, sino también restaurar la fe de la sociedad en las entidades responsables de salvaguardar el patrimonio y la certeza jurídica (Tirado, 2020).

En un mundo cada vez más interconectado, los delitos de estafa y apropiación fraudulenta tienen implicaciones globales significativas en el contexto internacional. La efectiva lucha contra los delitos cibernéticos requiere de la colaboración internacional y el cumplimiento de acuerdos internacionales sobre cibercrimen. Al ser parte de acuerdos internacionales, Ecuador debe continuar fortaleciendo su marco legal y sus capacidades operativas para colaborar en la

prevención y persecución de delitos transnacionales. Esto asegurará una protección integral para sus ciudadanos en un contexto globalizado.

1.2.2. Evolución de los delitos con el avance tecnológico

El progreso tecnológico ha provocado cambios significativos en la naturaleza de los delitos, como la estafa y la apropiación fraudulenta, tanto en su comisión como en su persecución. En el contexto ecuatoriano, se ha requerido que la normativa legal se ajuste para hacer frente a las nuevas formas de delitos que emergen en el ámbito digital. El Código Orgánico Integral Penal (COIP) establece penalizaciones para los delitos informáticos y fraudes cibernéticos, reconociendo la importancia de contar con un marco legal que se ajuste a las particularidades de dichas conductas delictivas. La tecnología ha incrementado la complejidad y extensión de los actos delictivos, lo cual demanda una revisión continua de las normativas legales y procedimientos judiciales.

El uso de internet y las redes sociales ha tenido un profundo impacto en la estafa, la cual está regulada por el artículo 186 del Código Orgánico Integral Penal (COIP). En la actualidad, los criminales emplean estrategias como el envío de correos electrónicos fraudulentos, la creación de sitios web falsos y perfiles engañosos en redes sociales con el propósito de estafar a sus víctimas y obtener ganancias económicas. En sus interpretaciones legales, la jurisprudencia ecuatoriana ha empezado a considerar las nuevas modalidades de estafa, reconociendo la diversidad de formas en que el engaño puede manifestarse en el entorno digital. Este enfoque posibilita una implementación más eficaz de las leyes penales en situaciones de fraude cibernético (Matos, 2021).

La evolución tecnológica también ha impactado en la modalidad delictiva de la apropiación fraudulenta, tipificada en el artículo 187 del Código Orgánico Integral Penal. En la actualidad, los criminales tienen la capacidad de intervenir en sistemas informáticos con el fin de obtener acceso a información confidencial y así adquirir ilegalmente propiedades o activos. La importancia de comprender las técnicas y herramientas tecnológicas utilizadas en estos delitos es resaltada por la doctrina jurídica, con el fin de prevenirlos y perseguirlos de manera adecuada (Tacuri, 2021). Los tribunales en Ecuador se han visto en la necesidad de ajustarse a estas nuevas circunstancias, elaborando criterios y procedimientos para evaluar pruebas digitales e identificar pautas de conducta delictiva en el ámbito virtual.

El progreso tecnológico ha contribuido a la realización de delitos a gran escala, los cuales traspasan fronteras y dificultan la labor de las autoridades judiciales en su persecución. La colaboración a nivel internacional resulta fundamental para abordar los retos derivados del cibercrimen. Ecuador ha suscrito múltiples convenios y acuerdos a nivel internacional que promueven la colaboración recíproca y la entrega de personas acusadas de cometer delitos informáticos. La importancia de estos instrumentos para asegurar una respuesta eficaz y coordinada frente a la criminalidad transnacional, protegiendo a las víctimas y garantizando la justicia, es resaltada por la jurisprudencia y la doctrina jurídica.

La respuesta del sistema judicial a estas transformaciones ha implicado la capacitación y especialización de los profesionales del derecho en el ámbito de los delitos informáticos. La formación en metodologías de investigación digital y la utilización de herramientas tecnológicas para recopilar y analizar pruebas son esenciales para abordar los desafíos actuales de la delincuencia cibernética. La doctrina jurídica defiende la importancia de la formación continua y la actualización de conocimientos para jueces, fiscales y personal de investigación (Gutiérrez, García, Alcívar, & Chancay, 2023). Esto se considera fundamental para asegurar la eficacia y eficiencia en la investigación y persecución de delitos.

La importancia de la prevención y la sensibilización pública se ha destacado con el avance tecnológico en la evolución de los delitos. La importancia de las campañas educativas sobre seguridad digital y el uso responsable de las tecnologías de la información radica en su papel fundamental para disminuir la exposición de los individuos a los delitos cibernéticos. La implementación de políticas públicas que fomenten una cultura de prevención y protección en el ámbito digital es promovida por la legislación ecuatoriana, en conjunto con la jurisprudencia y la doctrina jurídica. Esto tiene como objetivo garantizar un entorno más seguro y confiable para todos los ciudadanos.

1.2.3. Relevancia jurídica y social

En la sociedad ecuatoriana contemporánea, la importancia legal y social de los delitos de estafa y apropiación fraudulenta es innegable debido a su frecuencia y las repercusiones que provocan en diferentes esferas. Los delitos mencionados se encuentran definidos en el Código Orgánico Integral Penal (COIP), específicamente en los artículos 186 y 187, con el propósito de resguardar el patrimonio y fomentar la confianza en las interacciones económicas y sociales (Código Orgánico Integral Penal, COIP, 2021). Es esencial tipificar y sancionar

adecuadamente estos crímenes con el fin de preservar la integridad del sistema legal y garantizar la justicia para las personas afectadas.

La estafa y la apropiación fraudulenta tienen un efecto negativo en la confianza pública y la cohesión social, desde un punto de vista social. Las personas afectadas por estas transgresiones experimentan no solo consecuencias financieras, sino también un impacto emocional de gran magnitud. La falta de confianza en las transacciones comerciales y la percepción de inseguridad pueden provocar una reducción en la actividad económica y tener un impacto en la estabilidad social (Carvajas & Estrada, 2020). La importancia de una respuesta judicial efectiva para restituir la confianza pública y garantizar la protección de los derechos patrimoniales de los ciudadanos es subrayada por la doctrina jurídica.

En Ecuador, la jurisprudencia ha establecido criterios precisos para detectar y castigar estos crímenes, destacando la importancia de demostrar el acto de engaño o la violación de la confianza, así como el daño económico ocasionado. La importancia de estas interpretaciones reside en su habilidad para ajustarse a las nuevas formas de delincuencia, en particular aquellas que son facilitadas por el progreso tecnológico. La vitalidad en la interpretación judicial resulta fundamental para abordar de manera efectiva las nuevas manifestaciones de delincuencia y salvaguardar a los afectados en un entorno digital cada vez más sofisticado.

La importancia legal de estos crímenes se evidencia en la imperativa colaboración internacional requerida para su enjuiciamiento. Los tratados y acuerdos internacionales firmados por Ecuador, como la Convención de Budapest sobre Ciberdelincuencia, son instrumentos fundamentales en la lucha contra el fraude y la apropiación indebida en un entorno globalizado. La importancia de estos instrumentos para fortalecer la capacidad del sistema judicial ecuatoriano en la lucha contra el cibercrimen es destacada por la doctrina jurídica (Cabrera & Jiménez, 2021). Esto promueve una justicia más efectiva y coordinada a nivel internacional.

Otro aspecto fundamental de la relevancia social de estos delitos es la implementación de políticas públicas dirigidas a la prevención y educación. La reducción de la vulnerabilidad de la población ante estafas y apropiaciones fraudulentas es un objetivo fundamental que se logra a través de campañas de sensibilización y formación en seguridad digital. La legislación en Ecuador, respaldada por la doctrina jurídica, fomenta la implementación de acciones preventivas que incluyan la participación de múltiples actores sociales, tales como instituciones

educativas, empresas y entidades gubernamentales, con el fin de establecer un entorno más seguro y capaz de recuperarse ante adversidades (Espinoza, 2021).

En Ecuador, la relevancia jurídica y social de los delitos de estafa y apropiación fraudulenta es amplia y abarca diversos aspectos. Entre ellos se encuentra la protección del patrimonio, la restauración de la confianza pública y la adaptación a las nuevas realidades tecnológicas y globales. En tanto, estos delitos tienen implicaciones significativas en el ámbito legal y social del país. La implementación de políticas preventivas, la cooperación internacional y la evolución constante de la jurisprudencia y la doctrina jurídica son elementos fundamentales para abordar los desafíos mencionados y garantizar la efectividad del sistema judicial, así como promover una sociedad más segura y confiable.

1.3.Fundamentos teóricos

1.3.1. Teorías del comportamiento delictivo en el entorno digital.

Las teorías sobre el comportamiento delictivo en el ámbito digital tienen como objetivo analizar las razones y procesos que impulsan a las personas a cometer actos delictivos en el entorno virtual. En Ecuador, la legislación, representada por el Código Orgánico Integral Penal (COIP), ha experimentado modificaciones para abordar los retos actuales. Se han incluido enmiendas para definir y penalizar los delitos informáticos, así como para establecer consecuencias concretas para acciones como la estafa y la apropiación fraudulenta en el ámbito digital. La doctrina jurídica destaca la importancia de comprender dichas conductas con el fin de elaborar estrategias preventivas y de persecución que sean efectivas.

Una de las teorías más relevantes en el ámbito de la criminología es la teoría de la oportunidad. Esta teoría postula que los delitos cibernéticos se llevan a cabo en situaciones donde existen múltiples oportunidades para cometerlos y la probabilidad de ser descubierto es reducida. En el ámbito digital, la falta de identificación y la accesibilidad a las tecnologías de la información favorecen la perpetración de dichos delitos. En Ecuador, la jurisprudencia ha establecido que la ausencia de medidas de seguridad apropiadas en los entornos digitales puede incrementar de manera considerable la probabilidad de fraudes y apropiaciones indebidas (Di Angellis, 2021).

Otra teoría relevante es la teoría del aprendizaje social, la cual sostiene que los comportamientos delictivos son adquiridos mediante la interacción con individuos del entorno. En el ámbito virtual, los criminales tienen la capacidad de compartir información y habilidades mediante foros, redes sociales y otros canales digitales. La doctrina jurídica ecuatoriana resalta

la necesidad de una respuesta legal y educativa frente a la difusión de información delictiva en línea, con el objetivo de contrarrestar la influencia de estos entornos negativos y fomentar comportamientos seguros y éticos en el uso de la tecnología (Parra, Menjura, Pulgarín, & Gutiérrez, 2021).

La teoría de la neutralización es una perspectiva adicional que contribuye a la comprensión de la conducta delictiva en el contexto digital. Según esta teoría, los individuos que cometen actos delictivos recurren a racionalizaciones para justificar sus acciones, las cuales les permiten mitigar el sentimiento de culpa o responsabilidad. En el ámbito de los delitos informáticos, los responsables pueden reducir la magnitud del perjuicio percibido o persuadirse de que sus acciones no ocasionan daño directo a terceros (Macías, 2024). En el contexto legal de Ecuador, se han presentado dificultades para probar la existencia de dolo en determinadas situaciones, lo cual resalta la relevancia de contar con pruebas sólidas y concluyentes que demuestren la intencionalidad delictiva.

La teoría de la rutina de actividades ofrece una perspectiva significativa en relación a los delitos en el ámbito digital. Según esta teoría, la comisión de un delito se produce cuando coinciden tres factores: la presencia de un individuo con intenciones delictivas, la disponibilidad de una víctima vulnerable y la falta de agentes de seguridad capaces de evitar la perpetración del delito. En el ámbito virtual, las acciones habituales de los usuarios, como las transacciones financieras y la interacción en redes sociales, los exponen a posibles riesgos por parte de individuos malintencionados que buscan aprovecharse de ellos mediante estafas o fraudes (Cañas, 2021). En el contexto jurídico ecuatoriano, se destaca la importancia de reforzar las medidas de protección y vigilancia en el entorno digital con el fin de prevenir la comisión de delitos en este ámbito.

La teoría de la elección racional sostiene que los criminales digitales realizan decisiones considerando los beneficios y costos, evaluando las posibles ventajas frente a los riesgos de ser detenidos y penalizados. El aumento de la dificultad y el riesgo asociados con la comisión de delitos informáticos se plantea como un factor disuasorio para posibles infractores (Delgadillo, Avalos, & Ávila, 2022). La jurisprudencia ecuatoriana y la legislación actual del Código Orgánico Integral Penal (COIP) tienen como objetivo aumentar los riesgos asociados a los delitos cibernéticos a través de la imposición de sanciones más estrictas y la adopción de tecnologías avanzadas para la identificación y enjuiciamiento de estos delitos. Esto tiene como propósito fomentar un entorno digital que sea más seguro y confiable.

1.3.2. Modelos explicativos del fraude en línea

Los modelos explicativos del fraude en línea son fundamentales para comprender las dinámicas subyacentes a estos delitos, así como para la elaboración de estrategias eficaces destinadas a su prevención y control. Uno de los modelos más empleados en este contexto es el Modelo de la Oportunidad, el cual postula que la comisión de fraude en línea se ve facilitada por la presencia de oportunidades abundantes para llevar a cabo el delito, combinado con un bajo riesgo de ser detectado (Gil, 2020). La aplicación de este modelo abarca una variedad de formas de fraude digital, que van desde el phishing hasta la apropiación fraudulenta. Destaca la relevancia de reforzar las medidas de seguridad en las plataformas digitales con el fin de disminuir las posibilidades de cometer delitos.

Otro enfoque relevante es el Modelo del Triángulo del Fraude, el cual fue desarrollado por Donald Cressey. Este modelo identifica tres factores fundamentales que contribuyen a la comisión de actos fraudulentos: presión, oportunidad y racionalización. En el ámbito del fraude en línea, la presión puede surgir de la necesidad económica o la avaricia, la oportunidad se manifiesta a través de fallos en los sistemas de seguridad, y la racionalización permite al perpetrador justificar sus acciones (Chacón, 2021). Este modelo contribuye a la identificación de puntos críticos en los cuales las intervenciones podrían resultar más efectivas en la prevención del fraude.

El Modelo de la Teoría de la Actividad Rutina también proporciona una perspectiva significativa. De acuerdo con esta teoría, el fraude en línea se produce en el momento en que coinciden un delincuente con motivación, una víctima vulnerable y la carencia de mecanismos de protección eficaces que puedan evitar la comisión del delito. En el contexto digital, las acciones habituales de los usuarios, tales como las transacciones financieras y la interacción en redes sociales, los exponen a posibles riesgos de seguridad (Delgadillo, Avalos, & Ávila, 2022). Este modelo destaca la importancia de establecer medidas de vigilancia y protección que puedan funcionar como salvaguardas digitales para disuadir a los infractores.

El Modelo de la Neutralización es una teoría que proporciona una explicación sobre la forma en que los individuos que cometen actos delictivos justifican sus acciones fraudulentas. De acuerdo con esta teoría, los individuos que cometen fraude en línea recurren a técnicas de neutralización, tales como la minimización del daño, la atribución de culpa a la víctima o la negación de responsabilidad, con el fin de racionalizar su conducta delictiva (Salazar & ortíz,

2024). Este modelo resulta ser una herramienta valiosa para analizar las motivaciones psicológicas que subyacen al fraude. Resalta la relevancia de llevar a cabo campañas educativas que desarticulen dichas justificaciones y fomenten conductas éticas en el ámbito del uso de la tecnología.

La Teoría de la Elección Racional sostiene que los individuos que cometen fraudes en línea realizan una evaluación de costos y beneficios, considerando las posibles ganancias en contraposición a los riesgos de detección y castigo. Este modelo propone que la elevación de las sanciones y el perfeccionamiento de los métodos de detección pueden actuar como elementos disuasorios para individuos propensos a cometer actos delictivos (Garzón, Urrego, & Ocampo, 2023).

El Modelo de Influencia Social analiza el impacto de las interacciones y normas sociales en el comportamiento delictivo en el entorno virtual. A través de sus conexiones sociales y comunidades en línea, los individuos que cometen actos delictivos pueden adquirir habilidades fraudulentas y adoptar actitudes permisivas hacia el fraude (Chaverra & Celis, 2022). En este modelo se resalta la relevancia de intervenir en dichos entornos sociales y emplear campañas de concienciación y educación con el fin de modificar las normativas y actitudes hacia el fraude digital. La combinación de estos modelos ofrece una comprensión completa del fraude en línea y orienta la elaboración de políticas y estrategias de prevención eficaces.

1.4.Redes sociales como plataforma para delitos

1.4.1. Evolución y Popularidad de las Redes Sociales

La evolución de las redes sociales ha sido rápida desde su surgimiento, pasando de ser plataformas simples de interacción social a estructuras complejas de comunicación y comercio. En un principio, plataformas como Facebook y Twitter se originaron con el propósito de facilitar la interacción entre individuos y la difusión de información. No obstante, con su expansión y sofisticación, estas plataformas han captado el interés de individuos delictivos que buscan aprovechar sus atributos para llevar a cabo actividades ilegales (Guijarro, Casado, & Mayorga, 2021). La proliferación de las redes sociales ha dado lugar a un nuevo escenario propicio para la comisión de una variedad de delitos, tales como estafas, usurpaciones de identidad y otros tipos de fraudes digitales.

La popularidad de las redes sociales ha experimentado un crecimiento exponencial, llegando a abarcar a miles de millones de usuarios a nivel global. El aumento mencionado se ha visto

favorecido por la facilidad de acceso y la incorporación de dichas plataformas en la rutina diaria de la población. Con la ampliación de su alcance, las redes sociales han adquirido interés para individuos delictivos, los cuales emplean estrategias avanzadas con el propósito de engañar a los usuarios y obtener datos personales o financieros con el fin de llevar a cabo acciones fraudulentas. La falta de familiaridad con las medidas de seguridad digital por parte de numerosos usuarios contribuye a la vulnerabilidad ante posibles ataques perpetrados por individuos malintencionados.

La legislación ecuatoriana, según lo establecido en el Código Orgánico Integral Penal (COIP), ha debido ajustarse desde un enfoque jurídico para hacer frente a los retos derivados de los delitos perpetrados en plataformas de redes sociales. En Ecuador, la jurisprudencia ha reconocido la importancia de la actualización continua de la legislación para abordar las nuevas formas de delitos que emergen a raíz del progreso tecnológico. Las redes sociales representan un desafío importante para las autoridades encargadas de hacer cumplir la ley, debido a su capacidad de difundir información de manera rápida y a su alcance global (Layton, 2020).

Las redes sociales proporcionan un entorno propicio para el ocultamiento de la identidad y la falsificación de la misma, dos elementos que favorecen la perpetración de actos delictivos. Los criminales tienen la capacidad de generar identidades ficticias y emplear estrategias de manipulación psicológica con el fin de estafar a las personas afectadas. La falta de revelación de la identidad de los individuos dificulta el proceso de identificación y enjuiciamiento de los culpables, lo cual subraya la importancia de la colaboración a nivel internacional y el avance en tecnologías especializadas para la detección y prevención de actividades delictivas en el ciberespacio (Sanjuán, 2020). La importancia de la colaboración entre diferentes jurisdicciones para abordar eficazmente estos desafíos es enfatizada por la doctrina jurídica.

La evolución tecnológica de las redes sociales ha propiciado la emergencia de nuevas modalidades de fraude, tales como el phishing, el spoofing y otros tipos de ataques cibernéticos. Los métodos mencionados emplean las plataformas de redes sociales como medio para difundir enlaces perjudiciales y obtener información personal de forma engañosa. En Ecuador, tanto la legislación como la jurisprudencia han iniciado la atención de estas problemáticas mediante la aplicación de sanciones rigurosas y la creación de marcos legales orientados a la protección de los usuarios. Sin embargo, la veloz evolución de la tecnología requiere una actualización y adaptación continua de las estrategias legales.

1.4.2. Historia y desarrollo de las redes sociales.

La historia y desarrollo de las redes sociales se remonta a la década de 1990 con el surgimiento de los primeros sitios web que permitían la creación de perfiles y la conexión entre usuarios. Uno de los pioneros fue Six Degrees, lanzado en 1997, que permitía a los usuarios crear perfiles, listas de amigos y navegar por la red de conexiones. Aunque su popularidad fue limitada, sentó las bases para futuras plataformas más sofisticadas (Cárdenas, Rosero, Holovatyi, & Pazos, 2020). Este período inicial marcó el comienzo de la transición de internet hacia una herramienta de comunicación social.

En la década de 2000, la evolución de las redes sociales se aceleró con la aparición de sitios como Friendster, MySpace y LinkedIn. Friendster, lanzado en 2002, fue una de las primeras redes en alcanzar una masa crítica de usuarios, aunque eventualmente fue superada por MySpace, que se convirtió en la plataforma dominante. LinkedIn, también lanzada en 2002, se enfocó en la creación de redes profesionales, estableciendo un nicho importante en el mundo corporativo (Gozáles & Cortijo, 2023). Estas plataformas demostraron el potencial de las redes sociales para transformar las interacciones personales y profesionales.

El verdadero punto de inflexión llegó con el lanzamiento de Facebook en 2004 y Twitter en 2006. Facebook, creado por Mark Zuckerberg, se expandió rápidamente desde un proyecto universitario a una red global, redefiniendo la forma en que las personas se conectan y comparten información. Twitter, con su formato de microblogging, introdujo una nueva dinámica de comunicación rápida y concisa, popularizando el concepto de "tweets". Ambas plataformas no solo crecieron exponencialmente en usuarios, sino que también empezaron a influir en la cultura, la política y la economía global (Bravo & Ordóñez, 2021).

A lo largo de la década de 2010, las redes sociales continuaron diversificándose y especializándose. Instagram, lanzado en 2010, se centró en la compartición de fotos y videos, atrayendo a una audiencia joven y visualmente orientada. Snapchat, también lanzado en 2011, introdujo el concepto de mensajes efímeros, que desaparecen después de ser vistos, ofreciendo una nueva forma de comunicación más informal y temporaria (Lardies & Potes, 2022). Estas innovaciones demostraron cómo las redes sociales podían adaptarse a las preferencias cambiantes de los usuarios y continuar creciendo en popularidad.

El desarrollo de las redes sociales no ha estado exento de desafíos y controversias. La privacidad y la seguridad de los datos de los usuarios se han convertido en temas críticos,

especialmente tras incidentes como el escándalo de Cambridge Analytica en 2018, donde se reveló el uso indebido de datos personales de millones de usuarios de Facebook. La legislación en varios países, incluyendo Ecuador, ha comenzado a abordar estos problemas mediante la implementación de regulaciones más estrictas sobre la protección de datos personales y la transparencia en el uso de la información por parte de las plataformas (Fernández & García, 2020).

En la actualidad, las redes sociales continúan evolucionando, integrando nuevas tecnologías como la inteligencia artificial y la realidad aumentada para mejorar la experiencia del usuario. Plataformas como TikTok, lanzada en 2016, han introducido nuevas formas de contenido interactivo y viral, capturando la atención de una audiencia global joven. La historia de las redes sociales es una historia de innovación constante y adaptación, reflejando las cambiantes dinámicas sociales y tecnológicas. En el futuro, estas plataformas seguirán desempeñando un papel central en la comunicación y la interacción humana, mientras enfrentan desafíos continuos en términos de regulación, privacidad y seguridad.

1.4.3. Estadísticas de uso global y regional

En la última década, la popularidad de las redes sociales ha experimentado un crecimiento exponencial, convirtiéndose en un elemento fundamental en la rutina diaria de millones de individuos a nivel global. A nivel mundial, plataformas como Facebook, Instagram, Twitter y TikTok han logrado cifras significativas de usuarios activos, lo que demuestra su alcance e importancia en diferentes culturas y regiones. Estas plataformas desempeñan un papel fundamental no solo en la comunicación y el entretenimiento, sino también en el comercio, la educación y la difusión de información (Ruiz, gonzáles, & Lucendo, 2020).

En Ecuador, se ha observado un notable aumento en la utilización de redes sociales. La proliferación de dispositivos móviles y la accesibilidad a internet han permitido que una gran parte de la población ecuatoriana participe de forma activa en estas plataformas. En Ecuador, las redes sociales se emplean no solo con el propósito de mantener comunicación con amigos y familiares, sino también para llevar a cabo actividades de índole comercial, educativa y social. El impacto de dichas plataformas en la dinámica social y económica del país es incuestionable.

Se exhibe una tabla que muestra las estadísticas de utilización de las principales redes sociales a nivel global y regional, específicamente en Ecuador. Esta tabla permite visualizar el alcance y la popularidad de dichas plataformas tanto a escala mundial como en el contexto ecuatoriano.

Tabla 1. *Estadísticas de utilización de redes sociales*

Plataforma	Usuarios Activos Globales (millones)	Usuarios Activos en Ecuador (millones)
Facebook	2900	13.5
Instagram	2000	6.2
Twitter	450	2.1
TikTok	1000	3.8
LinkedIn	850	1.5
Snapchat	500	2.0
WhatsApp	2000	12.0
YouTube	2200	11.0

Nota: Elaboración propia basado en (Dean, 2024; Kemp, 2024)

1.5.Características de las redes sociales que facilitan delitos

1.5.1. Anonimato y falsificación de identidad

La comunicación ha sido transformada por las redes sociales, sin embargo, también han facilitado la perpetración de delitos debido a atributos particulares como el anonimato y la habilidad para falsificar identidades. El anonimato posibilita a los usuarios ocultar su identidad real, lo cual complica la tarea de rastrearlos y hacerlos responsables. Esta característica es aprovechada por individuos delictivos que cometen actos fraudulentos, extorsiones y acoso, mediante la creación de perfiles falsos con el propósito de engañar a otros usuarios (Mantilla, 2023). La proliferación de identidades falsas se ve favorecida por la falta de verificación rigurosa en el proceso de creación de cuentas, lo que a su vez contribuye a este problema al no existir una supervisión efectiva.

En Ecuador, la jurisprudencia ha iniciado el abordaje de los desafíos relacionados con la actualización de las leyes para combatir los delitos cibernéticos. De acuerdo con lo establecido en el Código Orgánico Integral Penal (COIP), la utilización de identidades ficticias en plataformas digitales puede ser considerada como un factor agravante en situaciones de fraude y otras infracciones relacionadas con la informática. La importancia de la transparencia y la

responsabilidad en las plataformas digitales para prevenir abusos es resaltada por la doctrina jurídica. No obstante, persiste como un desafío considerable la puesta en marcha de mecanismos eficaces para verificar identidades.

El uso del anonimato en plataformas de redes sociales puede propiciar la perpetración de conductas delictivas como el acoso y ciberacoso, permitiendo a los agresores hostigar a sus víctimas sin el riesgo de ser reconocidos. Esta situación genera un ambiente de impunidad que intensifica el impacto psicológico y emocional en las personas afectadas. Aunque han experimentado mejoras en los últimos años, las políticas de las plataformas sociales aún encuentran obstáculos para supervisar y castigar de manera efectiva dichas conductas (Panero, 2021). La protección de las víctimas en Ecuador ha experimentado avances significativos en su marco legal. Sin embargo, es necesario mantener una actualización constante y una adaptación continua de las leyes debido a la rápida evolución tecnológica.

La suplantación de identidad en plataformas digitales impacta no solo a personas particulares, sino también a organizaciones y personalidades públicas. Los perfiles falsos tienen la capacidad de difundir información inexacta, usurpar identidades y llevar a cabo actividades fraudulentas, como estafas financieras. Las actividades delictivas de este tipo no solamente causan daño a las personas afectadas directamente, sino que también minan la confianza en los servicios en línea (Galindo, 2024). Los actos mencionados han sido objeto de severas sanciones por parte de la jurisprudencia ecuatoriana, la cual ha destacado el perjuicio considerable que pueden ocasionar en la reputación y estabilidad económica de las personas afectadas.

La capacidad de crear y gestionar varias identidades falsas dificulta la labor de las autoridades en la investigación y prevención de delitos. La colaboración entre las plataformas de redes sociales y las autoridades de seguridad es fundamental para la detección y desarticulación de organizaciones criminales que operan de manera encubierta. La cooperación internacional desempeña un papel fundamental, ya que los criminales pueden llevar a cabo sus actividades delictivas desde diversas jurisdicciones. La doctrina jurídica destaca la importancia de reforzar los mecanismos de cooperación con el fin de enfrentar de manera efectiva los delitos cibernéticos.

1.5.2. Alcance y viralidad de la información.

El alcance y la viralidad de la información son características fundamentales de las redes sociales que facilitan la comisión de delitos. Las plataformas como Facebook, Twitter, e

Instagram permiten la difusión rápida y masiva de contenido, lo que puede ser explotado por delincuentes para propagar información falsa, realizar estafas y coordinar actividades delictivas (Contreras & Marín, 2022). La capacidad de llegar a millones de usuarios en cuestión de segundos amplifica el impacto de estos delitos, haciendo más difícil su control y mitigación por parte de las autoridades.

La viralidad de la información en redes sociales se debe en parte a los algoritmos que priorizan contenido atractivo y que genera interacción. Estos algoritmos pueden, inadvertidamente, favorecer la difusión de información falsa o engañosa que sirve como base para fraudes o manipulaciones. Según la jurisprudencia ecuatoriana, la difusión de noticias falsas y la manipulación de información para cometer delitos están penadas bajo el Código Orgánico Integral Penal (COIP). La legislación busca así mitigar los efectos negativos de la viralidad, aunque la implementación efectiva de estas normas sigue siendo un reto.

El alcance de las redes sociales también permite a los delincuentes coordinar operaciones en tiempo real, facilitando delitos como la suplantación de identidad y la estafa. La capacidad de comunicarse y organizarse rápidamente entre grandes grupos de personas puede convertir las redes sociales en herramientas para la planificación y ejecución de delitos complejos. La doctrina jurídica ecuatoriana enfatiza la necesidad de monitorear y regular estas actividades para prevenir el uso indebido de estas plataformas.

Además, la viralidad puede ser utilizada para la difusión de software malicioso y enlaces fraudulentos. Los ciberdelincuentes aprovechan la tendencia de los usuarios a compartir enlaces y archivos sin verificar su origen, lo que facilita la propagación de virus y el acceso no autorizado a información personal. La jurisprudencia ha reconocido la creciente incidencia de estos delitos y ha buscado fortalecer las medidas de seguridad digital, aunque la educación del usuario sigue siendo crucial para reducir estos riesgos (Salgado, 2022).

Otro aspecto crítico es la capacidad de las redes sociales para influir en la opinión pública y manipular percepciones mediante campañas coordinadas de desinformación. Estas campañas pueden tener fines delictivos, como el fraude electoral o la extorsión. La legislación ecuatoriana, a través del COIP, penaliza la difusión de información falsa con intenciones delictivas, pero la detección y prueba de estos delitos son complejas debido a la naturaleza dinámica y global de las redes sociales.

1.5.3. Vulnerabilidades en la seguridad de las plataformas.

Las vulnerabilidades en la seguridad de las plataformas de redes sociales representan un desafío significativo en la protección de la información personal y la prevención de delitos cibernéticos. Las vulnerabilidades pueden originarse por deficiencias en el diseño del software, configuraciones inadecuadas o la ausencia de actualizaciones de seguridad. Las vulnerabilidades de seguridad posibilitan a los agresores el acceso a información confidencial, la suplantación de identidades y la realización de acciones fraudulentas, impactando tanto a personas como a entidades. La aplicación de las leyes en Ecuador, específicamente en el ámbito penal según lo establecido en el Código Orgánico Integral Penal (COIP), se ve influenciada por la jurisprudencia nacional. Sin embargo, la constante evolución de la tecnología dificulta la efectividad en la aplicación de dichas normativas.

Las vulnerabilidades comunes que los delincuentes explotan para acceder a cuentas y datos personales incluyen la falta de cifrado robusto y el uso de contraseñas débiles. Las plataformas que no cuentan con un cifrado adecuado tanto para la transmisión como para el almacenamiento de datos son especialmente vulnerables a posibles ataques de interceptación y acceso no autorizado. La importancia de las medidas de seguridad preventiva, como la autenticación de dos factores y la educación de los usuarios sobre la creación de contraseñas seguras, es resaltada por la doctrina jurídica para mitigar los riesgos (Fernández, 2020).

Una vulnerabilidad adicional de importancia radica en la explotación de fallos de software que no han sido corregidos mediante parches de seguridad. Con frecuencia, los agresores buscan fallas en el código de las plataformas con el fin de insertar software malicioso o llevar a cabo ataques de denegación de servicio (DDoS). En Ecuador, la jurisprudencia ha tomado en consideración la seriedad de dichos ataques, y ha determinado medidas punitivas para aquellos individuos que se dedican a su explotación (García & Pesantez, 2023). No obstante, las empresas de redes sociales también tienen la responsabilidad de mantener actualizados y seguros sus sistemas, aplicando de manera oportuna parches de seguridad.

La ingeniería social es una técnica que se vale de las debilidades humanas con el fin de obtener información confidencial. Los métodos comunes incluyen los ataques de phishing y la creación de perfiles falsos con el propósito de engañar a los usuarios. La importancia de llevar a cabo campañas de sensibilización y educación es resaltada por la doctrina jurídica, con el fin de que los usuarios puedan identificar y prevenir caer en dichas estratagemas. Es necesario que las plataformas de redes sociales mejoren sus sistemas de identificación y eliminación de contenido fraudulento y perjudicial.

Las aplicaciones de terceros que se incorporan en las plataformas de redes sociales conllevan riesgos de importancia. Frecuentemente, estas aplicaciones requieren permisos amplios que podrían ser empleados para la recolección inapropiada de información personal. La falta de una supervisión estricta por parte de las plataformas líderes facilita la comisión de estos abusos. En Ecuador, la jurisprudencia ha iniciado un proceso de análisis para implementar regulaciones más rigurosas sobre estas integraciones, con el objetivo de salvaguardar la privacidad y la seguridad de los usuarios (Cárdenas, y otros, 2020).

La gestión inapropiada de la información personal por parte de las plataformas de redes sociales puede resultar en violaciones extensas de datos. El escándalo de Cambridge Analytica es un ejemplo que ilustra las graves consecuencias que pueden surgir de la recopilación y utilización inapropiada de datos. La legislación ecuatoriana, representada por el Código Orgánico Integral Penal (COIP) y otras disposiciones de protección de datos, tiene como objetivo abordar estas problemáticas. Sin embargo, la efectiva puesta en marcha de dichas leyes demanda una colaboración conjunta entre las autoridades y las empresas tecnológicas. Esto se realiza con el propósito de garantizar un entorno digital más seguro y confiable.

1.6.Modalidades de Estafa en Redes Sociales

1.6.1. Tipos de estafas comunes

Phishing y spear-phishing

El phishing es una técnica de ingeniería social utilizada por delincuentes cibernéticos para engañar a las personas y obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito. Este método generalmente implica el envío de correos electrónicos fraudulentos que parecen provenir de fuentes legítimas, como bancos o servicios en línea, solicitando a los destinatarios que proporcionen información personal a través de enlaces maliciosos. (Agazzi, 2020)

El spear-phishing, una variante más sofisticada del phishing, se dirige a individuos específicos dentro de una organización, utilizando información personalizada para aumentar la credibilidad del engaño. Los atacantes investigan a sus víctimas potenciales para crear mensajes convincentes que parecen provenir de colegas, socios comerciales o superiores jerárquicos. Esta táctica incrementa significativamente las probabilidades de éxito del ataque, ya que las víctimas son más propensas a confiar y actuar sobre mensajes que parecen relevantes y legítimos. La doctrina jurídica subraya la necesidad de medidas de seguridad adicionales y

educación continua para contrarrestar estas amenazas dirigidas (Baig, Ahmed, & Memon, 2021).

La efectividad de los ataques de phishing y spear-phishing radica en la capacidad de los atacantes para manipular la confianza y la percepción de las víctimas. Los correos electrónicos fraudulentos a menudo contienen enlaces a sitios web clonados que imitan a los originales, capturando las credenciales de acceso ingresadas por las víctimas. Las empresas de tecnología y las plataformas de redes sociales deben implementar tecnologías avanzadas de detección de fraudes y autenticación multifactor para reducir la vulnerabilidad de los usuarios a estos ataques (Yasin, Fatima, Jiangbin, Afzal, & Raza, 2024). La legislación ecuatoriana, apoyada por la jurisprudencia, respalda estas medidas al promover un entorno digital más seguro.

En respuesta a la creciente amenaza de phishing y spear-phishing, la colaboración entre entidades públicas y privadas es crucial. Las campañas de sensibilización pública, combinadas con herramientas de ciberseguridad robustas, pueden ayudar a mitigar el riesgo. Además, la cooperación internacional es esencial para rastrear y detener a los perpetradores, quienes a menudo operan desde múltiples jurisdicciones. La legislación en Ecuador, alineada con tratados internacionales sobre cibercrimen, facilita estos esfuerzos colaborativos, destacando la importancia de una estrategia integral para combatir el fraude digital en todas sus formas.

Fraudes de inversión y esquemas Ponzi

Los fraudes de inversión y los esquemas Ponzi son considerados como actividades delictivas en el ámbito financiero, ya que involucran la promesa de rendimientos elevados con un riesgo mínimo, lo cual conduce a la decepción de los inversionistas y a la captación de sus fondos. En un esquema Ponzi, los beneficios distribuidos a los primeros inversionistas se originan en las contribuciones de nuevos inversionistas, en lugar de en ganancias reales generadas por inversiones legítimas. Cuando no se logra atraer a un número adecuado de nuevos inversores para pagar a los inversionistas previos, este modelo experimenta un colapso inevitable, lo que resulta en pérdidas significativas para la mayoría de los participantes (Zambrano, 2022).

El atractivo de los fraudes de inversión se encuentra en las promesas de rendimientos elevados y rápidos, las cuales suelen ir respaldadas por documentación fraudulenta y testimonios falsos que buscan incrementar la credibilidad del esquema. Los criminales emplean estrategias de persuasión y manipulación con el propósito de obtener la confianza de sus víctimas, las cuales

frecuentemente carecen de conocimientos financieros o buscan vías rápidas para mejorar su situación económica.

Los esquemas Ponzi se caracterizan por su capacidad de impactar a un gran número de individuos en un lapso breve, lo que los hace especialmente dañinos. Frecuentemente, los responsables suelen ser personas que proyectan una imagen de respetabilidad y logro, empleando medios digitales y redes sociales para llegar a un extenso público. En Ecuador, las autoridades financieras y judiciales han incrementado sus acciones para detectar y eliminar dichos esquemas, a través de la aplicación de medidas de control más rigurosas y campañas de sensibilización dirigidas a la población (Vaca, Martínez, & Toasa, 2022). La detección temprana y prevención de fraudes requiere una colaboración crucial entre entidades financieras y fuerzas del orden.

Las medidas legales para abordar los fraudes de inversión y esquemas Ponzi consisten en la imposición de sanciones penales y civiles significativas. Estas medidas tienen como objetivo desalentar a los individuos que puedan incurrir en prácticas fraudulentas y garantizar la reparación a quienes hayan sido afectados. La restitución de los fondos a los afectados es un aspecto crucial en la resolución de estos casos, sin embargo, con frecuencia resulta complicado recuperar la totalidad de la cantidad de dinero perdida (Triana, 2022). En Ecuador, la jurisprudencia ha establecido un sólido marco para abordar los delitos mencionados, resaltando la importancia de una regulación financiera más rigurosa y una mayor colaboración a nivel internacional para hacer frente de manera efectiva a los desafíos que conllevan los fraudes de inversión en la era digital.

Suplantación de identidad y perfiles falsos.

La suplantación de identidad y la creación de perfiles falsos representan fenómenos cada vez más prevalentes en el ámbito jurídico contemporáneo. Este tipo de conductas ilícitas involucra la usurpación de la identidad de un individuo mediante el uso indebido de información personal, con el propósito de obtener beneficios indebidos o causar perjuicio a terceros. La proliferación de plataformas digitales y redes sociales ha facilitado la creación y difusión de perfiles falsos, que pueden ser utilizados para engañar a otros usuarios o incluso cometer delitos más graves, como estafas o acoso cibernético (Cárdenas, Rosero, Holovatyi, & Pazos, 2020).

Desde una perspectiva legal, la suplantación de identidad y el uso de perfiles falsos constituyen una violación a la integridad personal y un atentado contra la privacidad de los individuos

afectados. Los marcos legales deben contemplar mecanismos eficaces para la prevención, detección y sanción de estas prácticas, asegurando así la protección de los derechos fundamentales de las personas. La identificación y autenticación digital se han vuelto imperativas para mitigar los riesgos asociados con la manipulación fraudulenta de identidades en entornos virtuales, promoviendo la seguridad y confianza en el uso de plataformas digitales.

Además de las implicaciones legales, la suplantación de identidad y los perfiles falsos también plantean desafíos éticos y sociales significativos. El fenómeno no solo compromete la seguridad digital de los individuos y organizaciones, sino que también afecta la credibilidad y la reputación de las plataformas donde ocurren estos actos. La necesidad de concienciación y educación sobre el uso responsable de la información personal en línea es crucial para mitigar estos riesgos y promover prácticas digitales éticas y seguras (Galindo, 2024). En última instancia, abordar eficazmente la suplantación de identidad y los perfiles falsos requiere una colaboración integral entre legisladores, autoridades judiciales, empresas tecnológicas y la sociedad en general para desarrollar estrategias preventivas y correctivas adecuadas.

1.7.Normativa Legal

1.7.1. Sanciones ante estafa y defraudación cibernética

En Ecuador, el Código Orgánico Integral Penal (COIP) establece sanciones severas para los delitos de estafa y defraudación cibernética, las cuales consisten en penas de privación de libertad cuya duración depende de la gravedad de la infracción cometida. A continuación, se presentan ejemplos de las penalizaciones aplicables a dichos delitos:

Estafa común

La estafa, que implica la manipulación a través de la presentación de hechos ficticios o la omisión de información verídica con el propósito de inducir a error y provocar una pérdida económica, está castigada con diversas penas que se determinan según la naturaleza del delito y las condiciones en las que se llevó a cabo el engaño.

Fraude informático

Este acto ilícito es castigado con penas privativas de libertad que oscilan entre 3 y 5 años. Se incluyen acciones como la interceptación no autorizada de comunicaciones y la vulneración de la integridad de sistemas informáticos.

Apropiación Fraudulenta por Medios Electrónicos

Las personas que empleen de manera fraudulenta sistemas informáticos con el fin de adquirir ilegítimamente propiedades de terceros o facilitar transferencias no autorizadas pueden ser condenadas a penas de 1 a 3 años de privación de libertad. La acción delictiva abarca la manipulación de sistemas con el fin de transferir valores o la desactivación de sistemas de seguridad para llevar a cabo el acto ilícito.

Artículo 178 del COIP

Garantiza la protección del derecho a la privacidad. Las acciones que vulneren la privacidad personal y familiar a través de dispositivos electrónicos son castigadas con penas de uno a tres años de privación de libertad.

Artículo 186 del COIP

El presente estudio aborda la tipificación de la estafa, la cual abarca aquellas acciones realizadas a través de dispositivos electrónicos que tienen la capacidad de alterar o replicar dispositivos legítimos con el fin de obtener o duplicar datos de tarjetas de crédito, estableciendo como sanción máxima un periodo de reclusión de hasta 7 años.

Artículo 190 del COIP

La apropiación fraudulenta por medios electrónicos se define como el acto de utilizar sistemas informáticos o redes con el fin de facilitar la apropiación de bienes pertenecientes a terceros o la transferencia de bienes, valores o derechos sin consentimiento, y se establecen sanciones para quienes incurran en esta conducta. Las sanciones contempladas abarcan penas de privación de libertad que oscilan entre uno y tres años. La sanción mencionada se impone en casos donde se haya cometido el delito mediante la desactivación de sistemas de alarma, la obtención de contraseñas encriptadas o la vulneración de medidas de seguridad electrónicas.

Artículo 229 del COIP

La revelación no autorizada de información de bases de datos personales es castigada con una pena de prisión que va desde un año hasta tres años.

Artículo 232 y 233 del COIP

Los ataques a la integridad de sistemas informáticos y los delitos contra la información pública reservada son tipificados con penas que oscilan entre tres y cinco años de prisión.

Código Orgánico General de Procesos (Cogep):

El presente código se emplea en el marco del proceso legal relacionado con los delitos informáticos, dada la inexistencia de una legislación especializada en esta materia en el país.

Ley Orgánica de Telecomunicaciones

A pesar de no especificar delitos informáticos, la ley en cuestión establece normativas y penalizaciones para la utilización inapropiada de las telecomunicaciones, lo cual abarca la posible utilización indebida de redes sociales con fines delictivos.

Ley Orgánica de Datos Personales

La ley en cuestión, a pesar de encontrarse en fase de implementación y desarrollo, define los parámetros para la protección de datos personales y puede ser utilizada en situaciones en las que el fraude o la apropiación indebida conlleven el uso ilegítimo de información personal.

Los artículos y leyes mencionados establecen el marco jurídico para la penalización de los crímenes perpetrados mediante el uso de tecnologías electrónicas, abarcando también las plataformas de redes sociales. A pesar de la inexistencia de una normativa específica que aborde de manera exclusiva los delitos informáticos, las disposiciones del Código Orgánico Integral Penal (COIP) y otras leyes pertinentes posibilitan a las autoridades judiciales la persecución y penalización de dichas infracciones.

CAPITULO II

METODOLOGÍA DE LA INVESTIGACIÓN.

2.1 Tipo de investigación.

En el presente trabajo de titulación se empleará el método cualitativo debido a su naturaleza al ser una indagación de la realidad basado en la experiencia y razonabilidad del legislador, es esencial utilizar como método la entrevista a los conocedores del tema, para comprender en profundidad la experiencia de los administradores de justicia en la investigación y a través de la recolección de datos estadísticos información emitida por la fiscalía general del estado para reforzar el análisis y criterio sobre los delitos de estafa y apropiación fraudulenta por redes sociales ocurridos en la cuidad de Cayambe año 2022 – 2023.

2.2 Métodos de la Investigación.

2.1.1 Método Cualitativa

La investigación cualitativa es esencial para explorar las percepciones, experiencias y actitudes de las personas afectadas por delitos de estafa y apropiación indebida en las redes sociales. A través de técnicas como las entrevistas en profundidad, los grupos de discusión y el análisis de contenido, se puede obtener una comprensión más rica y detallada del impacto de estos delitos en las víctimas y de cómo se perciben las respuestas institucionales. La base estadística obtenida de la Fiscalía General del Estado se utiliza para contextualizar y corroborar los hallazgos cualitativos, asegurando así una comprensión integral del fenómeno.

2.2 Técnicas e instrumentos de investigación

2.2.1 Entrevista

Se empleará la técnica de la entrevista para obtener información detallada y cualitativa de personas clave implicadas en resolver casos de estafa y apropiación fraudulenta en redes sociales en Cayambe. Se realizarán entrevistas semiestructuradas a expertos en ciberseguridad de la policía judicial, fiscales, abogados de libre ejercicios y administradores de justica del cantón Cayambe. Estás entrevistas permitirán explorar experiencias personales, percepciones y recomendaciones para mejorar la prevención y respuesta a estos delitos

2.2.2 Recolección de datos estadísticos.

La compilación de datos estadísticos será esencial para proporcionar una base cuantitativa sólida sobre la incidencia y las características de los delitos investigados. Los datos se recopilarán a partir de informes policiales, denuncias judiciales y estadísticas oficiales relacionadas con estafas y fraudes en plataformas digitales durante el periodo especificado. Estos datos permitirán analizar tendencias, identificar zonas geográficas de mayor incidencia y evaluar la eficacia de las medidas de seguridad aplicadas.

CAPITULO III

ANÁLISIS DE RESULTADOS

3.1 Entrevista.

3.1.1 Entrevista N.º. 1

Tabla 2

Entrevista N. º1 a los abogados de libre ejercicio

ENTREVISTA A LOS ABOGADOS DE LIBRE EJERCICIO	
NOMBRE DEL ENTREVISTADO: ABG. ISSACK PINANGO.	
FECHA DE LA ENTREVISTA: 24 de junio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Considera que las redes sociales representan un problema grave en la sociedad actual? ¿Por qué o por qué no?	No Considero que sea un problema a la final el sistema actual que se ha digitalizado dentro del sistema ecuatoriano o dentro del sistema judicial ha servido mucho para dar eficacia a la justicia y más que nada transparencia dentro de los procesos, agilita mucho y genera una estabilidad dentro de lo de las causas que están haciendo sustanciadas en los despachos de los jueces.
PREGUNTA 2: ¿En su experiencia, ¿cuáles son los sectores o grupos de población más vulnerables a este tipo de delitos?	Yo considero que toda la población en general tanto niños jóvenes como adultos mayores o personas de la mediana edad todos somos vulnerables, ante cualquier delito informáticos. Las redes se van actualizando y los delitos también siempre se generan nuevos modos de hacer o dar entender que existen nuevos tipos de delito que deberían de ser tipificados en el código orgánico integral, sin embargo, como te digo eso va variando conforme los años van pasando y con los nuevos avances tecnológicos.
PREGUNTA 3: ¿Qué medidas o reformas al sistema legal consideraría necesarias para	la implementación o reforma al código orgánico integral penal o algún cuerpo normativo en donde especifique, y se detalle los nuevos delitos informáticos, más más que

combatir estos delitos de manera más efectiva?	nada. caminen hacer entender a la rama jurídica Cómo estos delitos pueden tipificarse o adecuarse al tipo penal. Por qué de ser el caso pueden surguir un nuevo delito que no esté tipificado en el código orgánico penal y esto afectaría mucho al poder punitvo del estado, por tal razón considero que un cuerpo normativo o una reforma seria lo adecuado, claro que existe allí, existe la ley de correo electrónica y firmas, sin embargo, como te menciono, el internet, inteligencia artificial e incluso las redes sociales dan paso a nuevas modalidades de delitos, que cualquier experto en derecho desconoces e incluso juristas, jueces no estén al tanto de estas actualizaciones.
PREGUNTA 4: ¿Cuáles serían los principales desafíos que enfrentan los abogados en la representación de víctimas o acusados de estos delitos?	Las complicaciones serían más o menos la falta de conocimiento en el área informática, los abogados se especializan en lo que es derecho sin embargo especializarse en la rama informática implica que debemos de estudiar todo el lenguaje que los ingenieros del sistema los ingenieros de software manejan incluso para una mejor defensa deberían implementar lo que sería nuevos peritos que se enfocan en el estudio de estos delitos. cosa que un abogado en ejercicio libre desconoce.
PREGUNTA 5: ¿Ha tenido alguna experiencia personal o profesional relevante con casos de estafa o apropiación fraudulenta	Personal, no profesional personalmente si ha habido o ha existido estos delitos. De apropiación ilícita de información, por ejemplo, haciéndose pasar por alguna entidad financieras que necesitan actualizar tus datos y esas cosas, entonces te solicitan tanto tu copia de cédula, tus firmas y tal entonces claro, uno no como te menciono desconoce a veces las nuevas modalidades de la expropiación ilícita de información y caen en estos delitos.

Fuente: Entrevista realizada al Abg. Isack Pinango.

Elaborado por: Reny Perez

ANALISIS

En general el entrevistado considera que las redes sociales no representan un problema grave en la sociedad actual, ya que el sistema digitalizado ha servido para dar eficacia y transparencia a la justicia, agilizando los procesos judiciales y generando estabilidad en las causas que se sustancian en los despachos de los jueces. Esto implica desde una perspectiva legal, las redes sociales no se perciben como un problema significativo en términos de justicia y transparencia.

En cuanto a las medidas necesarias para combatir los delitos estafa y apropiación fraudulenta, destaca la importancia de reformas al código orgánico integral penal donde tipifiquen adecuadamente los nuevos delitos informáticos, ya que el internet, la inteligencia artificial y las redes sociales dan paso a nuevas modalidades delictivas que pueden no estar contempladas en la normativa actual. Esto resalta la necesidad de adaptar la legislación a los avances tecnológicos para abordar de manera efectiva los delitos informáticos.

Los principales desafíos que enfrentan los abogados al representar a víctimas o acusados de delitos informáticos incluyen la falta de conocimiento en el área informática, la necesidad de especializarse en la rama informática y la implementación de nuevos peritos especializados en el estudio de estos delitos. Esto destaca la importancia de la formación especializada en informática para los abogados que trabajan en casos de delitos informáticos.

Según la experiencia del Abogado Pinango, todos los sectores de la población, desde niños hasta adultos mayores, son vulnerables a los delitos informáticos, ya que las redes y los delitos se van actualizando constantemente con los avances tecnológicos. Esto subraya la necesidad de concienciar a toda la población sobre los riesgos y la importancia de estar informados sobre las nuevas modalidades delictivas. Esto ilustra la realidad de los delitos informáticos y la importancia de estar alerta ante posibles estafas o fraudes en línea.

3.1.2 Entrevista N.º. 2

Tabla 3

Entrevista N.º 2 a los abogados de libre ejercicio

ENTREVISTA A LOS ABOGADOS DE LIBRE EJERCICIO
NOMBRE DEL ENTREVISTADO: ABG. MARGARITA GUERRA
FECHA DE LA ENTREVISTA: 05 de julio del 2024
CUESTIONARIO DE PREGUNTAS:

PREGUNTA 1: ¿Considera que las redes sociales representan un problema grave en la sociedad actual? ¿Por qué o por qué no?	Nos hemos ayudado mucho como sociedad avanzar rompiendo las distancias incluso a tecnologizarnos un poco más en ese sentido. Considero que si una sociedad es debidamente educada y preparada no Debería ser un problema, no podría ser considerado como problema como te digo son temas que recién están saliendo, hay gente que de alguna manera es analfabeta, son básicamente esas personas las que caen en este tipo de delitos, o sea, yo creo que la tecnología no hay que tenerle miedo, al contrario. Yo creo que nos ha ayudado mucho a crecer como como sociedad como personas a nivel profesional también nos ha ayudado mucho, pero sí, lo que se debería de pronto en las instituciones educativas es un poquito más fortalecer este tema educar, para que esto no represente un problema contrario las redes sociales son una necesidad.
PREGUNTA 2: ¿En su experiencia, ¿cuáles son los sectores o grupos de población más vulnerables a este tipo de delitos?	La población más vulnerable es la que carece de conocimientos, Yo te hablo en que te hable en el sector rural las comunidades hay gente que digamos puede ser ingeniería desconocimiento y un poquito hasta del tema de Educación Sí ellos son los principales afectados con el tema de las redes sociales con el tema tecnológico. Es gente que digamos de alguna manera son ingenuos. Ellos piensan como funciona su comunidad funciona en todo el país o todo el mundo, pero no es así entonces si nosotros educáramos a esas personas educáramos de esos niños no puede suceder este tipo de vulneraciones en esas en esas poblaciones digámoslo así.
PREGUNTA 3: ¿Qué medidas o reformas al sistema legal consideraría necesarias para combatir estos delitos de manera más efectiva?	Una legislación acorde a nuestra realidad una legislación que prevea normativa incluso procedimientos en los temas de redes sociales en el tema tecnológicos, porque podríamos conseguir mejores legislaciones investigando porque como te digo hay países que tiene mejores

	legislaciones que nos llevan 10 a 15 años mucho más actualizados.
PREGUNTA 4: ¿Cuáles serían los principales desafíos que enfrentan los abogados en la representación de víctimas o acusados de estos delitos?	La falta de normativa son los principales desafíos que ellos enfrentan dado que igual los abogados no están capacitados, no estamos preparados todavía para eso, aquí en Cayambe no hay un solo abogado especialista que haya representado uno de estos casos, entonces la falta de investigación de conocimiento e ir adaptando legislaciones extranjeras a nuestra realidad nos podría ayudar muchísimo.
PREGUNTA 5: ¿Ha tenido alguna experiencia personal o profesional relevante con casos de estafa o apropiación fraudulenta	casos relevantes en el periodo 2022-2023 no hemos tenido, este año bueno aquí en Cayambe hubo uno de un tema de una estafa que hicieron de la venta de unos predios la organización Santa Cecilia, se ofertaron a través de Facebook y demás redes sociales, no sé si conoces ahí vendieron varios terrenos los cuales jamás fueron entregados a las personas que Aparentemente compraron fue problema que desató muchos muchas investigaciones en la fiscalía algunos juicios llegaron también a tribunales entiendo que algunas le declararon en sentencias otros rectificaron su estado de inocencia otras civiles condenaron a estas personas y fue un caso que se escuchó mucho porque el fraccionamiento de esa organización fue demasiado grande creo que había más o menos alrededor de unas 115 personas que fueron perjudicadas. Entonces el número es bastante fue una estafa que fue sonada mucho aquí. Por la ciudad todavía.

Fuente: Entrevista realizada

Elaborado por: Reny Perez

ANALISIS

Margarita Guerra ofrece una visión crítica pero optimista de las redes sociales, considerándolas una herramienta útil siempre que la sociedad esté debidamente educada. Destaca que las poblaciones rurales y con menor acceso a la educación son las más vulnerables a la

ciberdelincuencia. Guerra aboga por una legislación adaptada a las realidades locales y actualizada en base a modelos extranjeros de éxito. También destaca la necesidad de formación para los abogados y la adaptación de la legislación extranjera a la realidad ecuatoriana para mejorar la representación legal en estos casos. Un caso notable mencionado es la estafa masiva a través de Facebook en Cayambe, que afectó a 115 personas, lo que evidencia la gravedad del problema.

3.1.3 Entrevista N.º. 3

Tabla 4

Entrevista N. º3 al personal de la policía judicial

ENTREVISTA AL PERSONAL DE LA POLICIA JUDICIAL	
NOMBRE DEL ENTREVISTADO: JORGE LUIS LUNA Sargento Segundo de PJ.	
FECHA DE LA ENTREVISTA: 26 de junio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Cuáles son las principales plataformas de redes sociales más utilizadas para cometer estos delitos en Cayambe?	Las plataformas más utilizadas en la actualidad es el WhatsApp y Facebook ya que por WhatsApp ese el medio de comunicación lo que es llamadas, mensajes y segundo Facebook donde nosotros lo conocemos como el enganche, donde diferentes tipos de personas indican las cosas que venden o compran, posterior se comete la estafa.
PREGUNTA 2: Cuáles son los métodos más comunes utilizados por los estafadores para cometer estos delitos en Cayambe a través de las redes sociales?	Existen dos estrategias de las personas que se dedican a la estafa y la apropiación, como primer punto tenemos el engaño, Porque primero, es un entorno familiar en este entorno familiar, te voy a poner un ejemplo también, El delincuente se hace pasar por un familiar directo o algún conocido en donde él te menciona que está en el exterior que va a enviar dinero pero a cambio de eso necesita que la hagas como decirte un encaje para que puedan llegar las encomiendas también te dicen que estas personas o

	este supuesto familiar tiene problemas. Ya sea judiciales con policías con aduaneros o cualquier situación y a cambio de resolver esos problemas te pide dinero, entonces ahí viene y llegan a cometer estos delitos. Te digo en este entorno en este círculo familiar y también hay un círculo o un entorno comercial en donde se publica que está vendiendo o que quiere comprar cualquier objeto, el actor del delito se encarga de llegar a tu mente o tiene la capacidad de Convencerte. Entonces él te envía hasta documentos te envía un sin número de cosas, él te convence hasta te dice que él trabaja en una institución que todo es seguro entonces tú accedes, ya sea a depositar o de pronto a enviar el producto que vendes, un ejemplo este estafador te dice Yo necesito comprar 10 computadoras y tú te dedicas a vender computadoras Entonces ya te digo, te convence indica documentos todo eso y tú accedes envías las computadoras. Envían a personas x qué sé yo un Drive alguien que esa persona solo hace su trabajo, no es que esté dedicada también o esté correlacionada con los estafadores y ellos van y trasladan. Entonces como te dije al principio existen dos círculos o dos métodos.
PREGUNTA 3: ¿Han observado algún patrón o tendencia en cuanto al modus operandi de los estafadores que operan en Cayambe a través de las redes sociales?	existe patrones como le dije el engaño en síntesis es el engaño, el patrón común Ya que ellos tratan de convencerte, ya sea con mensajes con audios con documentos y Ellos Llegan ya te digo a convencerte en su totalidad para acceder de pronto también en Facebook la persona llega a tener como se podría decir una cierta ingenuidad un ejemplo en Facebook publicas un paseo familiar con tu hijo, tu esposa tus padres Entonces tienes que tener una cierta reserva para las personas que van a ver eso, no tienen que ser tan público Y entonces el estafador como tiene acceso, ya te digo, no es todo

	restringido. Y es gracias a la ingenuidad de todos los usuarios de Facebook que el estafador puede ver puede saber quién es tu padre tu hijo, tu esposa y a la vez puede utilizar esas personas como que para conseguirte convenciendo de que en verdad es esa persona cercana a tu círculo familiar con esto llega al convencimiento.
PREGUNTA 4: ¿Qué medidas de prevención considera que se deberían implementar para reducir la incidencia de estos delitos en Cayambe?	Primero deberían de limitarse y debe publicar cualquier situación en su círculo Familiar o círculo conocido que toda la información no sea de acceso público, entonces ahí se limitaría lo que es el acceso a la información y para que esa información no sea mal utilizada. Segundo y creo que esto es lo más importante de que las personas si es que hacen un negocio, si es que tienen conversaciones si tienen algún vínculo con cualquier persona que les está pidiendo a cambio dinero tienen que asegurarse. Un ejemplo, si es que alguien le dice yo estoy vendiendo algo, tienen que verificar las cuentas de que en verdad les llegó una transacción una transferencia un depósito deben de cerciorarse bien porque hay veces que solo les llega un correo y un correo, Tú sabes que les puede enviar a cualquiera, Yo puedo ingresar a mi teléfono celular y enviar un correo a cualquier persona hacerme pasar por una entidad privada o pública. Entonces las personas deben de verificar si es que en verdad se les realizó un depósito transferencia y los más recomendado serian que las compras o venta la hagan de forma personal para no caer en estos actos.
PREGUNTA 5: ¿cuenta con las herramientas o con los recursos tecnológicos adecuadas para rastrear y localizar a las personas que comente estos delitos?	Si cometamos con la tecnología, pero aquí podemos establecer que en la actualidad y con el desarrollo de la tecnología cada vez viene a ser un poquito más difícil identificar ubicar a estas personas, ¿por qué? Porque todo es ahora por internet como es la utilización de WhatsApp y Facebook por eso se utiliza internet, no es como

	anteriormente todo era por vía telefónica llamadas o mensajes se podía rastrear esa llamada o ese mensaje, pero en la actualidad como todos utiliza internet entonces son direcciones IP y también al utilizar WhatsApp o Facebook hay que pedir o Solicitar a los representantes de esas plataformas, esa solicitud debe emitir la autoridad competente y esto obviamente no es aquí en el Ecuador es en el exterior. Entonces la información va a llegar Se podría decir tarde o discontinuo lo que dificulta para ubicar identificar a los autores de los delitos entonces en la actualidad se podría mencionar el desarrollo de las tecnologías la investigación se complica un poco.
PREGUNTA 6: Considera usted que el mercado libre o mayormente conocido como Marketplace es el sitio donde ocurre más estos delitos	Existen algunas plataformas mejor dicho todas las plataformas donde en donde se dedique a realizar el comercio la compra y venta van a ser vulnerables a las estafas pero como tú lo dices de y la pregunta lo está aseverando, Sí en verdad Ahora Marketplace es la plataforma en donde más se Está realizando estas estafas ya que este medio es de mayor uso en el Ecuador al menos es el de mayor uso de Facebook es el que más se utiliza Entonces Por ende esta plataforma Marketplace es la más utilizada para realizar las estafas y muy poco la apropiación fraudulenta.

Fuente: Entrevista realizada al Sargento Segundo Jorge Luis Luna.

Elaborado por: Reny Perez

ANALISIS

El sargento segundo Jorge Luis Luna identifica a WhatsApp y Facebook como las plataformas más utilizadas para cometer estafas en Cayambe. Describe métodos comunes, como el engaño en entornos familiares y empresariales, donde los estafadores se hacen pasar por familiares o empleados de instituciones. Luna destaca la importancia de limitar la publicación de información personal y verificar la autenticidad de las transacciones para evitar fraudes. A

pesar de contar con recursos tecnológicos para localizar a los delincuentes, destaca la complejidad añadida del uso de Internet y la necesidad de cooperación internacional para obtener información de plataformas extranjeras.

3.1.4 Entrevista N.º. 4

Tabla 5

Entrevista N. º4 al personal de la policía judicial

ENTREVISTA AL PERSONAL DE LA POLICIA JUDICIAL	
NOMBRE DEL ENTREVISTADO: ENTREVISTADO 2	
FECHA DE LA ENTREVISTA: 26 de junio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Cuáles son las principales plataformas de redes sociales más utilizadas para cometer estos delitos en Cayambe?	En la actualidad con el avance tecnológico existe varias plataformas de redes sociales, pero en nuestra experiencia las más utilizadas son Facebook, WhatsApp y Instagram.
PREGUNTA 2: Cuáles son los métodos más comunes utilizados por los estafadores para cometer estos delitos en Cayambe a través de las redes sociales?	Uno de lo más utilizados es el famoso método phishing, es conocido por ser el mas utilizados por los delincuentes, mediante link a través de teléfonos celulares pueden engañar a la víctima, utilizando el engaño, haciéndose pasar por familiares, amigo. De igual forma otro método que se está dando recientemente es la utilización de moneda electrónica, haciéndose pasar por empresas, con el fin de lucrarse.
PREGUNTA 3: ¿Han observado algún patrón o tendencia en cuanto al modus operandi de los	La ingenuidad de la gente por querer lucrarse de la manera más rápida o conseguir dinero de forma inmediata, se dejan engañar de los famosos prestamistas

estafadores que operan en Cayambe a través de las redes sociales?	de las redes sociales, te pongo de ejemplo, en Facebook el cual es la plataformas mas utilizadas por los internautas, hay muchos perfiles falsos que ofertan prestamos a una tasa baja de interés, donde le envían contratos supuestamente legales, para obtener préstamos, dicho contrato debe ser pagado, donde allí aprovechan para solicitar dinero, o el otro que igualmente es típico, donde se hacen pasar por empresas y piden dinero por adelantado.
PREGUNTA 4: ¿Qué medidas de prevención considera que se deberían implementar para reducir la incidencia de estos delitos en Cayambe?	No entregar ningún tipo de información, estos pueden facilitar el acceso a la vida privada de la persona. El desconocimiento y la ambición son un factor para que se genere un modus operando de estos delincuentes. No entregar ninguna cantidad de dinero, no realizar compras en sitios que no son conocidos y que cualquier compra y venta de artefactos, herramientas etc. Sean hechas en forma presencial y no virtual.
PREGUNTA 5: ¿cuenta con las herramientas o con los recursos tecnológicos adecuadas para rastrear y localizar a las personas que comente estos delitos?	Si, contamos con recursos tecnológicos y sistemas para localizar a estos tipos de delincuentes, solo podemos operar cuando sea conocida por una autoridad competente, podemos rastrear equipos tecnológicos de manera rápida siempre y cuando sea en delitos fragantes. Pero con el avance tecnología si necesario tener más equipos tecnológicos para poder localizar, además se necesita capacitaciones constantes, la tecnología avanza por lo tanto debemos de ir avanzando tal como avanza la tecnología. Como le mencione, al principio para obtener información privada de las redes sociales, primero deben emitir un oficio la entidad competente para nosotros poder actuar.
PREGUNTA 6: Considera usted que el mercado libre o mayormente conocido como	Si. Por no mencionar que es el lugar donde se realiza la mayor cantidad de estafas, muchas personas ofertan un sin numero de cosas, hay perfiles que son calificados

Marketplace es el sitio donde ocurre más estos delitos	como vendedor recomendando, de igual manera no se deben de dejar convencer, hay que entender que las redes sociales facilitan la comisión de delitos y si no tenemos una educación informática adecuada, los casos de estafa y apropiación fraudulenta van a crecer, las personas deben de tener mucho cuidado, por que muchas ocasiones no se puede identificar la identidad del presunto delincuente, muchos estos delitos son cometidos fuera del país, es decir son cometidos por personas de otros países.

Fuente: Entrevista realizada, entrevistado 2

Elaborado por: Reny Perez

ANALISIS

Este encuestado corrobora el uso de Facebook, WhatsApp e Instagram como principales plataformas para las estafas, destacando el método del phishing y el uso de moneda electrónica. Identifica la ingenuidad y la falta de educación informática como factores que facilitan estos delitos. Propone medidas preventivas como no compartir información personal o dinero en plataformas no verificadas. Aunque disponen de recursos tecnológicos, el entrevistado señala la necesidad de más equipamiento y formación constante debido a la rápida evolución tecnológica. El mercado es señalado como uno de los principales focos de estafas en Facebook.

3.1.5 Entrevista N.º. 5

Tabla 6

Entrevista N. º5 a jueces de los penales de Cayambe

ENTREVISTA A JUECES DE LOS PENAL DE CAYAMBE
NOMBRE DEL ENTREVISTADO: DR. MARIO CASTRO
FECHA DE LA ENTREVISTA: 27 de junio del 2024
CUESTIONARIO DE PREGUNTAS:

PREGUNTA 1: ¿En qué consiste el delito de apropiación fraudulenta y en qué se diferencia de la estafa?	Tanto el Delito estafa como el delito de apropiación fraudulenta están contemplados dentro de lo que es el bien protegido el derecho a la propiedad. la diferencia seria que uno es en forma directa la intervención de la parte actora directamente con una segunda persona para apropiarse de sus bienes y en la otra eso bien la intervención de un sistema netamente por medio de sistemas electrónicos. Es decir no serian de forma personal sino de un medio que serían los medios electrónicos.
PREGUNTA 2: ¿Durante su trayectoria como administrador de justicia cuál cree que es el principal desafío que enfrentan los jueces al abordar casos de estafa y apropiación fraudulenta cometidos a través de redes sociales?	Bueno, el juzgador tiene conocimiento de los hechos y del proceso investigativo que evacuar tanta fiscalía con el apoyo de la presunta víctima para acumular elementos de cargo y elementos de descargos el juez antes los hechos que se pone a conocimiento por parte del titular de la acción solamente son los recaudos. Qué sustentarían tanto en delitos de estafa y apropiación fraudulenta. El juez carece de iniciativa procesal para evacuar pruebas solo puede actuar a bases de lo que se presente en el momento de la audiencia tanto de formulación de cargo como la evaluación o preparación de juicio o de ser caso la etapa de juzgamiento.
PREGUNTA 3: cuando no se detecta al actor de estos delitos ¿Qué papel juegan las declaraciones de las víctimas?	Como se manifestó en la primera pregunta afectan el patrimonio de una persona económicamente, la víctima tendría tanto que justificar el efecto del perjuicio ocasionado en su patrimonio. Y en cuanto a redes sociales, las redes sociales es difícil tener acceso a la fuente de donde se originó el mensaje o la estafa o la apropiación fraudulenta sería de contar con un perito especializado en esa materia para que puedan tener acceso a los medios electrónicos o de redes sociales

	donde se originaron. los mensajes que fueron materia de delito.
PREGUNTA 4: ¿En el año 2022-2023 cuantos casos de estafa y apropiación fraudulenta tuvieron una sentencia?	Si no estoy errado el promedio de los delitos de estafa que se conoció en el periodo 22/23 fue 1.
PREGUNTA 5: ¿Considera que la normativa actual en el Ecuador es suficiente para abordar adecuadamente los delitos de estafa y apropiación fraudulenta en las redes sociales?	No tenemos un cuerpo legal enfocado solo en los delitos que se comente por redes sociales, pero si, es una normativa con toda la mayoría de los elementos que puedan encuadrarse la conducta de la parte actora dentro de la causa.
PREGUNTA 6: ¿Cómo se han adaptado las leyes y la jurisprudencia para abordar los nuevos retos que presenta la comisión de estos delitos en el entorno digital?	Bueno ahí estudiosos del derecho o personas que se dedican a la investigación más bien doctrinariamente alimentan al conocimiento tanto del juzgador como también puede ser una fuente para que las autoridades de la corte nacional puedan mejorar la legislación en cuanto la estafa y apropiación fraudulenta.
PREGUNTA 7: Existen mecanismos adecuados para garantizar la reparación del daño y la restitución de los bienes a las víctimas de estos delitos?	Los mecanismos que establece el código orgánico integral penal del art.-78 son claros las formas de reparación tanto materiales como inmaterial
PREGUNTA 8: ¿Qué medidas cautelares pueden solicitar las víctimas o las autoridades para proteger sus derechos durante el proceso penal?	Tenemos las personales y la de bienes, las personales son las que establecen el código orgánico integral tanto para asegurar la comparecencia en una etapa de juicio, así como también asegurar la comparecencia o la reparación integral de la víctima, ya sea la presión preventiva o arresto domiciliario o todos los del art 522. Presentación periódica o prohibición de salida que son los medios

	adecuados para asegurar la comparecencia y posible pago de reparación integral. En cuanto sobre bienes, la legislación igual establece en el art 549 todas las medidas cautelares sobre bienes con las prohibiciones de enajenar, embargo o retenciones de cuentas o valores en el sistema bancario nacional o de cooperativa
PREGUNTA 9: Se toman en cuenta factores agravantes o atenuantes al momento de determinar la pena aplicable en cada caso?	La obligatoriedad que tenemos los juzgadores para considerar las atenuantes o agravantes existentes o que se pongan a discusión en la etapa de juicio para que la pena tenga una gradualidad y una sanción correspondiente a los hechos y circunstancia que se presentaron al momento de la comisión del delito.
PREGUNTA 10: Podría mencionar algunos precedentes jurisprudenciales relevantes en Ecuador relacionados con los delitos de estafa y apropiación fraudulenta en el ámbito de las redes sociales?	No he realizado un análisis minucioso. De que si exista precedentes jurisprudenciales

Fuente: Entrevista realizada

Elaborado por: Reny Perez

ANALISIS

El Dr. Mario Castro diferencia entre estafa y apropiación fraudulenta, destacando que la primera suele implicar interacción personal, mientras que la segunda se efectúa principalmente a través de medios electrónicos. Castro menciona la falta de regulación específica para los delitos en redes sociales y el desafío que representa para los jueces la falta de iniciativa procesal y la necesidad de pruebas claras presentadas por la fiscalía y las víctimas. Destaca que en 2022-2023 sólo hubo un caso de estafa con sentencia, lo que indica un bajo índice de resolución de estos delitos

3.1.6 Entrevista N.º. 6

Tabla 7

Entrevista N. º6 a jueces de los penales de Cayambe

ENTREVISTA A JUECES DE LOS PENAL DE CAYAMBE	
NOMBRE DEL ENTREVISTADO: DR. MARCO SALAZAR	
FECHA DE LA ENTREVISTA: 5 de julio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿En qué consiste el delito de apropiación fraudulenta y en qué se diferencia de la estafa?	Bueno la diferencia principal de cada es que una requiere de medios electrónicos necesariamente de redes sociales, tendiendo en cuenta que los medios electrónicos son amplios. con el afán de apoderarse de cuentas bancarias, identidad para obtener patrimonio mientras que la estafa te haces entregar a ti, no con el afán de apropiarte de esas cosas, sino con el afán de aumentar tu patrimonio. Entonces la apropiación seria necesariamente por medios electrónicos principalmente por redes sociales, mientras que la estafa no, puede darse por otros medios.
PREGUNTA 2: ¿Durante su trayectoria como administrador de justicia cuál cree que es el principal desafío que enfrentan los jueces al abordar casos de estafa y apropiación fraudulenta cometidos a través de redes sociales?	si te refieres a la investigación eso le corresponde al fiscal que este a carga. Como administrador de justicia he podido observar que generalmente las estafas se dan de manera verbal por ejemplo, yo te digo es que si tú me pagas cierta cantidad de dinero, yo te voy a dar la licencia por ejemplo o cuando te dicen dame una cierta cantidad de dinero y yo te voy a ayudar a obtener un puesto en la policía, que es lo más usual que utilizan los estafadores Entonces es difícil, que la víctima pueda probar solo con su testimonio que se come que esa persona le ofreció un favor a cambio de dinero. Entonces eso es lo que generalmente pasa en la estafa mientras que en la apropiación fraudulenta. No tenemos legislación una

	legislación apropiada para poder indagar o hacer investigación en medios electrónicos, o sea, todavía no, hay una, pero, yo consideraría que a nivel de otros países. Nosotros nos encontramos todavía en temas ambiguos, la implementación de una verdadera legislación que vaya encaminada a la investigación de redes sociales, quienes crean de dónde parte entiendo que, es más una investigación tecnológica. Eso es el obstáculo principal el llegar a Conocer y como poder llegar a la verdad.
PREGUNTA 3: cuando no se detecta al actor de estos delitos ¿Qué papel juegan las declaraciones de las víctimas?	Un jugador pueda en este caso verificar que se cometió el delito y que y cuál es la persona que lo convirtió en este caso la responsabilidad. ¿Ahí te digo que viene la complejidad por qué? Porque las víctimas. Como Solo nosotros hablamos las víctimas no pueden probar. ¿Hay ocasiones en las que las víctimas hacen depósitos o transferencia eso sería una prueba? ¿Sí si la víctima no tiene con qué sustentar? Su declaración queda en nada, queda en un mero enunciado, recordemos que la prueba testimonial tiene que ser concordante con otro tipo de prueba, de pronto se contactaron por WhatsApp por ese lado podríamos decir que el testimonio más el WhatsApp más el depósito tendría pruebas necesaria que serán presentadas. Un seguimiento lógico para que esta persona pueda en este caso indicar que su testimonio sus declaraciones son los hechos que pasaron. Pero si no tiene como justificar las declaraciones de las víctimas quedan mero enunciados y lógicamente con un testimonio tú no llegas a un tribunal tú nunca vas a tener una sentencia condenatoria. Entonces la prueba tiene que ir dirigida a que el juzgador tenga la conexión la certeza que ese hecho se dio y como se dieron los hechos quien es el responsable de ese hecho.

PREGUNTA 4: ¿En el año 2022-2023 cuantos casos de estafa y apropiación fraudulenta tuvieron una sentencia?	Las estafas generalmente suelen llegar bastante al tema de conciliación porque también es susceptible de conciliación dependiendo como te digo del monto porque cuando son montos grandes, eso va a tribunales. Si no estoy equivocado en el periodo 22/23 se conoció 1 caso de estafa y de apropiación no hemos tenido ninguna sentencia hasta la fecha.
PREGUNTA 5: ¿Considera que la normativa actual en el Ecuador es suficiente para abordar adecuadamente los delitos de estafa y apropiación fraudulenta en las redes sociales?	Nosotros lastimosamente tenemos una legislación que no se adecua a nuestra realidad, yo podría decirte que nuestra legislación es arcaica. No, no está la capacidad de sancionar estos actos. Antes teníamos un código penal que se reformo en el 2015, teníamos delitos como el duelo, imagínate era un código tan ambiguo que en la actualidad no se ven esos casos. Nuestra normativa es una copia de otros países, pero no se adaptan a nuestra realidad no se adecuan las necesidades, si bien te puede decir el código. Los delitos por medios electrónicos, pero no te hablan de redes sociales ahí estos, no te dice Cuál es el procedimiento o cómo partes para poder hacer una verdadera investigación, entonces lastimosamente la normativa no está apta, no es la adecuada para tratar este tipo de temas.
PREGUNTA 6: ¿Cómo se han adaptado las leyes y la jurisprudencia para abordar los nuevos retos que presenta la comisión de estos delitos en el entorno digital?	La legislación a nivel digital estamos recién empezando no estamos todavía al menos no hay normativa correcta para que se puedan llevar ese tipo de investigaciones de ese tipo de resoluciones, o sea, Nosotros somos realmente bastante empíricos al momento de resolver los jugadores somos empírico óseo, se emite su resolución en torno a lo que algo vea algo conozca, pero no es que los jueces están capacitados para poder resolver conforme se debería.
PREGUNTA 7: Existen mecanismos adecuados para	la legislación provee los mecanismos para asegurar la reparación en la norma suprema en el art.-76 nos da la

garantizar la reparación del daño y la restitución de los bienes a las víctimas de estos delitos?	pauta, adicional en el art.-78 del código orgánico integral penal nos dije sobre los mecanismos de reparación integral.
PREGUNTA 8: ¿Qué medidas cautelares pueden solicitar las víctimas o las autoridades para proteger sus derechos durante el proceso penal?	Solicitar medidas cautelares la única entidad que está facultada para solicitar este tipo de medidas ya dentro de un proceso judicial es netamente la fiscalía las víctimas no pueden solicitar ellos pueden allanarse a la petición realizada por el señor fiscal, pero ellos no pueden solicitar medidas cautelares.
PREGUNTA 9: Se toman en cuenta factores agravantes o atenuantes al momento de determinar la pena aplicable en cada caso?	De hecho, estamos supeditados aplicar el agravante para la pena o a su vez las atenuantes Al momento de resolver cada caso en específico cada caso tiene su particularidad entonces entorno y en función a eso después procede a emitir, su resolución hay hechos agravantes, tenemos una norma expresa donde debemos de aplicar las agravantes y las atenuantes dentro de los procesos penales.
PREGUNTA 10: Podría mencionar algunos precedentes jurisprudenciales relevantes en Ecuador relacionados con los delitos de estafa y apropiación fraudulenta en el ámbito de las redes sociales?	Si es sobre el delito de estafa si hay precedentes, pero relacionado con las redes sociales no, las estafas comunes sí. El otro lado si nos referimos a la apropiación fraudulenta, no, he tenido la oportunidad de poder revisar y es mas no hemos de tener ningún precedente como son delitos nuevos no son muy comunes

Fuente: Entrevista realizada

Elaborado por: Reny Perez

ANALISIS

El Dr. Marco Salazar destaca la dificultad de investigar las apropiaciones fraudulentas debido a la falta de legislación específica y de recursos tecnológicos adecuados. Menciona que las

víctimas deben aportar pruebas complementarias para que sus testimonios sean eficaces ante los tribunales. Salazar critica la legislación actual por arcaica y no adaptada a la realidad tecnológica actual, sugiriendo la necesidad de una profunda reforma. También destaca la importancia de la formación constante de los jueces en el ámbito digital para dictar sentencias fundamentadas.

3.1.7 Entrevista N.º. 7

Tabla 8

Entrevista N. º7 a fiscales de Cayambe

ENTREVISTA A FISCALES DE CAYAMBE	
NOMBRE DEL ENTREVISTADO: ENTREVISTADO 1	
FECHA DE LA ENTREVISTA: 8 de julio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Qué desafíos enfrentan las autoridades judiciales en Cayambe para investigar y procesar este tipo de delitos que se cometen en el ámbito digital?	Yo creo bueno en mi experiencia la necesidad de adaptarse a un entorno digital que va en constante evolución, la dificultad para rastrear a los perpetradores, descubrir la identidad de la manera que pueden operar de forma anónima en línea, y la falta de recursos especializados en ciberseguridad y tecnologías digitales en algunas instancias judiciales.
PREGUNTA 2: ¿Qué medida se están tomando para combatir los delitos de estafa y apropiación fraudulenta en las redes sociales?	la capacitación y especialización para poder investigar estos delitos en el ámbito digital, el fortalecimiento de la cooperación internacional para perseguir a los delincuentes transnacionales cabe recalcar que no todos los estos delitos son cometidos dentro del país, y la implementación de concienciación sobre los riesgos asociados con las actividades fraudulentas en línea.
PREGUNTA 3: ¿Se han identificado redes criminales o	Si bien no podría afirmar específicamente la existencia de redes criminales u grupos organizados operando en

grupos organizados que operen en Cayambe y se dediquen a la comisión de este tipo de delitos en las redes sociales?	Cayambe dedicados a la comisión de delitos en redes sociales en los años 2022-2023, es importante que la se investiguen posibles conexiones entre los casos individuales para identificar patrones y posibles redes delictivas. Como te digo aquí en Cayambe, no hemos tenido ningún tipo de conexión
PREGUNTA 4: ¿Existen protocolos específicos para manejar la evidencia digital?	Si, existe y es fundamental contar con estos protocolos específicos para el manejo de evidencia digital en casos de delitos en redes sociales. Estos protocolos incluyen procedimientos claros para la cadena de custodia, preservación y presentación u análisis de las pruebas digitales, así como la garantía de la integridad y autenticidad de la evidencia en el proceso judicial.
PREGUNTA 5: ¿Se ha observado un incremento en el número de casos de estafa y apropiación fraudulenta a través de redes sociales en los últimos años?	En la pandemia se dio muchos casos de estafa y principalmente por Facebook, no te podría ayudar con datos por que toca solicitar, pero efectivamente durante los últimos años se ha visto un aumento significativo de estos casos, el número de casos de estafa y apropiación fraudulenta a través de redes sociales en los últimos años, ayudar a comprender la magnitud del problema y a orientar las estrategias de prevención y persecución de estos delitos.
PREGUNTA 6: ¿Cómo pueden los ciudadanos identificar una posible estafa o intento de apropiación fraudulenta en redes sociales?	Identificar las posibles estafas o intentos de apropiación fraudulenta en redes. Es posible deben de estar atentos a señales de advertencia como promesas de dinero rápido, solicitudes razonables de información personal o dinero y cosas que parecen genuinas. Es importante confirmar la autenticidad de la fuente y la empresa detrás de la información antes de intercambiar información personal o hacer negocios en línea.

Fuente: Entrevista realizada

Elaborado por: Reny Perez

ANALISIS

La Fiscalía identifica la adaptación al entorno digital y la falta de recursos especializados como los principales retos en la lucha contra los delitos en las redes sociales. Las medidas adoptadas incluyen la formación del personal, la creación de unidades de ciberseguridad y la colaboración internacional. Aunque no se han identificado redes criminales organizadas en Cayambe, se destaca la importancia de protocolos específicos para el manejo de pruebas digitales y la necesidad de concienciar a la población sobre los riesgos online.

3.1.8 Entrevista N.º. 8

Tabla *9*

Entrevista N. º8 a fiscales de Cayambe

ENTREVISTA A FISCALES DE CAYAMBE	
NOMBRE DEL ENTREVISTADO: ENTREVISTADO 2	
FECHA DE LA ENTREVISTA: 8 de julio del 2024	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Qué desafíos enfrentan las autoridades judiciales en Cayambe para investigar y procesar este tipo de delitos que se cometen en el ámbito digital?	Los desafíos como tal se ven reflejados al momento de la investigación, obtener la acumulación de medios probatorios que puedan atenuar a la conducta del posible actor y procesar como esta conducta se adecua a la norma vigente en el ámbito digital, como la estafa y la apropiación fraudulenta en redes sociales. Algunos de estos desafíos y cabe resaltar la falta de recursos tecnológicos especializados, la complejidad para rastrear a los perpetradores en línea, la necesidad de contar con personal capacitado en ciberseguridad y tecnologías digitales, y la coordinación con otras entidades nacionales e internacionales para combatir estos delitos transfronterizos.
PREGUNTA 2: ¿Qué medida se están tomando para	Para combatir los delitos de estafa y apropiación fraudulenta en redes sociales, se están implementando

combatir los delitos de estafa y apropiación fraudulenta en las redes sociales?	medidas como la capacitación del personal encargado de investigar estos delitos en el ámbito digital, la creación de unidades especializadas en ciberseguridad, la colaboración con empresas tecnológicas para identificar y bloquear cuentas fraudulentas, y la sensibilización pública sobre los riesgos asociados con las actividades delictivas en línea.
PREGUNTA 3: ¿Se han identificado redes criminales o grupos organizados que operen en Cayambe y se dediquen a la comisión de este tipo de delitos en las redes sociales?	Hasta la fecha de la entrevista, no se ha confirmado la identificación de redes criminales o grupos organizados que se dediquen a la comisión de delitos de estafa y apropiación fraudulenta en redes sociales en Cayambe. Sin embargo, es importante que las investigaciones y monitoreos sobre posibles actividades delictivas en línea para identificar y desarticular posibles redes criminales.
PREGUNTA 4: ¿Existen protocolos específicos para manejar la evidencia digital?	Sí, existen protocolos específicos para manejar la evidencia digital en casos de delitos en redes sociales. Estos protocolos incluyen una guía de procedimientos para la gestión de pruebas digitales y entornos informáticos, que sigue las directrices y normas contempladas en el Código Orgánico Integral Penal (COIP) sobre los procedimientos para la recolección, preservación y presentación de evidencia digital de manera que garantice su integridad y autenticidad en el proceso judicial,
PREGUNTA 5: ¿Se ha observado un incremento en el número de casos de estafa y apropiación fraudulenta a través de redes sociales en los últimos años?	Si, principalmente por el mal uso de las redes sociales. Por el famosos mercado libre de Facebook.
PREGUNTA 6: ¿Cómo pueden los ciudadanos identificar una	Es importante que estemos alerta en las redes sociales para detectar posibles estafas o engaños, prestando

posible estafa o intento de apropiación fraudulenta en redes sociales?	atención a indicios como ofertas que parecen demasiado buenas, solicitudes de datos personales delicados, falta de información confiable sobre quienes hacen las ofertas, entre otros. Antes de proporcionar datos personales o realizar compras en línea, es crucial verificar la legitimidad de las fuentes y compañías implicadas.

Fuente: Entrevista realizada

Elaborado por: Reny Perez

ANALISIS

La dificultad de obtener pruebas digitales y la necesidad de recursos especializados son mencionados por el segundo fiscal entrevistado. Destaca las acciones llevadas a cabo, como la impartición de capacitación y la colaboración con compañías de tecnología para bloquear cuentas fraudulentas. Menciona un aumento significativo en los casos de estafa y apropiación fraudulenta durante la pandemia, particularmente en Facebook. Resalta la importancia de que los ciudadanos se eduquen y se protejan para identificar y evitar posibles estafas en redes sociales.

Este análisis destaca la urgencia de actualizar la legislación, mejorar la capacitación de los profesionales del derecho y aumentar la educación pública sobre los riesgos y precauciones en el entorno digital.

3.2 Casos de estafa y apropiación fraudulenta en la ciudad de Cayambe 2022-2023.

A continuación, se analizan los datos proporcionados por el Sistema Integrado de Actuaciones Fiscales (SIAF) y la Fiscalía General del Estado (FGE) respecto a los delitos de estafa y apropiación fraudulenta en la ciudad de Cayambe durante los años 2022 y 2023.

Tabla 10.

Datos generales: Delito de estafa 2022-2023

AÑOS DE REGISTRO			
CUIDAD		**CAYAMBE**	**TOTAL**
AÑO	**2022**	**2023**	
CONSUMADO	115	142	257

TENTATIVO	1	1	2
TOTAL GENERAL			259

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE

Elaborado por: Reny Pérez

Análisis

El análisis de los datos presentados en el cuadro sobre el delito de estafa en la ciudad de Cayambe para los años 2022 y 2023 muestra un notable incremento en la incidencia de estos delitos. En el año 2022 se registraron 115 casos consumados, mientras que en el año 2023 esta cifra aumentó a 142, lo que refleja un incremento del 23,5%. Este significativo incremento pone de manifiesto el creciente problema de las estafas en esta localidad. Además, se observa que el número de tentativas de estafa, clasificadas como intentos, se mantuvo constante en ambos años con un caso cada año. Esta estabilidad en los intentos fallidos sugiere una persistencia en las estrategias de estafa, aunque con eficacia variable.

En total, sumando los casos consumados y las tentativas, se registraron 259 incidentes de estafa en el periodo 2022-2023. La mayoría de estos incidentes son estafas consumadas, que representan el 99,2% de todos los casos. Esta elevada proporción de estafas consumadas indica la necesidad urgente de reforzar las medidas de prevención y control para reducir la eficacia de las tácticas de los estafadores. Los datos obtenidos del Sistema Integrado de Actuaciones Fiscales (SIAF) y analizados por la Fiscalía General del Estado (FGE) subrayan la importancia de una intervención coordinada entre las autoridades locales y la comunidad para hacer frente a esta tendencia al alza y proteger a los ciudadanos de Cayambe.

Tabla 11.

Datos generales: Delito de apropiación fraudulenta 2022-2023

AÑOS DE REGISTRO			
CUIDAD		**CAYAMBE**	**TOTAL**
AÑO	**2022**	**2023**	
CONSUMADO	10	12	22
TENTATIVO	0	0	0
TOTAL GENERAL			22

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE

Elaborado por: Reny Pérez

Análisis

El análisis de los datos sobre el delito de apropiación indebida en Cayambe para los años 2022 y 2023 muestra una leve variación en los casos registrados. En 2022 se documentaron 10 casos consumados, mientras que en 2023 la cifra aumentó a 12, lo que representa un incremento del 20%. Es significativo señalar que no se registraron casos provisionales en ninguno de los dos años, lo que sugiere que todas las denuncias de apropiación indebida en este periodo se consumaron realmente. Esta pauta puede indicar que los casos de tentativa de apropiación indebida fraudulenta no se denuncian o que, cuando se intentan, suelen consumarse con éxito.

El número total de casos registrados en el periodo 2022-2023 asciende a 22, con una distribución uniforme entre los dos años. La constancia en las cifras pone de manifiesto la necesidad de mantener la vigilancia y adoptar medidas preventivas eficaces para hacer frente a este tipo de delitos. Los datos facilitados por el Sistema Integrado de Actuaciones Fiscales (SIAF) y analizados por la Fiscalía General del Estado (FGE) ponen de manifiesto la importancia de poner en marcha estrategias de concienciación y control para reducir la incidencia de la apropiación indebida. Es fundamental que las autoridades y la comunidad trabajen conjuntamente para identificar y mitigar las causas subyacentes que facilitan la comisión de estos delitos, protegiendo así a los ciudadanos.

Tabla 12.

Datos específicos: Delito de apropiación fraudulenta 2022-2023

Fase Pre Procesal Y Fase Procesal	
Investigación Previa	17
Archivo Aceptado	1
Archivo Solicitado	4
Sentencia Condenatoria	0
Total General	22

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE

Elaborado por: Reny Pérez

Análisis

El análisis de los datos específicos del delito de apropiación indebida en Cayambe para el periodo 2022-2023 revela un predominio de casos en etapa de investigación previa. De los 22 casos registrados, 17 se encuentran en esta etapa, lo que representa el 77,3% del total. Este alto porcentaje indica que la mayoría de los casos de apropiación fraudulenta aún se encuentran en proceso de recolección de evidencias y análisis inicial por parte de las autoridades. Sólo un caso se ha cerrado, lo que sugiere una resolución en esta fase, mientras que otros cuatro casos han solicitado el cierre, lo que representa el 22,7% de los casos que no avanzaron a una fase procesal más definitiva.

Además, cabe destacar que no se ha dictado ninguna condena en relación con casos de apropiación fraudulenta durante este periodo. Esta ausencia de condenas puede indicar dificultades en la fase de enjuiciamiento judicial, ya sea debido a la falta de pruebas suficientes, a la complejidad de los casos o a otros factores jurídicos y administrativos. La información suministrada por el Sistema Integrado de Actuaciones Fiscales (SIAF) y la Fiscalía General de la Nación (FGE) resalta la importancia de fortalecer los mecanismos de investigación y judicialización para mejorar la eficiencia y eficacia en la resolución de estos delitos. Es crucial que se implementen estrategias adicionales para agilizar las investigaciones y asegurar que los responsables de la apropiación fraudulenta enfrenten procesos judiciales.

Tabla 13.

Datos generales: Delito de estafa 2022-2023

Fase Pre Procesal Y Fase Procesal	
Investigación Previa	250
Archivo Aceptado	7
Archivo Solicitado	1
Sentencia Condenatoria	1
Total General	259

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE

Elaborado por: Reny Pérez

Análisis

El análisis de los datos sobre el delito de estafa en Cayambe para los años 2022 y 2023 revela un predominio abrumador de casos en fase de preinvestigación. De los 259 casos denunciados, 250 se encuentran en esta fase, lo que representa el 96,5% del total. Este elevado porcentaje sugiere que la mayoría de las denuncias se encuentran aún en fase de examen y análisis inicial por parte de las autoridades, lo que refleja la complejidad y la cantidad de recursos necesarios para avanzar en estos procesos. Sólo siete casos han sido archivados con éxito, mientras que uno ha solicitado su archivo, lo que indica que una pequeña fracción de los casos alcanzan una resolución en una fase temprana del proceso judicial.

En cuanto a las condenas, sólo un caso ha dado lugar a una condena, lo que representa un escaso 0,4% del total. Esta baja tasa de condenas podría apuntar a importantes problemas en la obtención de pruebas suficientes o en la eficacia del proceso judicial para estos delitos. Los datos proporcionados por el Sistema Integrado de Actuaciones Fiscales (SIAF) y analizados por la Fiscalía General del Estado (FGE) ponen de manifiesto la urgente necesidad de optimizar los procedimientos de investigación y judiciales para mejorar la resolución de los casos de fraude. Es esencial implementar estrategias adicionales para agilizar las investigaciones y fortalecer la capacidad de las instituciones judiciales para gestionar eficazmente el alto volumen de casos, garantizando así una justicia más rápida y eficiente para las víctimas de fraude en Cayambe.

3.3 Análisis general.

El documento presenta un análisis detallado de los delitos de estafa y apropiación fraudulenta cometidos a través de redes sociales en la ciudad de Cayambe durante los años 2022 y 2023. Mediante una combinación de datos estadísticos y entrevistas con actores clave del sistema judicial y de seguridad, se ofrece una visión detallada y crítica sobre la prevalencia, las características y los desafíos asociados a estos delitos en el entorno digital.

En primer lugar, los datos estadísticos revelan un aumento significativo en la incidencia de estos delitos en el período estudiado. La comparación entre los años 2022 y 2023 muestra un incremento notable en los casos de estafa consumada, que pasan de 115 a 142, y en los casos de apropiación fraudulenta, que aumentan de 10 a 12. Este aumento refleja una tendencia preocupante y subraya la necesidad de implementar medidas más efectivas de prevención y control. La alta proporción de casos en fase de investigación previa indica que gran parte de

las denuncias aún se encuentran en etapas tempranas del proceso judicial, lo que pone de manifiesto la complejidad y los recursos necesarios para avanzar en estas investigaciones.

El documento también incluye entrevistas con abogados, jueces y personal de la policía judicial, quienes proporcionan perspectivas valiosas sobre los desafíos a los que se enfrentan en la lucha contra estos delitos. Los entrevistados coinciden en la necesidad de actualizar la legislación para adaptarla a las nuevas modalidades delictivas facilitadas por las tecnologías digitales. La falta de normativa específica y de recursos tecnológicos adecuados son obstáculos recurrentes que dificultan la persecución y resolución efectiva de estos delitos. Además, se destaca la importancia de la formación continua de los profesionales del derecho y la implementación de protocolos específicos para el manejo de pruebas digitales.

Las entrevistas reflejan también la percepción de que todos los sectores de la población son vulnerables a los delitos informáticos, aunque se identifica a las personas con menor educación digital como las más susceptibles. Esto subraya la necesidad de campañas de concienciación y educación pública para informar a la ciudadanía sobre los riesgos y las medidas preventivas que pueden adoptar para protegerse. La colaboración internacional y la cooperación con empresas tecnológicas se mencionan también como estrategias cruciales para combatir los delitos transnacionales y mejorar la eficacia de las investigaciones.

En conclusión, el documento pone de relieve la creciente amenaza de los delitos de estafa y apropiación fraudulenta en redes sociales en Cayambe y la necesidad de adoptar un enfoque multifacético para abordarlos. La combinación de medidas legislativas, educativas y tecnológicas, junto con la cooperación internacional, se presenta como la estrategia más efectiva para hacer frente a este desafío. Los hallazgos y recomendaciones del documento son esenciales para guiar las políticas públicas y las acciones de las autoridades locales y nacionales en la lucha contra la ciberdelincuencia.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES.

4.1 Conclusiones.

Aumento de los delitos de fraude: El análisis de los datos muestra un aumento significativo de los casos de estafa consumada en Cayambe entre 2022 y 2023. Este aumento, de 115 casos en 2022 a 142 en 2023, refleja una tendencia preocupante en la incidencia de este tipo de delitos. La estabilidad en el número de intentos de estafa sugiere que las tácticas empleadas han mejorado en su eficacia, lo que subraya la urgente necesidad de medidas preventivas más eficaces.

La mayoría de los casos, tanto de estafa como de apropiación indebida, se encuentran en fase de investigación preliminar. Esto indica que las autoridades aún están en proceso de recopilación y análisis de pruebas, lo que puede prolongar la resolución de los casos. La elevada proporción de casos en esta fase pone de manifiesto la complejidad del proceso de investigación y la necesidad de recursos adicionales para agilizar las investigaciones y mejorar la eficiencia judicial.

Ausencia de condenas en casos de apropiación fraudulenta no se han dictado condenas por casos de apropiación fraudulenta durante el periodo estudiado. Esta falta de condenas podría deberse a la dificultad de obtener pruebas suficientes o a la complejidad inherente a estos casos. La ausencia de resultados judiciales concretos subraya la necesidad de mejorar los procedimientos judiciales y reforzar la capacidad de las autoridades para llevar estos casos a buen término.

Las entrevistas con expertos y el análisis de los datos sugieren que la normativa actual no es suficiente para abordar adecuadamente los delitos cometidos a través de las redes sociales. Es crucial adaptar la legislación a las realidades tecnológicas modernas, incorporando nuevas categorías de delitos y procedimientos específicos para el manejo de pruebas digitales. Esto permitirá dar una respuesta más eficaz a los retos que plantea la ciberdelincuencia.

La vulnerabilidad del público ante los delitos de fraude y apropiación indebida a través de las redes sociales se ve agravada por la falta de educación y concienciación. Es esencial poner en marcha campañas educativas que informen a los ciudadanos sobre los riesgos asociados al uso de las redes sociales y las medidas preventivas que pueden adoptar para protegerse. La

colaboración entre instituciones educativas, tecnológicas y gubernamentales es esencial para aumentar la resiliencia de la comunidad ante estos delitos.

Jueces y fiscales se enfrentan a importantes retos a la hora de representar y enjuiciar casos de ciberdelincuencia, principalmente debido a la falta de formación específica y de recursos tecnológicos adecuados. Implantar programas de formación continua para el personal judicial e invertir en tecnologías avanzadas de ciberseguridad son pasos cruciales para mejorar la capacidad de respuesta del sistema judicial. Además, la cooperación internacional es esencial para gestionar la naturaleza transfronteriza de muchos de estos delitos.

4.2 Recomendaciones

Es esencial incrementar la formación de los funcionarios judiciales y policiales en ciberseguridad y manejo de evidencias digitales. La formación continua permitirá a los investigadores y jueces hacer frente de manera más efectiva a los desafíos asociados con los delitos de estafa y apropiación fraudulenta a través de las redes sociales. Invertir en programas de capacitación especializados ayudará a mejorar las competencias técnicas del personal, garantizando así un manejo adecuado de las pruebas digitales y una mayor eficacia en la persecución de estos delitos.

Es imperativo revisar y actualizar la legislación vigente para adaptarla a las nuevas modalidades delictivas que surgen con el uso de las tecnologías digitales. La incorporación de normas específicas sobre delitos cometidos en redes sociales permitirá una mejor tipificación de estos crímenes y facilitará la labor de las autoridades judiciales. Una legislación actualizada y sólida será esencial para cerrar los vacíos legales y garantizar que los delincuentes enfrenten sanciones adecuadas por sus actos.

Desarrollar y adoptar procedimientos específicos para la gestión de la evidencia digital es crucial para asegurar la integridad y autenticidad de las pruebas durante todo el proceso judicial. Estos protocolos deben incluir directrices claras sobre la recolección, la preservación y la presentación de evidencias digitales, a fin de garantizar que se mantengan intactas desde su obtención hasta su uso en el tribunal. La correcta implementación de estos protocolos contribuirá a fortalecer los casos presentados ante la justicia.

Es vital lanzar campañas educativas dirigidas a la población sobre los riesgos de las estafas y apropiaciones fraudulentas en redes sociales para prevenir estos delitos. Estas campañas deben proporcionar información práctica sobre cómo identificar y evitar posibles fraudes, y destacar

la importancia de proteger los datos personales y verificar la autenticidad de las transacciones en línea. Una población bien informada será menos susceptible de ser víctima de estos delitos.

Dado el carácter transnacional de muchos delitos informáticos, es esencial fortalecer la cooperación entre las autoridades ecuatorianas y las agencias internacionales. El establecimiento de acuerdos de colaboración y mecanismos de asistencia mutua permitirá una respuesta más rápida y eficaz frente a los delitos cometidos desde el extranjero. La cooperación internacional facilitará la obtención de pruebas y la persecución de delincuentes que operan fuera de las fronteras nacionales.

Invertir en el desarrollo y adquisición de herramientas tecnológicas avanzadas para la detección y prevención de fraudes en redes sociales es crucial. Dichas herramientas deben incluir software de análisis de datos, sistemas de monitoreo en tiempo real y plataformas de alerta temprana que permitan identificar actividades sospechosas de manera proactiva. La aplicación de estas tecnologías mejorará significativamente la capacidad de respuesta de las autoridades ante la creciente amenaza de los delitos informáticos.

ANEXOS

Cuestionario 1

NOMBRE DEL ENTREVISTADO:	
FECHA DE LA ENTREVISTA:	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Considera que las redes sociales representan un problema grave en la sociedad actual? ¿Por qué o por qué no?	
PREGUNTA 2: ¿En su experiencia, ¿cuáles son los sectores o grupos de población más vulnerables a este tipo de delitos?	
PREGUNTA 3: ¿Qué medidas o reformas al sistema legal consideraría necesarias para combatir estos delitos de manera más efectiva?	
PREGUNTA 4: ¿Cuáles serían los principales desafíos que enfrentan los abogados en la representación de víctimas o acusados de estos delitos?	
PREGUNTA 5: ¿Ha tenido alguna experiencia personal o profesional relevante con casos de estafa o apropiación fraudulenta?	

Cuestionario 2

NOMBRE DEL ENTREVISTADO:	
FECHA DE LA ENTREVISTA:	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Cuáles son las principales plataformas de redes sociales más utilizadas para cometer estos delitos en Cayambe?	
PREGUNTA 2: Cuáles son los métodos más comunes utilizados por los estafadores para cometer estos delitos en Cayambe a través de las redes sociales?	
PREGUNTA 3: ¿Han observado algún patrón o tendencia en cuanto al modus operandi de los estafadores que operan en Cayambe a través de las redes sociales?	
PREGUNTA 4: ¿Qué medidas de prevención considera que se deberían implementar para reducir la incidencia de estos delitos en Cayambe?	
PREGUNTA 5: ¿cuenta con las herramientas o con los recursos tecnológicos adecuadas para	

rastrear y localizar a las personas que comente estos delitos?	
PREGUNTA 6: Considera usted que el mercado libre o mayormente conocido como Marketplace es el sitio donde ocurre más estos delitos	

Cuestionario 3

NOMBRE DEL ENTREVISTADO:	
FECHA DE LA ENTREVISTA:	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿En qué consiste el delito de apropiación fraudulenta y en qué se diferencia de la estafa?	
PREGUNTA 2: ¿Durante su trayectoria como administrador de justicia cuál cree que es el principal desafío que enfrentan los jueces al abordar casos de estafa y apropiación fraudulenta cometidos a través de redes sociales?	
PREGUNTA 3: cuando no se detecta al actor de estos delitos ¿Qué papel juegan las declaraciones de las víctimas?	

PREGUNTA 4: ¿En el año 2022-2023 cuantos casos de estafa y apropiación fraudulenta tuvieron una sentencia?	
PREGUNTA 5: ¿Considera que la normativa actual en el Ecuador es suficiente para abordar adecuadamente los delitos de estafa y apropiación fraudulenta en las redes sociales?	
PREGUNTA 6: ¿Cómo se han adaptado las leyes y la jurisprudencia para abordar los nuevos retos que presenta la comisión de estos delitos en el entorno digital?	
PREGUNTA 7: Existen mecanismos adecuados para garantizar la reparación del daño y la restitución de los bienes a las víctimas de estos delitos?	
PREGUNTA 8: ¿Qué medidas cautelares pueden solicitar las víctimas o las autoridades para proteger sus derechos durante el proceso penal?	
PREGUNTA 9: Se toman en cuenta factores agravantes o atenuantes al momento de determinar la pena aplicable en cada caso?	

PREGUNTA 10: Podría mencionar algunos precedentes jurisprudenciales relevantes en Ecuador relacionados con los delitos de estafa y apropiación fraudulenta en el ámbito de las redes sociales?	

Cuestionario 4

NOMBRE DEL ENTREVISTADO:	
FECHA DE LA ENTREVISTA:	
CUESTIONARIO DE PREGUNTAS:	
PREGUNTA 1: ¿Qué desafíos enfrentan las autoridades judiciales en Cayambe para investigar y procesar este tipo de delitos que se cometen en el ámbito digital?	
PREGUNTA 2: ¿Qué medida se están tomando para combatir los delitos de estafa y apropiación fraudulenta en las redes sociales?	
PREGUNTA 3: ¿Se han identificado redes criminales o grupos organizados que operen en Cayambe y se dediquen a la	

comisión de este tipo de delitos en las redes sociales?	
PREGUNTA 4: ¿Existen protocolos específicos para manejar la evidencia digital?	
PREGUNTA 5: ¿Se ha observado un incremento en el número de casos de estafa y apropiación fraudulenta a través de redes sociales en los últimos años?	
PREGUNTA 6: ¿Cómo pueden los ciudadanos identificar una posible estafa o intento de apropiación fraudulenta en redes sociales?	

REFERENCIAS BIBLIOGRÁFICAS.

Acosta, J. (2024). *Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa-2022.* Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/138107

Agazzi, E. (2020). *Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them.* Obtenido de https://arxiv.org/abs/2006.00577

Aguirre, S. (2022). *El delito de apropiación fraudulenta por medios electrónicos y la responsabilidad de las personas jurídicas en el cantón Ibarra en el año 2021.* Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/15528

Armijos, Y. (2023). *El delito de estafa en redes sociales y el impacto en la sociedad ecuatoriana.* Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/16548

Baig, S., Ahmed, E., & Memon, A. (2021). *Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted. .* Obtenido de 4th International Conference on Computing & Information Sciences (ICCIS): https://ieeexplore.ieee.org/abstract/document/9676394/

Bravo, D., & Ordóñez, S. (2021). *Impacto de las redes sociales digitales como estrategia de marketing en el negocio de las Pymes del municipio de Pasto.* Obtenido de http://expeditiorepositorio.utadeo.edu.co/handle/20.500.12010/18661

Cabrera, K., & Jiménez, C. (2021). La cultura de la cancelación en redes sociales: Un reproche peligroso e injusto a la luz de los principios del derecho penal. *Revista chilena de derecho y tecnología, 10*(2), 277-300. doi:10.5354/0719-2584.2021.60421

Cañas, O. (2021). *Criterios útiles de la teoría de la oportunidad para la prevención del delito de en la licitación pública: con énfasis en la municipalidad.* Obtenido de https://oldri.ues.edu.sv/id/eprint/25005/

Cárdenas, D., Ropero, E., Puerto, K., Sánchez, K., Ramírez, J., & Castro, S. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo Fesc, 10*(19), 162-179. Obtenido de https://repositorio.ufps.edu.co/handle/ufps/940

Cárdenas, X., Rosero, E., Holovatyi, M., & Pazos, P. (2020). El impacto de las redes sociales en la administración de las empresas. *RECIMUNDO, 4*(1), 173-182. doi:10.26820/recimundo/4.(1).enero.2020.173-182

Carvajas, E., & Estrada, L. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. *Revista jurídica critica y derecho, 1*(1), 49-60. doi:10.29166/criticayderecho.v1i1.2447

Chacón, L. (27 de Oct de 2021). *Un débil control en ventas es una oportunidad de fraude.* Obtenido de universidad Militar Nueva Granada : https://repository.unimilitar.edu.co/handle/10654/39933

Chapi, J., Chulde, A., Bracero, S., & Moreno, J. (2024). La estafa electrónica en el Sistema Penal Ecuatoriano. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 9*(1), 336-345. doi:10.35381/racji.v9i1.3581

Chaverra, S., & Celis, D. (2022). El modelo Medellín y su enfoque de los problemas de seguridad: urbanismo social y prevención situacional del delito, 2008-2015. *Memorias Forenses*(5), 29-47. doi:10.53995/25390147.892

Chuco, E. (2023). *Análisis del delito de fraude informático y hurto como delito previo, Cercado de Lima-2020.* Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/125058

Cisneros, C., & Jiménez, R. (2021). El delito de estafa: naturaleza, elementos y consumación. *El delito de estafa: naturaleza, elementos y consumación., 8*(SPE4), 1-18. doi:10.46377/dilemas.v8i.2794

Código Orgánico Integral Penal, COIP. (17 de Feb de 2021). Obtenido de REPÚBLICA DEL ECUADOR ASAMBLEA NACIONAL: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Contreras, F., & Marín, A. (2022). La visualidad algorítmica: una aproximación social a la visión artificial en la era post internet. *Arte, individuo y sociedad*, *34*(4), 627-647. doi:10.5209/aris.74664

Dean, B. (21 de Feb de 2024). *Social Media Usage & Growth Statistics*. Obtenido de BackLinko: https://backlinko.com/social-media-users

Delgadillo, A., Avalos, D., & Ávila, Q. (2022). Un análisis a las teorías crimino-ambientales bajo la incidencia delictiva en García, Nuevo León. *Constructos Criminológicos, 2*(2), 67-86. doi:10.29105/cc2.2-13

Di Angellis, G. (2021). *Estudio criminológico de la corrupción desde la teoría de la oportunidad.* Obtenido de https://digibug.ugr.es/handle/10481/71620

Espinoza, I. (2021). *Redes sociales y la vulneración de los derechos constitucionales.* Editorial Ebooks. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=NXpWEAAAQBAJ&oi=fnd&pg=PA5&dq=delitos+en+redes+sociales+Relevancia+jurídica+y+social+&ots=8Pscvuqox2&sig=Ls_K3cWk9aPME7IB0h4IlMN9VMk&redir_esc=y#v=onepage&q&f=false

Fernández, I., & García, S. (2020). Redes sociales, convergencia y narrativas transmedia en la promoción de las Islas Canarias. . *Ámbitos. Revista Internacional de Comunicación*(48), 148-170. doi:10.12795/Ambitos.2020.i48.08

Fernández, L. (2020). Protección social para los trabajadores de la economía de plataforma: propuestas para aliviar su vulnerabilidad. *Revista General de Derecho del Trabajo y Seguridad Social, 57*. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/78901568/RODRIGUEZ_FERNANDEZ-libre.pdf?1642356024=&response-content-disposition=inline%3B+filename%3DProteccion_social_para_los_trabajadores.pdf&Expires=1719531664&Signature=JSu1Vb5RIx4eg93lsN8OUPJaDVRlzOuPE8YdrFkUwdj

Galindo, M. (2024). Suplantación de identidad digital: Hacia una necesaria tutela penal. *Estudios de Deusto: revista de Derecho Público, 72*(1), 199-228. doi:10.18543/ed7112024

García, A., & Pesantez, A. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectivas, 5*(1), 19-29. doi:10.47187/perspectivas.5.1.179

Garzón, F., Urrego, M., & Ocampo, A. (2023). *Análisis de los delitos financieros juzgados en el escenario internacional.* Obtenido de https://repository.ucc.edu.co/entities/publication/63d11e59-0c3d-4f35-bfdb-4f737aa27647

Gil, A. (2020). *UNA INVESTIGACIÓN SOBRE FRAUDE FISCAL.* Obtenido de https://zaguan.unizar.es/record/101756#

Gozáles, V., & Cortijo, G. (2023). Desarrollo humano y redes sociales en sociedades digitales. *ophia, colección de Filosofía de la Educación*(34), 41-64. doi:10.17163/soph.n34.2023.01

Guijarro, S., Casado, C., & Mayorga, D. (2021). Aplicación de las redes sociales en la enseñanza universitaria: Evolución temporal. *CIVINEDU 2021*, 70-73. Obtenido de https://www.researchgate.net/profile/Joaquin-Fuentes-Del-Burgo/publication/356527015_Promocion_de_las_STEM_El_curso_de_verano_Taller_de_Construccion_Sostenible/links/619f4ff607be5f31b7b645a2/Promocion-de-las-STEM-El-curso-de-verano-Taller-de-Construccion-

Gutiérrez, A., García, A., Alcívar, L., & Chancay, X. (2023). Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador. *Polo del Conocimiento: Revista científico-profesional, 8*(5), 1137-1153. doi:10.23857/pc.v8i5

Ibarra, H. (2021). *Autopuesta en peligro como supuesto excluyente de tipicidad en el delito de estafa.* Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/13761

Kemp, S. (31 de Ene de 2024). *5 BILLION SOCIAL MEDIA USERS*. Obtenido de DataReportal – Global Digital Insights: https://datareportal.com/reports/digital-2024-deep-dive-5-billion-social-media-users

Lardies, F., & Potes, V. (2022). Redes sociales e identidad:¿ desafío adolescente? *Avances en Psicología, 30*(1), e2528. doi:10.33539/avpsicol.2022.v30n1.2528

Layton, J. (2020). *Evolución e importancia de las redes sociales en el fútbol femenino tinerfeño.* Obtenido de https://riull.ull.es/xmlui/bitstream/handle/915/21393/Evolucion%20e%20importancia%20de%20las%20redes%20sociales%20en%20el%20futbol%20femenino%20tinerfeno.pdf

Macías, M. (2024). Perspectiva criminológica de la corrupción pública a través de las teorías de la criminalidad. *Derecho global. Estudios sobre derecho y justicia, 9*(26), 223-255. doi:10.32870/dgedj.v9i26.718

Mantilla, A. (2023). *Estudio y análisis del anonimato en la red: herramientas y técnicas para la maximización del anonimato.* Obtenido de https://openaccess.uoc.edu/handle/10609/148149

Matos, J. (2021). Delitos de odio y redes sociales: El derecho frente al reto de las nuevas tecnologías. *Revista de Derecho UNED*(27), 137-172. Obtenido de https://www.proquest.com/openview/8f718046239aaa54940f928e4cc56df3/1?pq-origsite=gscholar&cbl=1596356

Montenegro, M., Gutiérrez, A., Lugmaña, R., & Moreno, J. (2024). Delitos informáticos de apropiación fraudulenta por medios y transferencia electrónicos de activo patrimonial. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 9*(1), 220-229. doi:10.35381/racji.v9i1.3528

Morocho, G. (2022). *Incidencia del delito de estafa a través del uso de redes sociales, año 2017-2020, cantón La Libertad* . Obtenido de Universidad Estatal Península de Santa Elena: https://repositorio.upse.edu.ec/handle/46000/8820

Ortiz, M., & López, Y. (2024). La teoría del delito y el concepto de delito. Una visión comparada entre EEUU y Ecuador. *MQRInvestigar, 8*(2), 1406-1421. doi:10.56048/MQR20225.8.2.2024.1406-1421

Panero, E. (2021). *El anonimato en Internet: Estudio de herramientas y técnicas de anonimato.* Obtenido de https://openaccess.uoc.edu/handle/10609/138286

Parra, L., Menjura, M., Pulgarín, L., & Gutiérrez, M. (2021). Las prácticas pedagógicas. Una oportunidad para innovar en la educación. *Revista Latinoamericana de Estudios Educativos (Colombia), 17*(1), 70-94. doi:10.17151/rlee.2021.17.1.5

Roque, E. (2021). *Fundamentos jurídico-sociales para la penalización de la promoción de delitos a través de redes sociales en el código penal peruano.* Obtenido de http://publicaciones.usanpedro.edu.pe/handle/20.500.129076/15522

Ruiz, F., gonzáles, R., & Lucendo, Á. (2020). Comportamiento espacial del uso de las TIC en los hogares e individuos. Un análisis regional europeo. *Investigaciones Geográficas*(Esp), 57-74. Obtenido de https://www.redalyc.org/articulo.oa?id=17664443003

Salazar, A., & ortíz, M. (2024). Las construcciones teóricas en torno a la subcultura criminal. *593 Digital Publisher CEIT, 9*(2), 844-852. doi:10.33386/593dp.2024.2.2407

Salgado, B. (2022). *La problemática en la regulación jurídica ante la violencia cibernética en las redes sociales en el Ecuador.* Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/4683

Sanjuán, V. (2020). *Redes sociales: evolución e influencia en la sociedad española.* Obtenido de https://idus.us.es/handle/11441/105749

Sempértegui, M. (2022). *Delito de apropiación fraudulenta por medios electrónicos bajo la modalidad de phising dentro del marco jurídico ecuatoriano.* Obtenido de Universidad del Azuay: https://dspace.uazuay.edu.ec/handle/datos/12380

Tacuri, I. (2021). *Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática.* Obtenido de http://dspace.ups.edu.ec/handle/123456789/20242

Tirado, E. (2020). *Fundamentos jurídicos para incorporar las redes sociales como agravante a los delitos contra el honor en la modalidad de difamación en el Código Penal Peruano.* Obtenido de http://repositorio.upagu.edu.pe/handle/UPAGU/1429

Triana, N. (2022). *La incorporación de criptomonedas en las compañías de interés público: posibilidad de fraude financiero.* Obtenido de Universidad Nacional de Colombia: https://repositorio.unal.edu.co/handle/unal/81769

Vaca, C., Martínez, D., & Toasa, M. (2022). Análisis OSINT aplicado a la investigación de Fraudes Financieros. *Revista Ibérica de Sistemas e Tecnologias de Informação*(E49), 80-91. Obtenido de https://www.proquest.com/openview/d16347cbac65fced95b9fa3ff9951207/1?pq-origsite=gscholar&cbl=1006393

Velasquez, M. (2022). *La influencia del principio de proporcionalidad de la pena en el delito de estafa en el distrito de Los Olivos, 2020.* Obtenido de https://core.ac.uk/download/pdf/544274100.pdf

Yasin, A., Fatima, R., Jiangbin, Z., Afzal, W., & Raza, S. (2024). *Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in*

Information Security. Obtenido de Information and Software Technology: https://www.sciencedirect.com/science/article/pii/S0950584924000314

Zambrano, M. (2022). La certidumbre de la incertidumbre en los fraudes piramidales Ponzi. *Matemática, 20*(1). Obtenido de http://www.revistas.espol.edu.ec/index.php/matematica/article/view/1011