**UNIVERSIDAD TECNOLOGICA ECOTEC**

**FACULTAD:**

**DERECHO Y GOBERNABILIDAD**

**TITULO:**

“Análisis por la estafa como delito electrónico por medio de las redes sociales para determinar la posible restauración económica como medida de reparación en el Cantón Guayaquil-2020/2022”

**LINEA DE INVESTIGACIÓN**

GESTION DE LAS RELACIONES JURIDICAS

**MODALIDAD DE TITULACION:**

PROYECTO E INVESTIGACIÓN

**CARRERA:**

DERECHO CON ENFASIS EN CIENCIAS PENALES Y CRIMINOLÓGICAS

**TITULO A OBTENER:**

ABOGADA

**AUTOR:**

ESTHER NICOLLE SANI LEÓN

**TUTOR**

PAOLO DOMÍNGUEZ VÁSQUEZ

**GUAYAQUIL 2023**

## DEDICATORIA

A Dios que ha sido mi guía y fortaleza desde el inicio por este gran camino que está a punto de culminar, porque sin él en mi vida nada de esto fuera posible el día de hoy.

A mis padres, Wendy León y Christian Sani, quienes han sido mi base y refugio ante cualquier adversidad que se haya presentado, creyeron en mí desde el primer día sin poner excusas por ayudarme a alcanzar mis metas. El sacrificio y dedicación que hicieron por mí, estaré eternamente agradecida.

A mis docentes, que a la mayoría puedo llamar maestros; guiándome en todo momento hasta el día de hoy, impartiendo cada uno de sus conocimientos y experiencias en esta ardua, pero maravillosa carrera, gracias por ser parte de este gran logro.

**A TODOS USTEDES GRACIAS POR TODO**

## AGRADECIMIENTO

Mis más sinceros agradecimientos deseo otorgar a cada persona que fue partícipe durante este largo y satisfactorio camino.

En primer lugar, a Dios al brindarme vida y salud hasta el día de hoy para continuar con la meta que me tracé hace 4 años atrás y hoy en día la culmino de forma muy satisfactoria y melancólica.

A mi familia, por ser mi apoyo incondicional en cada aspecto de mi vida porque sin ellos no fuera la persona que soy hoy en día, con su amor han sido capaces de ayudarme a alcanzar cada meta que me he trazado a lo largo de mi vida.

A mi Peluchina, aunque hoy no esté conmigo en este plano terrenal agradezco por cada madrugada acompañándome esperando que termine de estudiar para cada examen; puesto que en sus ojitos se reflejaba el cansancio que tenía, jamás me dejó sola por ninguna circunstancia. Este éxito también te pertenece.

Quiero también agradecer a cada amigo que he podido hacer en el transcurso de este tiempo, han sido compañeros de corazón que me han apoyado y ayudado durante la trayectoria en la carrera de Derecho, en Ecotec realmente pude apreciar el significado de la palabra amigo, esta etapa que culmina estará conmigo encasillada en un recuerdo maravilloso lleno de alegrías, éxitos, melancolía, satisfacción y muchos sentimientos encontrados de los cuales estaré profundamente agradecida.

Gracias por haber sido parte de esta gran aventura llena de privilegios y obstáculos que después de Dios y ustedes he podido sobrellevarla con una enorme plenitud. *EBENEZER (Hasta aquí Jehová me ha ayudado)*

## CERTIFICADO DE REVISION FINAL

Universidad Ecotec

**ANEXO N°15**

**CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS**

Habiendo sido nombrado PAOLO DOMÍNGUEZ VÁSQUEZ, tutor del trabajo de titulación **"Análisis por la estafa como delito electrónico por medio de las redes sociales para determinar la posible restauración económica como medida de reparación en el Cantón Guayaquil-2020/2022"** elaborado por **ESTHER NICOLLE SANI LEÓN,** con mi respectiva supervisión como requerimiento parcial para la obtención del título de **ABOGADO.**

Se informa que el mismo ha resultado tener un porcentaje de coincidencias **10(%)** mismo que se puede verificar en el siguiente link: https://app.compilatio.net/v5/report/3b0faee04721014d71abb77c339f60e0cc80f05a/summary .

Adicional se adjunta print de pantalla de dicho resultado.


**FIRMA DEL TUTOR**
**Mgtr. Paolo Domínguez Vasquez**

Universidad Ecotec

**ANEXO N°16**

**CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL**

Samborondón, 12 de diciembre de 2023

Magíster
**Andrés Madero Poveda**
**Decano(a) de la Facultad**
**Facultad de Derecho y Gobernabilidad**
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación **"Análisis por la estafa como delito electrónico por medio de las redes sociales para determinar la posible restauración económica como medida de reparación en el Cantón Guayaquil-2020/2022"**: según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **SANI LEÓN ESTHER NICOLLE,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

**ATENTAMENTE,**

**Mgtr. Paolo Dominguez Vasquez**

**Tutor(a)**

## RESUMEN

La estafa es un acto fraudulento que engaña a personas para obtener beneficios injustos. Implica engaño, manipulación o falsedad con la intención de obtener dinero, bienes o servicios ilegítimamente. Este proyecto de investigación tiene como objetivo describir la importancia que ha traído consigo este nuevo *modus operandi* a raíz del avance tecnológico, como lo ha sido la estafa por medio de redes sociales vulnerando el bien jurídico de la víctima como lo es el patrimonio. Para esto, se ha recurrido a un método de investigación con enfoque cualitativos, de tipo descriptivo, empleando recopilación bibliográfica y entrevistas a expertos para la obtención de la información. Todo esto en conjunto permitió establecer un panorama amplio de cómo los criterios jurídicos y fundamentos normativos sustentando la estafa establecido en el Código Orgánico Integral Penal, Se destacan como resultados principales que, a pesar de que la normativa tiene como objetivo regular la imposición de la prisión preventiva en relación con tales actos delictivos, la simple presencia de la ley o sus modificaciones no basta; es necesario establecer procedimientos que garanticen la reparación total de la víctima, convirtiendo este proyecto de investigación buscar una reforma sobre el artículo donde se tipifica el delito de estafa.



**Palabras claves: estafa, COIP, bien jurídico, reparación total.**

## ABSTRACT

The Scam is a fraudulent act that deceives people to obtain unfair benefits. Involves deception, manipulation, or falsehood with the intent to obtain money, goods, or services illegitimately. This research project aims to describe the importance that this new modus operandi has brought with it as a result of technological advance, such as the scam through social networks, violating the legal rights of the victim such as assets. For this, a research method with a quantitative, descriptive approach has been used, using bibliographic compilation and interviews with experts to obtain information. All of this together allowed us to establish a broad overview of how the legal criteria and regulatory foundations supporting the fraud established in the Comprehensive Organic Penal Code. The main results stand out that, despite the fact that the regulations aim to regulate the imposition of prison preventive in relation to such criminal acts, the simple presence of the law or its amendments is not enough; It is necessary to establish procedures that guarantee full reparation to the victim, making this research project seek a reform of the article that classifies the crime of fraud.



**Keywords: scam, COIP, legal good, total reparation.**

## Índice de contenidos

## Introducción

El mundo ha tenido cambios a lo largo de los años desde el principio de sus tiempos sea en el ámbito social, económico, y el tecnológico no sería una excepción a la regla; investigar los delitos desde cualquier categoría trae consigo un desenlace complejo logrando incorporar diversos delitos en las normativas penales como lo es en el Código Orgánico Integral Penal reconocidos como delitos informáticos.

En el ámbito de la "estafa informática", el Código Penal no definió explícitamente el alcance de este delito; simplemente estableció que, en los casos de estafa perpetrada mediante medios electrónicos o telemáticos, se aplicaría la pena máxima prevista para la estafa en general. Por lo tanto, se puede inferir, siguiendo la misma normativa, que la estafa electrónica implica la apropiación indebida de bienes ajenos, ya sean muebles, obligaciones, finiquitos o recibos, llevada a cabo a través de engaños y, en el caso particular que nos ocupa, haciendo uso de medios electrónicos o telemáticos. (Padilla, La responsabilidad bancaria frente a los delitos informáticos , 2022)

Del análisis que llevo a cabo a continuación, se deduce que en el Código Orgánico Integral Penal (COIP) se han tipificado delitos informáticos con el objetivo no solo de salvaguardar los derechos fundamentales dispuestos en la Constitución y los bienes jurídicos comúnmente examinados, como el derecho a la propiedad, no solo abarcan aspectos tradicionales, sino también aspectos actuales como el derecho a la información, considerado esencial para garantizar el "derecho al bienestar".

El Dr. Diego Salamea determina que para la realización del *phishing* se han creado incluso programas como el *spyware*, centrados en obtener las contraseñas ingresadas por el usuario en su computadora, los backdoors son aplicaciones maliciosas creadas con el propósito de facilitar al atacante el acceso directo a la información almacenada en la computadora. Esto puede lograrse mediante la revisión directa de la información o mediante métodos como correos electrónicos no

deseados, mensajes de spam o solicitudes falsas de amistad. (La responsabilidad bancaria frente a los delitos informáticos , 2021)

Se observa que, aunque el internet es fácilmente accesible, su uso puede representar una amenaza no solo por las acciones de los usuarios, sino también porque los datos del usuario pueden ser recopilados por terceros. Por lo tanto, es crucial que este progreso tecnológico esté acompañado de una información adecuada, especialmente por parte de los proveedores de servicios. En el ámbito bancario, se está haciendo un esfuerzo por concienciar a los usuarios sobre los riesgos asociados con el uso de los canales electrónicos.

El propósito principal de este trabajo consiste en determinar la eficacia de los mecanismos establecidos en la legislación ecuatoriana para evaluar la completa reparación a las víctimas de delitos informáticos relacionados con estafas. Por ende, resulta esencial analizar si nuestra legislación en este ámbito dispone de las herramientas adecuadas para salvaguardar a los ciudadanos ante posibles situaciones de este tipo.

## Antecedentes

Las formas recientes de fraude se incluyen en el COIP desde el 10 de agosto de 2014, especialmente aquellas que involucran a personas que perjudican a más de dos individuos con un monto igual o superior a cincuenta salarios básicos unificados. Durante el año 2014, se presentaron 8 denuncias, y hasta el 27 de octubre de 2015, se registraron 9 casos, todos relacionados con denuncias por compra o venta pública de valores por medio de cualquiera práctica fraudulenta que implican el uso de recursos provenientes de fuentes privadas, públicas o de la seguridad social; se registraron tres reportes en el año 2015 relacionados con la manipulación, duplicación, sustracción o robo de tarjetas de crédito. Este tipo de estafas incluyen acciones como el engaño al entregar productos o servicios. Una certificación fraudulenta que aborda las actividades financieras o inversiones ejecutadas por una entidad legal, mediante transacciones ficticias relacionadas con cualquier valor, así

como la emisión de boletos o entradas para eventos en espacios públicos o de gran concurrencia que exceden el límite de capacidad autorizado por la autoridad pública correspondiente.” (FGE, 2015)

Las redes de comunicación han dado origen a nuevas manifestaciones delictivas, tanto individuales como organizadas, que representan una amenaza para la privacidad de la información, la seguridad durante la navegación y la integridad de instituciones tanto públicas como privadas. En el marco del Código Orgánico Integral Penal (COIP), se imponen sanciones a los delitos informáticos, los cuales emplean tecnología para vulnerar la confidencialidad y la disponibilidad de datos personales. Entre las conductas ilícitas que se manifiestan a través de la Internet, se incluyen acciones como el fraude, robo, falsificación, suplantación de identidad, espionaje y clonación de tarjetas de crédito, entre otras. (Altamirano)

Las redes de comunicación ocasiona nuevas formas de delincuencia, tanto común como organizada, que representan una amenaza para la información privada, la seguridad durante la navegación y la integridad de instituciones tanto públicas como privadas. En el Código Orgánico Integral Penal (COIP), se imponen sanciones específicas para los delitos informáticos, los cuales emplean tecnología para vulnerar la confidencialidad y disponibilidad de datos personales. Entre los actos perpetrados a través de Internet se incluyen el fraude, robo, falsificación, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros. (Pena máxima aplicada en los tipos delictivos, 2015)

La legislación ecuatoriana también menciona en su codificación penal acerca de la transferencia electrónica de bienes patrimoniales en la que una persona, con el objetivo de obtener beneficios económicos, altere, manipule o modifique el funcionamiento de un programa, sistema informático, telemático o mensaje de datos para lograr la transferencia o apropiación no autorizada de un activo patrimonial perteneciente a otra persona, causándole perjuicio a ella o a un tercero, será castigada con una pena de prisión de tres a cinco años. De manera similar, se impondrá la misma pena a aquella persona que, con la intención de obtener, recibir o captar de manera ilícita un activo patrimonial a través de una transferencia electrónica resultante de dicho delito, facilite o proporcione datos de su cuenta bancaria, ya sea

para su propio beneficio o para el de otra persona.” (COIP, 2015, Art. 231). (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

Es esencial comprender que en el ámbito de los delitos informáticos, el Código Orgánico Integral Penal (COIP) establece que aquel individuo que acceda sin autorización, total o parcialmente, a un sistema informático y lo retenga contra la voluntad del legítimo propietario, con el propósito de utilizar de manera ilícita el acceso obtenido, modificar un sitio web, desviar o redirigir el flujo de datos o voz, o suministrar servicios que estos sistemas ofrecen a terceros sin remunerar a los proveedores de servicios legítimos, se verá sujeto a una pena de privación de libertad que varía entre tres y cinco años. (COIP, 2015, Art. 234). (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

El delito de estafa, con sus diversas formas y variantes, ofrece la oportunidad de analizar y comprender cómo el ámbito legal penal ha debido ajustarse continuamente a los cambios en la sociedad. En algunos países, este delito se complementa con figuras legales especiales diseñadas para salvaguardar el patrimonio público. Además, la presentación de información falsa y sus derivados se ha dirigido hacia la protección de inversiones de capital y la concesión de préstamos por parte de las instituciones financieras, como en el caso de estafas mediante cheques o acuerdos anticompetitivos. Siguiendo la misma línea de pensamiento, en Ecuador, el delito de estafa se encontraba dentro del capítulo V del Código Penal, titulado "De las estafas y otras defraudaciones", e incluía varios tipos delictivos como la estafa, el engaño al consumidor, el abuso de confianza, la receptación, entre otros, donde el bien jurídico protegido estaba claramente definido como la propiedad. Es fundamental resaltar la importancia de determinar el bien jurídico protegido, ya que su definición es crucial para el desarrollo y la evolución del tipo penal. (Crespo, El delito de estafa en el Código Orgánico Integral Penal., 2021)

A partir de la disposición habitual del antiguo Código Penal, resulta evidente que no abarcaba diversas formas delictivas que en la actualidad son consideradas esenciales por numerosas legislaciones en el mundo, entre ellas el vigente Código Orgánico Integral Penal de Ecuador. Este último no solo ha decidido ampliar las modalidades de estafa, sino que también ha introducido la responsabilidad penal de las personas jurídicas en este tipo de delitos. En este artículo, se buscará examinar

la tipificación de la estafa según el Código Orgánico Integral Penal, las opiniones doctrinales acerca de los elementos del delito, así como las diversas modalidades que impactan a los actores económicos y al mercado, dando lugar a la imposición de responsabilidad penal a las entidades jurídicas. (Crespo, Análisis del tipo penal y las reformas del 2019)

Conceptualmente, el delito de estafa se define como aquellas conductas que tienen como común denominador producir un perjuicio patrimonial mediante una conducta engañosa, en otras palabras, se puede entender como todo acto doloso, que producto de un engaño produce o busca producir un perjuicio en el patrimonio de un tercero. De la definición anterior se deduce que el bien jurídico protegido en el delito de estafa es el patrimonio ajeno en cualquiera de los elementos integrantes de éste, ya sean bienes muebles o inmuebles, derechos, dinero, representación de capitales, que puedan constituir el objeto material del delito. Sin embargo, hay autores que consideran que este concepto es únicamente aplicable siempre que medien los elementos esenciales de la estafa general o común, estos son: engaño, error y disposición del patrimonio. Además, su desarrollo debe continuar obligatoriamente en el ámbito doctrinario y de la jurisprudencia, sin pretender nunca una definición legal. (Crespo, Análisis del tipo penal y las reformas del 2019)

En nuestro código, se observa la noción de patrimonio como un bien legalmente resguardado, con un alcance amplio y significativo en el contexto del derecho penal económico. Esto se debe a que busca salvaguardar contra diversas formas de conducta dolosa y fraudulenta que podrían tener consecuencias adversas para la economía en general, incluyendo el patrimonio a nivel personal. (Casillas, 2022)

Otro aspecto debatido en relación con el concepto de patrimonio, que ha adquirido considerable importancia, es la determinación de si el delito de estafa debe incluirse en el ámbito de estudio del derecho penal económico. En la actualidad, existe consenso en que el fraude y la estafa en el ámbito económico son elementos fundamentales para la investigación en el campo del derecho penal económico. Esta perspectiva se refleja en la última modificación al Código Orgánico Integral Penal, que amplía las categorías de personas que pueden ser consideradas responsables del delito de estafa. La doctrina generalmente identifica como elementos esenciales de

este delito el engaño, el error y la disposición indebida de bienes ajenos, todos claramente reconocibles en el contexto legal ecuatoriano. El artículo 186 del Código Orgánico Integral Penal, por ejemplo, incorpora el engaño en su definición como "la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos". En cuanto al error, se refiere a "inducir a error a otra persona", mientras que la disposición indebida de bien ajeno implica "realizar un acto que perjudique su patrimonio o el de una tercera persona". (DONNA, 2021)

## Planteamiento del Problema

¿Se necesita la reparación económica en los delitos de estafa? ¿Es necesaria la reparación económica dentro de los delitos de estafa?

La respuesta cada vez se prolonga a medida que pasa el tiempo y se dificulta encontrarla, los motivos son variables entre ellos se encuentra: la falta de recursos, poco personal, capacitación necesaria para acudir a este tipo de actos delictivos, falta de pruebas que trae consigo los especialistas necesarios para encontrarlas y entre otros. La necesidad que se busca suplir es dar respuesta a la pregunta anteriormente mencionada a partir de mecanismos necesarios acudiendo en resolver cada conflicto que existe en la vía judicial del país. En primer lugar, importancia y control ante este tipo de causas el cual trae consigo la autoridad competente para dar cabida a buscar soluciones estratégicas y con resultados favorables antes dicha situación; la norma jurídica está planteada solo es necesario el enfoque e impulso que se debe dar para llevarla en práctica y para ello es necesario solventar cada vacío que pueda existir ante dicha problemática.

Hoy en día las denuncias están visibles y las pruebas se encuentran plasmadas junto a ellas, del mismo modo la sanción específica para cada uno de estos delitos, aunque no exista al momento de forma completa la reparación integral que se espera ante dicho tema. Ante dichos actos se espera dos objetivos: en primer lugar, encontrar de manera eficaz los causantes sea uno o los que se encuentren involucrados ante dicho problema y entregarlos a la vía judicial correspondiente con el fin de cumplir las sanciones respectivas, en segundo lugar, se busca establecer una reparación total ante las distintas víctimas sea de forma económica o moral.

Para obtener óptimos resultados se llegará a utilizar el enfoque cualitativo dando cabida a encontrar el punto clave donde inicia la deficiencia al no conseguir una reparación total siendo las posibilidades como: Falta de recursos, poco personal especializado en temas informáticos, interrupción del proceso por continuidad de la persona que ingresa la denuncia como así el mal manejo al implementar las sanciones respectivos ante este tipo de delitos, el método de entrevistas más recolección de testimonios dará a conocer cuáles son los puntos débiles dentro del sistema judicial en la ciudad de Guayaquil.

## Objetivos:

### Objetivo General:

Determinar si la reparación económica es necesaria dentro de los delitos de estafa a través de las redes sociales como delitos electrónicos en Guayaquil desde el periodo del 2020 hasta el 2022.

### Objetivos Específicos

A. Demostrar la deficiencia en el sistema judicial con los casos de estafa a través de redes sociales a causa de las faltas de recursos en el periodo 2022.
B. Definir la importancia de la reparación económica en los delitos de estafa en Guayaquil en el periodo 2022 que genera compensación total a la víctima.
C. Establecer en la propuesta dentro de la reforma los posibles resultados que trae consigo la propuesta de proyecto dentro de la reforma penal.

## Justificación:

Sin lugar a dudas, el uso de tecnologías ha llevado a la introducción de normativas legales en el ámbito del derecho para abordar las necesidades de la

ciudadanía. A medida que las tecnologías han progresado, también lo han hecho las diversas formas de conductas delictivas, que han requerido adaptaciones normativas. En este contexto, la implementación del COIP ha representado avances significativos al abordar conductas previamente consideradas ilícitas. No obstante, a pesar de estos avances, no se ha contemplado la existencia de una normativa legal específica que aborde el delito de estafa perpetrado a través de las redes sociales.

Examinar e indagar sobre el delito desde diversas perspectivas representa una tarea de gran complejidad, sin lugar a dudas. En los últimos tiempos, el fenómeno ha experimentado un notable progreso, especialmente en consideración a la influencia de la globalización. Este fenómeno, si bien ha traído consigo beneficios, también ha contribuido al aumento masivo de delitos, destacándose entre ellos los Delitos Informáticos, que se han visto tecnificados. Es fundamental identificar y comprender el origen de las principales causas que impiden una reparación total en casos de delitos, como es el caso de estafas a través de redes sociales. La descripción y explicación detalladas de esta problemática permitirán realizar correcciones o reforzar aspectos clave donde el sistema falla al brindar reparación a la víctima. En este contexto, se reconoce que lograr una prevención efectiva de la criminalidad informática demanda, en primer lugar, un análisis imparcial de las necesidades de protección y de las fuentes de peligro.

En fin, el propósito principal llega a ser proteger y garantizar que dichos delitos serán sancionados mediante la vía correspondiente junto a los recursos y equipo especializado, la víctima accederá a la reparación total por su bien jurídico violentado y estos actos no queden en la impunidad.

# CAPITULO I

# MARCO TEÓRICO

## 1.1. ORIGEN Y EVOLUCIÓN DE LAS REDES SOCIALES

Con el avance tecnológico y la globalización, es evidente la existencia de la necesidad de relacionarse a través de los diferentes métodos telemáticos posibles, puesto que esto beneficia el ámbito social, educativo y comercial, dando claramente un cambio en cuanto a las formas de comunicación.

El origen principal de las redes sociales se remonta en los años 1994 – 1995 en donde surgieron algunos sitios de internet que fueron añadiendo paulatinamente capacidades técnicas de su momento y en ámbitos de carácter restringidos, con la oportunidad de crear foros, mensajes instantáneos, sin olvidar la conocida lista de amigos.

En 1994 se originó GeoCities, una plataforma que permitía la creación de redes sociales a través del internet con la idea de que los usuarios crearan su propia red con el fin de fomentar la creatividad para lograr socializar con otras personas fuera de su rango de localidad en determinados segmentos. (hernánfartocrespo, 2019)

En el año 1995 TheGlobe.com permitió a sus usuarios la posibilidad de personalizar las experiencias de su perfil online dándoles la oportunidad de crear contenido e interactuar con desconocidos al azar basándose en sus intereses similares. (PAÚL, 2023)

Desde 1997 a 2001, la evolución de la tecnología aportó diversas facilidades para las nuevas herramientas como diarios en línea o una lista de amigos favoritos para mantener interesados a los usuarios en los diferentes sitios, a finales de 2001 Ryze.com fomentó el impulso y creación de redes empresariales para lograr mejores conexiones entre profesionales en internet para conocer a los usuarios y lograr segmentaciones para saber cuál lograría la mayor venta de los productos. (CAROLINA, 2023)

Empresas fundadoras como LinkedIn, Tribe y Friendster utilizaban este tipo de sitios para mantener conversaciones y así poder ayudarse mutuamente para mejorar la experiencia de los usuarios, compartiendo su filosofía para lograr alcanzar el éxito deseado sin competir entre ellos y mantener seguro sus archivos privados de agentes externos. (Delito Informático. Procedimiento Penal en Ecuador , 2019)

En los últimos años, se ha prestado considerable atención a Internet en numerosas publicaciones, destacando el notable interés que suscita. Uno de los análisis más detallados aborda con precisión las características fundamentales de este fenómeno. Estas incluyen la ausencia de límites geográficos, la disminución de la importancia del espacio físico, la presencia de multiculturalidad y multilingüismo, la comunicación de "uno para muchos", la facilidad de difusión de la información, el crecimiento constante, la portabilidad, la carencia de identificadores seguros y la falta de una autoridad real que lo regule. Aunque este trabajo no tiene como objetivo principal el examen de Internet, no profundizaremos en la exploración específica de los presupuestos mencionados. Es suficiente señalar que todos los factores enumerados serán relevantes para orientar la posterior discusión sobre la ciberdelincuencia. (DÍAZ GÓMEZ, 2010)

Alrededor de dos tercios de los países participantes que han respondido a la encuesta han señalado un aumento en el uso de temáticas relacionadas con la COVID-19 en prácticas delictivas como el phishing y estafas en línea desde el inicio de la pandemia. Según Trend Micro, un colaborador privado de INTERPOL, se han identificado 907 000 mensajes vinculados a la COVID-19 desde enero de 2020. Los delincuentes cibernéticos han capitalizado la recesión económica y la ansiedad generalizada para perfeccionar sus estrategias de ingeniería social, centrando sus ataques en la COVID-19. Específicamente, varios grupos delictivos organizados han modificado sus enfoques para aprovechar la información relacionada con la pandemia y la escasez de suministros, incluyendo la promoción de medicamentos fraudulentos, paquetes fiscales y beneficios de emergencia. (INTERPOL, 2020)

Un considerable porcentaje de los informes presentados a las fuerzas policiales involucra situaciones en las cuales los perpetradores de amenazas utilizan tácticas de phishing vinculadas a la COVID-19 con el propósito de obtener credenciales y contraseñas de los usuarios. En muchos casos, estos correos electrónicos falsos suplantan la identidad de entidades gubernamentales y de salud legítimas, simulando proporcionar información y recomendaciones relacionadas con la pandemia. Además de esta conexión directa con eventos pandémicos, Kaspersky, colaborador privado de INTERPOL, ha identificado la actividad delictiva de individuos que ofrecen incentivos fiscales relacionados con la COVID-19 para persuadir a sus

víctimas a que visiten sitios web fraudulentos, los cuales recopilan información financiera y fiscal de usuarios desprevenidos. (UNIVERSO, 2021)

Por lo tanto, los mensajes electrónicos fraudulentos que se hacen pasar por comunicados de los Ministerios de Salud o la Organización Mundial de la Salud incluyen archivos adjuntos contaminados que explotan vulnerabilidades para activar códigos perjudiciales. Se ha observado que los países colaboradores y los asociados privados de INTERPOL identifican la presencia común de programas maliciosos como Emotet, Trickbot y Cerberus en estos correos fraudulentos, los cuales están diseñados específicamente para la sustracción de información. ( Los delitos informáticos con pena de prisión, 2021)

De acuerdo con la información proporcionada por los colaboradores privados, la suplantación de identidad a través de correos electrónicos (conocida como BEC, por sus siglas en inglés) sigue siendo la preferida por muchos perpetradores de amenazas. Para llevar a cabo sus ataques, han ajustado sus tácticas al contexto actual de la COVID-19, empleando, por ejemplo, direcciones de correo electrónico pertenecientes a proveedores y clientes, o direcciones que son prácticamente idénticas. La urgencia extrema en la adquisición de suministros y productos sanitarios esenciales proporciona a los delincuentes una oportunidad propicia para obtener información o redirigir grandes sumas de dinero hacia cuentas fraudulentas. (FISCALIA GENERAL DEL ESTADO, 2023)

### 1.2. CONVENIO DE BUDAPEST

El 23 de noviembre de 2001, en la ciudad de Budapest se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa, como también para aquellos países que, sin formar parte de este, quisieran adoptar la normativa contenida en él. El Convenio, viene a complementar otros tratados existentes en el Consejo de Europa en materia de cooperación en materia penal, pero manteniendo el foco en dos objetivos principales; en primer lugar, mejorar la efectividad de las pesquisas y procesos legales vinculados a delitos cometidos a través de la Red, y, por otra parte, permitir la obtención y mantención de la evidencia electrónica obtenida en estas investigaciones, con miras a su inclusión

en juicio. (Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional., 2020)

Hasta este momento, se ha abordado la transformación que Internet ha generado en diversas esferas de la vida humana, inserta en el contexto dinámico de la globalización. Ahora, nos enfocaremos en contextualizar este fenómeno dentro del ámbito específico abordado en este trabajo: la criminalidad. De hecho, en los capítulos dos y tres se detallarán algunos de los aspectos relacionados con la delincuencia en el entorno digital. (Abarca., 2020)

Es fundamental tener en consideración que, tal como mencionamos previamente, la red ofrece innumerables oportunidades para que las personas lleven a cabo sus actividades diarias; sin embargo, es igualmente cierto que también brinda numerosas ocasiones para violar la ley. Estas oportunidades están al alcance de todos, y resulta imprudente asumir una postura ingenua al creer que las vastas ventajas de diversos tipos reveladas por la nueva era informática no serán empleadas de manera ilegítima para perjudicar a los demás. (Harán, 2020)

Dado el impacto de la realidad que se suscita a nivel mundial por consecuencia del covid-19 la realidad de muchas personas ha evolucionado, a tal magnitud que los establecimientos de comercio manejan el giro del negocio mediante plataformas digitales para evitar propagaciones y contagios de este nuevo virus. En el contexto de esta realidad existen personas que han malversados estos actos, a través de la simulación de hechos falsos perjudicando su patrimonio, induciendo más concretamente a que los consumidores finales se vean por completo afectados y también el mercado ya que se genera desconfianza en una perspectiva generalizada, lamentablemente esta temática abarca lineamientos para extensos que se requieren tratar con bastante dedicación para lograr pausar el cometimiento de este delito. (GUSQUI, 2020)

La acogida que ha tenido el Convenio a nivel internacional ha sido positiva, en general, sin embargo, algunos Estados han preferido no adherir al Convenio, ya que estiman que la forma en que se debe regular tanto la cooperación internacional, como las materias de ciberdelincuencia debería darse mediante tratados regionales que contemplen la forma de trabajo y necesidades de la región. En este sentido, el alcance

y desarrollo de la ciberdelincuencia en América Latina es menor en comparación a algunos países de Asia o Europa. En la misma línea países como Brasil e India se han restado de adoptar el Convenio sobre la base de que no participaron en su redacción; los países del grupo BRIC17 y afines argumentan que por motivos técnicos y políticos el Convenio de Budapest no es una respuesta suficiente al problema y buscan un mandato para la elaboración de un instrumento jurídico universal bajo el auspicio de las Naciones Unidas. (Mundo, 2021)

Los casos de cooperación internacional, mediante las plataformas 24/7 tienen la particularidad de que mediante un contacto directo entre los organismos encargados de las investigaciones en distintos países, circule la información que permita la ubicación de sospechosos; así por ejemplo, en el año 2009, en España, el cantante David Bisbal, denunció estar siendo víctima de una extorción de parte de desconocidos, que habrían ingresado de manera ilícita a su correo electrónico, y del que habrían obtenido información personal e imágenes intimas, las que amenazaban con subir a la web a cambio de una alta suma de dinero; el cantante puso la denuncia ante el Juzgado de Almería, el cual solicitó a la Guardia Civil española (símil de Carabineros de Chile) se iniciara una investigación para determinar el origen de dichas amenazas; mediante la coordinación de la policía española, se logró determinar que la dirección de acceso a la cuenta de correo de la víctima, se encontraba en República Dominicana, lugar donde fueron detenidas las personas involucradas; este es un caso en que la coordinación entre países de distintas regiones fue esencial para la detección, captura y sanción de los autores del delito. (pandemia, 2021)

Según la afirmación de Rodríguez Bravo O. M. (2020), se destaca que Ecuador, desde el año 2001, no ha sido parte del Convenio de Budapest, y la investigación de los Ciberdelitos transnacionales se lleva a cabo mediante asistencias penales. Esta situación genera una preocupación significativa, especialmente porque el país carece de una legislación específica para abordar los Ciberdelitos. En este contexto, es crucial que Ecuador se adhiera al convenio, lo que facilitaría el intercambio de información y permitiría sancionar la criminalidad informática en colaboración con otros países firmantes.

El aumento de la delincuencia informática se atribuye a diversos factores, entre los cuales se incluye la evolución tecnológica. La falta de conocimiento o información sobre cómo protegerse contra posibles ataques a través de las nuevas tecnologías contribuye a esta problemática. La escasa comprensión de dichas tecnologías brinda a los delincuentes la oportunidad de llevar a cabo ataques potenciales contra sus víctimas. (Casillas, 2022)

En esa época, específicamente en el año 2001, Ecuador experimentó uno de sus primeros incidentes de ataques cibernéticos, donde la página oficial del Municipio de Quito fue comprometida mediante la técnica de hacking. Este suceso condujo a la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el año 2002. Como consecuencia, surgieron los primeros delitos informáticos en la legislación nacional, los cuales fueron posteriormente incorporados en el Código Penal. (Gómez, 2022)

El inconveniente, según la perspectiva planteada, radica en que en nuestro país, con la implementación del Código Orgánico Integral Penal, se abordaron los delitos informáticos de manera general, sin otorgarles una consideración singular que refleje adecuadamente su importancia e independencia tipificadora con respecto a las características específicas de cada uno. De este modo, se observa a los delitos informáticos como transgresiones comunes, lo que resulta en la creación de disposiciones legales con características particulares según el bien jurídico protegido. El legislador no se percató de que hay delitos que se asemejan entre sí y que, debido a ciertas palabras o actos, poseen naturalezas diferentes. Por lo tanto, esto podría conducir a un tratamiento indebido durante la fase de investigación. (Tamaulipeca, 2022)

Tomando en consideración que el Ecuador a pesar de ser un Estado garantista de derechos, de la pluriculturalidad, la libertad de conciencia, desarrollo y de los derechos de intimidad personal, familiar y patrimonial, o que incluso mantiene una normativa vigente y que regula un cierto porcentaje de los delitos que se cometen en el plano virtual, esta es insuficiente y no se actualiza con la misma velocidad que evolucionan dichos delitos, dejando una evidencia clara que todavía existe un vacío en el derecho informático, a su vez no existe una unidad ni un procedimiento específico a nivel judicial que permita dar un seguimiento adecuado para sancionar a

los delitos informáticos, lo que nos hace pensar que en su mayoría estos quedan impunes y el usuario desprotegido por lo que no es posible que el Ecuador aún no se adhiera a un convenio de vital importancia, el cual brindaría la protección adecuada a derechos vulnerados en relación de los delitos informáticos tales como la seguridad jurídica, derecho a la privacidad de datos y comunicaciones, a la intimidad e integridad personal, integridad sexual, datos o sistemas informáticos; derechos que con facilidad y con ayuda de la tecnología son vulnerados y que en muchos casos quedan en la impunidad. (León Felipe, 2020)

Según la investigación llevada a cabo y en sintonía con la perspectiva de especialistas en el campo, se observa que Ecuador se encamina hacia una posible futura inclusión en el Convenio de Budapest. Dado que este instrumento reviste una importancia crucial, los Estados que ratifican su adhesión o se unen por primera vez buscan establecer una política común en relación con los delitos informáticos. Esto, en última instancia, refuerza la cooperación internacional y la gestión de tecnologías innovadoras, permitiendo una mejora sustancial en la investigación y tratamiento eficiente de dichos delitos. (ASOBANCA, 2021)

### 1.3. EVOLUCIÓN DEL DELITO DE ESTAFA

Al ser la naturaleza del derecho positivo, la seguridad jurídica para los gobernados , ello se encuentra sustentado en el principio de derecho "…Nullum crimen, nulla poena sine praevia lege…" (Von Feuerbach, 1801), sin embargo en virtud de la relaciones que se crean desde el constructo social, los operadores jurídicos se ven en la obligación de enfrentar esta normatividad vigente con la realidad de las situaciones fácticas de las cuales tienen conocimiento, lo que en algunos casos da oportunidad a que el juez tenga la potestad de la interpretación de las normas con el fin de aplicarlas en el caso en concreto, lo que los doctrinarios han denominado teoría del realismo jurídico. (Crespo, El delito de estafa en el Código Orgánico Integral Penal. Breve análisis del tipo penal y las reformas del 2019.)

Este movimiento jurídico reconoce la parte dinámica que posee el Derecho desde los jueces, "…La tarea de los realistas fue insistir en el carácter indeterminado e incompleto del derecho y en la consecuente incidencia en la decisión judicial de

factores que, de acuerdo con la concepción dominante, eran extrajurídicos…" (Díaz, Angulo, & Barboza, 2018).

Antes de abordar la definición del tipo penal y sus componentes, es crucial destacar que la configuración del delito de estafa experimenta transformaciones en consonancia con el progreso de la sociedad. Un ejemplo ilustrativo sería el hecho de que, en sus inicios, la acción delictiva se limitaba exclusivamente a afectar a individuos. En la actualidad, se identifican diversas situaciones en las cuales la víctima ni siquiera está presente al momento de consumarse el delito, como en el caso de sistemas informáticos o cajeros automáticos.6 No obstante, son precisamente las nuevas modalidades de estafa las que han complicado la evolución de este tipo penal. Por consiguiente, se han llevado a cabo numerosos estudios destinados a analizar cómo definir, incluir y penalizar ciertas conductas que actualmente se encuadran en la estafa, siendo los desafíos más prominentes aquellos relacionados con la conceptualización, la identificación del bien jurídico protegido y los elementos constitutivos del tipo penal de estafa. (Arrimadas Abogados, 2021)

Desde un punto de vista conceptual, se describe la estafa como aquellas acciones que comparten la característica de causar un perjuicio económico mediante prácticas engañosas. En otras palabras, se puede concebir como cualquier acto intencional que, a través de un engaño, resulta en o busca causar daño al patrimonio de un tercero. A partir de esta definición, se infiere que el delito de estafa tiene como objeto de protección el patrimonio ajeno, abarcando diversos elementos como bienes muebles o inmuebles, derechos, dinero, y representación de capitales, los cuales pueden constituir el objeto material de la infracción.

No obstante, existen autores que sostienen que esta conceptualización solo es aplicable cuando están presentes los elementos esenciales de la estafa común, a saber: engaño, error y disposición del patrimonio. Es importante señalar que su análisis debe permanecer exclusivamente en el ámbito doctrinario y jurisprudencial, sin buscar una definición legal. (Teoría general del delito de estafa, 2020)

Después de realizar una breve revisión de los componentes fundamentales que componen el delito de Estafa en el contexto ecuatoriano y examinar su evolución en aras de salvaguardar tanto al mercado como a la sociedad en general, resulta

crucial examinar la reforma implementada en el año 2019. Esta reforma, desde mi perspectiva, representa el cambio más significativo en relación con el delito de estafa en Ecuador, ya que por primera vez se introduce la imputabilidad penal de las entidades jurídicas de la siguiente manera:

En caso de que se determine la responsabilidad penal de una persona jurídica, esta será sancionada con una multa que oscila entre cien y doscientos salarios básicos unificados del trabajador en general. La inclusión de la responsabilidad penal de las personas jurídicas en Ecuador fue uno de los cambios significativos introducidos por el Código Orgánico Integral Penal en 2014. Este código sigue el principio de "numerus clausus", lo que implica que solo para ciertos delitos específicos expresamente establecidos por la ley se permite la imputación de responsabilidad a las personas jurídicas. No obstante, parece que el legislador ecuatoriano, guiado por la importancia que tiene el delito de estafa en el ámbito del derecho penal económico, ha optado por incluir el delito de estafa y sus modalidades agravadas dentro de las circunstancias que pueden dar lugar a la responsabilidad penal de las personas jurídicas. (Fresneda, 2022)

La fundamentación de la responsabilidad penal de las personas jurídicas radica en la protección de los derechos que el Estado está obligado a salvaguardar para la sociedad ante ciertas empresas que han acumulado un poder adquisitivo superior al de muchos países en desarrollo. El propósito de esta responsabilidad no es perseguir la libertad de mercado ni la competencia desleal, ni tampoco servir como un medio de presión para obtener ganancias económicas. En cambio, busca incentivar que las empresas implementen programas de cumplimiento obligatorio, con el fin de reducir los riesgos asociados a ciertos delitos en el desarrollo de sus actividades.

En el contexto ecuatoriano, es imperativo que la jurisprudencia y los órganos de justicia ejerzan precaución para evitar abusos en la aplicación del derecho penal y para asegurarse de que este no se extienda de manera indebida. Existen situaciones en las cuales se podría intentar vincular a las personas jurídicas con responsabilidad penal en cuestiones que deberían resolverse en el ámbito civil, lo que podría comprometer la reputación de estas entidades al criminalizar sus actividades comerciales. (Briceño, 2023)

Aunque el examen del delito de estafa abarca diversos aspectos, se busca proporcionar de forma sucinta y general una visión de la evolución de este tipo penal. Dicha evolución se caracteriza por la expansión de las conductas penalmente censurables que se incorporan al tipo general. Además, se aborda la motivación detrás de la imputación de responsabilidad penal a las personas jurídicas en Ecuador en relación con el delito de estafa, así como las implicaciones asociadas a esta determinación. (Jácome & Briones, 2022)

En cuanto a Brasil, desde el año 2015 muestra resistencia a unirse a este acuerdo debido a que no participó en su creación. Fundamenta su posición en la creencia de que el foro más apropiado para adoptar un convenio de esta índole son las Naciones Unidas, siendo Brasil un líder en Sudamérica. Además, el país aún no se muestra convencido por el instrumento de adhesión, el cual surgió ante la falta de normativas específicas. En su lugar, Brasil está desarrollando protocolos y reglas de buenas prácticas y cooperación mutua entre los países miembros, con el objetivo de consolidar los valores democráticos y los derechos universales. (ASOBANCA, 2021)

En la actualidad, el Convenio se extiende prácticamente a todas las naciones del continente europeo. En este contexto, la incorporación de nuestro país a dicho acuerdo persigue un objetivo fundamental: lograr eficacia en la colaboración y la aplicación de la justicia a nivel global en relación con delitos que, por su índole, con frecuencia trascienden fronteras. Muchos de estos delitos se caracterizan por su capacidad de convertirse en amenazas organizadas, lo que subraya la importancia de abordarlos de manera conjunta. (Pereyra Maita, 2020)

El Estado Peruano es miembro por Resolución Legislativa Nº 30913, desde el 13FEB2019, esto lo convierte en un respaldo legal que asegura la protección en la batalla contra estos crímenes u otras formas emergentes de conducta delictiva. Si sus reglas se ajustan específicamente a nuestro Sistema Legal de resguardo a la privacidad personal, contribuiría a garantizar su ejecución efectiva. (Arrimadas Abogados, 2021)

La ausencia de límites físicos constituye una cualidad esencial de Internet, brindando numerosas ventajas y, naturalmente, desventajas en el ámbito de la persecución de actividades delictivas. En primer lugar, cualquier estrategia criminal requiere comprender el terreno de actuación, es decir, identificar la ubicación virtual

de Internet. Este desafío representa uno de los principales obstáculos para abordar eficazmente estas cuestiones. (Altamirano)

La basta cantidad de información que constituye la red está almacenada en servidores distribuidos globalmente. Estos servidores, esencialmente compuestos por discos duros y otras herramientas interconectadas a través de la Red, residen en edificios denominados centros de datos. Estos centros de datos poseen un valor incalculable en diversos aspectos, ya que albergan desde datos bancarios hasta conocimientos multidisciplinarios que ya no se encuentran en los libros. Dada la importancia de su contenido, estos centros de datos son altamente protegidos, y en muchas ocasiones, las empresas no revelan su ubicación, ya que un ataque físico podría no solo destruir información, sino también afectar a empresas e incluso a Estados. (Fresneda, 2022)

Este hecho presenta un desafío significativo, ya que la dificultad de rastrear el origen exacto de la información en Internet complica la tarea, por ejemplo, de eliminar datos que violan el derecho al honor de una persona. Además, este aspecto impacta directamente en reformulación sin incurrir en plagio: la identificación de la competencia y jurisdicción de los Estados, como se abordará en la siguiente sección. La complejidad se intensifica si los contenidos ilícitos se ocultan detrás de una cortina de espejos, lo que significa que una página web puede estar ubicada en un lugar diferente al que aparenta. (Carrasco, 2011)

Cometer crímenes informáticos resulta ser más accesible de lo que podría parecer inicialmente. En primer lugar, apenas se requieren recursos por parte del delincuente, como un simple ordenador conectado a la red. Como se ha evidenciado, estos delitos pueden perpetrarse desde cualquier lugar del mundo. Además, la ejecución puede ser sorprendentemente sencilla, al punto de que incluso una persona con conocimientos informáticos limitados podría teóricamente llevarlo a cabo. Incluso podría realizarlo sin ser plenamente consciente de sus acciones. Es importante destacar que, en este contexto, es necesario distinguir entre diversos tipos de delitos, ya que resulta evidente que las grandes estafas informáticas o la creación de programas destructivos complejos están fuera del alcance de individuos con conocimientos informáticos limitados. Sin embargo, existen otros delitos

aparentemente más simples que podrían ser cometidos por personas con conocimientos informáticos básicos. Por ejemplo, enviar virus creados por terceros o sabotear programas informáticos utilizando herramientas como cracks o generadores de claves disponibles en la World Wide Web sin demasiada dificultad. (Crespo, El delito de estafa en el Código Orgánico Integral Penal., 2021)

Hacemos referencia específicamente a la aplicación geográfica de la legislación penal. La amplia libertad para cometer delitos sin restricciones territoriales, como se detalló previamente, plantea importantes problemas. Es importante destacar que el autor de un delito puede llevar a cabo sus acciones desde un Estado distinto al de la víctima, incluso sin conocer la ubicación de esta última. Esta perspectiva novedosa genera incertidumbres en diversos niveles, tanto en lo que respecta a la entidad estatal encargada de abordar el caso, como a la viabilidad de ejecutar la decisión tomada. Además, surge un problema significativo relacionado con la variada regulación del derecho sustantivo en diferentes Estados. Podría surgir una percepción equivocada si asumimos que, debido a que en el ámbito penal la jurisdicción y la ley aplicable siempre coinciden, no existen dificultades en cuanto a las normas materiales que deben ser aplicadas. Sin embargo, la realidad es que, más allá de esta circunstancia, nos enfrentamos a numerosos casos en los que ciertos actos son considerados punibles según las diferencias en el sistema de derecho penal entre dos Estados, generando así discrepancias evidentes desigualdades y áreas de impunidad. (Carrasco, 2011)

En resumen, esto da lugar a un vacío normativo a nivel internacional en lo que respecta a la jurisdicción competente en casos de delitos informáticos, generando numerosos conflictos que afectan principalmente a los individuos. La incertidumbre resultante es significativa, ya que determinar qué legislación nacional se estaría infringiendo, si es que existe alguna, se vuelve difícil debido a que el contenido de Internet se encuentra simultáneamente en todo el mundo. En este contexto, prácticamente todas las actividades en línea adquieren un carácter internacional que podría implicar múltiples jurisdicciones o dar lugar al llamado efecto indirecto. (Briceño, 2023)

No obstante, al afinar aún más el panorama legal actual, en el ámbito del Derecho español, se acepta la posibilidad de que ciertas entidades jurídicas cometan

estos delitos (aunque, como se mencionó previamente, las posibles sanciones deberán recaer, en su contexto, en relación a los individuos responsables de la gestión de la entidad). Evitaremos adentrarnos en la discusión acerca de la aplicabilidad del artículo 30 del Código Penal de España. En consonancia con la perspectiva de Gómez Tomillo, que sostiene que no hay inconvenientes en aplicarlo a los delitos informáticos perpetrados a través de internet, detallaremos a continuación su alcance. (Altamirano)

En situaciones más habituales, se trata de una responsabilidad subsidiaria de los directivos de las empresas, ya que resulta prácticamente imposible tomar medidas contra el creador del contenido ilícito alojado en la World Wide Web. Normalmente, esto se traduce en constancia, se observa una falta por parte de la entidad, la cual se abstiene de tomar medidas para evitar la divulgación del contenido. Sin embargo, es importante destacar que para condenar por varios de estos ciberdelitos se requiere la presencia de dolo (algunos expertos solo exigen el "conocimiento efectivo" de la existencia de los datos, mientras que otros requieren "algo más" que facilitar el simple acceso a internet, es decir, una colaboración más allá de proporcionar simplemente el acceso) La presencia de una posición oficial de responsabilidad es destacada, y el autor previamente citado requiere la "similitud estructural entre la omisión y la posibilidad de conducta activa". (DONNA, 2021)

### 1.3.1. LA ESTAFA

De manera amplia, se reconoce que aquellos que, con el objetivo de obtener beneficios económicos, emplean artimañas fraudulentas, para generar un fallo en alguien más, incitándolo a llevar a cabo una acción perjudicial para sí mismo o para otros, también según la definición proporcionada por el Diccionario Jurídico Espasa, en España se tipifica como estafa aquellos casos en los cuales, con intenciones de lucro, y haciendo uso de manipulaciones informáticas u otros artificios similares, se logre la transferencia no autorizada de cualquier activo patrimonial en detrimento de un tercero.” (Palés, 2001).

El fraude se produce cuando una persona es engañada monetariamente por otra persona, esto sucede cuando una persona miente a otra al provocar a realizar algo o no hacer algo que deriva en una pérdida monetaria, este se puede cometer vía online, presencialmente o por correspondencia. "…La lesión al patrimonio consiste en su disminución económica…" (Balmaceda, 2016).

Son recursos constitutivos de la estafa, la simulación de hechos erróneos o La distorsión o encubrimiento de eventos verídicos puede resultar en perjuicio económico o menoscabo patrimonial.

En la esfera de la actividad fraudulenta, se requiere hacer frente a una completa transgresión que resulta en un perjuicio tangible para el patrimonio de la persona afectada o en la posibilidad de que dicho perjuicio ocurra. En este sentido, la estafa se configura como un delito concretamente material, susceptible de presentarse de manera imperfecta. Quien emplea el engaño con el claro propósito de influir. (CUNICH, 2021)

El engaño se apoya en la mutación o variación de la realidad, inclinado a ocasionar o conservar un error ajeno, como medio de lograr la recepción de la cosa. Es recomendable destacar que el propósito y la finalidad del acto fraudulento se centran en el impacto la entrega de valores. Puede revestir incontables maneras, tantas como sea capaz de notar la imaginación humana, situación está que distingue el engaño la composición esencial que define el delito de estafa se encuentra en la falsificación documentaría. (Rosso Pérez, 2022)

*"Art. 186.- Estafa.- (Reformado por el Art. 2 de la Ley s/n, R.O. 598-3S, 30-IX-2015; y por el Art. 42 de la Ley s/n, R.O. 107-S, 24-XII-2019).- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años".* (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

### 1.3.2. ESTAFAS Y REDES SOCIALES

En la estafa “tipo” de la que se parte, la elemental, una persona, el vendedor, oferta un producto definido en una red social, entra en contacto con el cliente, quien tendrá que hacer el ingreso de la porción concertada con carácter anterior a la recepción del producto, si bien hablado producto jamás llegará a su destinatario, quien, tras diversos intentos por solucionar el problema, en el mejor de los casos, optará por interponer la denuncia que corresponde. En otras posibilidades, el cliente efectúa el ingreso acordado, o bien, lo hace al mando de la contabilización de un tercero desconocedor de la transacción, o lo hace al mando de una cuenta bancaria de su titularidad esta podría ser real o ficticia, realizado el ingreso y remitido el comprobante al vendedor, al obtener el producto en cuestión, anula el cargo o este es anulado por el titular de la contabilización bancaria. (Ron, 2019)

El encontrarnos frente a estafas usuales no involucra que no se susciten inconvenientes prácticos. Hace años, un ladrón atracaba un banco y robaba un millón de euros; ahora, aquel mismo ladrón, sin necesidad de salir de su vivienda, puede hurtar un euro a un millón de individuos. Esta nueva realidad conlleva una problemática propia y constante en la indagación de tales hechos. (Sánchez, 2022)

## 1.4. FUDAMENTACIÓN LEGAL

La evolución de las herramientas en medios electrónicos ha generado cambios significativos en los instrumentos legales, instando a los Estados miembros de la Organización de Estados Americanos a adoptar nuevas directrices. El impacto del Internet ha propiciado un notable crecimiento en la economía global, mejorando la eficiencia, productividad y creatividad en todo el hemisferio. Cada vez más, individuos, empresas y entidades gubernamentales recurren a las redes de información para diversas actividades, que abarcan desde transacciones comerciales hasta la planificación de actividades personales, empresariales y gubernamentales, la transmisión de comunicaciones, y la realización de investigaciones. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

Reconociendo que, en la Tercera Cumbre de las Américas, en la ciudad de Quebec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en telecomunicaciones en las Américas.

Lamentablemente, el Internet ha dado lugar a nuevas y persistentes amenazas que representan un riesgo constante para la comunidad global de usuarios. La información circulante en la red puede ser deliberadamente distorsionada y manipulada, comprometiendo la privacidad de los usuarios y generando fraudes comerciales. La alteración o destrucción de datos almacenados en computadoras conectadas a la red puede tener consecuencias graves, como obstaculizar las funciones gubernamentales y perturbar los servicios públicos de telecomunicaciones, así como otras infraestructuras críticas como redes eléctricas, aeropuertos y suministro de agua. Estas amenazas, que afectan a ciudadanos, economías y servicios esenciales, no pueden abordarse de manera efectiva por un solo gobierno ni pueden combatirse mediante una única disciplina o práctica. (diciembre, 2023)

### 1.4.1. LEGISLACIÓN ECUATORIANA

El Código Orgánico Integral Penal (2021) en su art. 186 referente con la estafa, establece que la persona que, para obtener un beneficio patrimonial mediante la simulación de hechos falsos; art. 190, utilizando medios electrónicos de manera fraudulenta, se lleva a cabo la apropiación ilícita de un bien mediante la manipulación fraudulenta de un sistema informático o redes electrónicas y de telecomunicaciones la apropiación de un bien ajeno, el artículo 191 aborda la reprogramación o alteración de datos en dispositivos móviles, así como la modificación de la información de identificación de dichos dispositivos. Por otro lado, el artículo 229 se refiere a la divulgación no autorizada de bases de datos, destacando aquellos casos en los que se revele información registrada de manera deliberada e intencional, lo que constituye una violación directa del deber de mantener el secreto. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

La infracción relacionada con la informática se encuentra definida en el artículo 190 del Código Orgánico Integral Penal, conforme a lo dispuesto en la categorización de delitos “el uso de un sistema informático o redes electrónicas y de telecomunicaciones con el propósito de adquirir ilegítimamente un bien perteneciente a otra persona o de llevar a cabo la transferencia no autorizada de bienes, valores o derechos, causando perjuicio a la víctima o a terceros, con el objetivo de obtener beneficios propios o para favorecer a terceros, mediante la alteración, manipulación

o modificación del funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será penalizada con una condena de privación de libertad que oscilará entre uno y tres años". (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2023)

## 1.5. LEGISLACIÓN COMPARADA

### 1.5.1. Argentina

Se menciona un catálogo completo de delitos informáticos considerando que la información, como valor a proteger, ha sido tenida en relevancia por el Derecho Penal en otras ocasiones. De por si se lo ha hecho desde el punto de vista de la confidencialidad, pero no como un nuevo bien jurídico tutelado de varios intereses dignos de protección penal. Según nuevos y mejorados estudios, la respuesta es que el Código Penal argentino no posee reglas específicas sobre delitos cometidos a través de los ordenadores. (Jácome & Briones, 2022)

Un ataque a través de mensajes electrónicos infectados con virus efectivamente en la que puede haber sido afectada una empresa, logrando interrumpirla su línea de producción, puede causar daños realmente graves y severos lo que sin duda causa pérdida de tiempo y un consecuente perjuicio económico pero que de ninguna manera se configura en un daño de tipo tutelado y de reparación. (Penal., 2019)

La salvaguarda de la información personal emerge como una prioridad legal respaldada inicialmente por el reconocimiento de un derecho fundamental conocido como Hábeas Data. Este derecho se erige con el propósito de prevenir la divulgación de datos íntimos y privados, posibilitando la corrección, actualización o modificación de dicha información en cualquier momento. Por ende, es imperativo fortalecer la protección jurídica en relación con los datos personales, implementando mecanismos que abarquen desde la regulación legal en los procesos de adquisición,

almacenamiento, sistematización, hasta las modalidades de compartición. (Novik, 2021)

Las tecnologías de la información mejoradas y actuales también influyen en el ámbito de la producción segura, lo cual ha generado avances normativos en áreas como contratos electrónicos, flujo de datos transfronterizos, comercio electrónico, gobierno electrónico y delitos informáticos. Por lo tanto, resulta prescindible establecer un mecanismo de protección legal específico para los datos personales. Se debe garantizar un procedimiento que asegure el ejercicio de los derechos relacionados con la información personal y facilite el acceso a dicha información por parte de los individuos titulares de la misma. (Institute, 2022)

Una de las más significativas en cuanto hablamos del derecho comparado es el del Código Penal Español a criterio de Borrallo, fue lo incluido en el ya por sí novedoso y confuso capítulo Primero “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio” donde se castiga con las mismas penas que establece el número Uno, esto es, prisión de uno a cuatro años…, en primera instancia, el apoderamiento, la utilización, la modificación o hasta inclusive la malversación sin estar autorizado y en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro que se hallen registrados en soportes informáticos electrónicos, o en cualquier otro tipo de fichero o registro público o privado. (PENAL, 2022)

### 1.5.2. Colombia

La legislación colombiana en materia penal, a través de la ley 599 de 2000 (República de Colombia, Senado de la República, 2000), aborda en su séptimo capítulo, dentro del Libro segundo, Título III, los delitos relacionados con la libertad individual y otras garantías, así como la vulneración de la intimidad, la reserva y la interceptación de comunicaciones. En este contexto normativo, se establecen distintas conductas delictivas, entre las cuales se encuentran: la violación ilícita de comunicaciones (Artículo 192), la oferta, venta o compra de instrumentos aptos para la interceptación de comunicaciones privadas entre personas (Artículo 193), la divulgación y utilización de documentos reservados (Artículo 194), el acceso abusivo a un sistema informático (Artículo 195), la violación ilícita de comunicaciones o

correspondencia de carácter oficial (Artículo 196) y la utilización indebida de equipos transmisores o receptores. (Artículo 197).

Según Salazar (2009), fue en el año 2009 cuando el legislador colombiano introdujo modificaciones al catálogo delictual mediante la promulgación de la Ley 1273, también conocida como Ley de Delitos Informáticos. Esta legislación, al establecer un nuevo bien jurídico protegido, es decir, la información y los datos, incluye una serie de disposiciones que condenan las acciones de la delincuencia informática. Es relevante señalar que la creación de esta norma fue impulsada académicamente por el juez Alexander Díaz García y el profesor Harvey Rincón Ríos, quienes, basándose en el convenio de Budapest de 2001, redactaron el proyecto de ley que finalmente se convirtió en la mencionada Ley de Delitos Informáticos. (p. 98; en el mismo sentido Arias & Daza, 2010).

Con este enfoque, Colombia alcanzó un nivel comparable al de los países pertenecientes a la Comunidad Económica Europea (CEE), garantizando la calidad de la información mediante la inclusión de aspectos relacionados con la administración y control, dentro del marco de la protección integral. Por lo tanto, la Ley 1273 de 2009 representa un importante progreso en la estrategia para abordar los delitos informáticos en el país, subrayando la necesidad de una preparación integral en diversos sectores, tanto en el ámbito público como en el privado. (Briceño, 2023)

Después de analizar algunos antecedentes, resulta fundamental señalar que la disposición relativa al delito de estafa informática se halla en el artículo 246 del Código Penal ecuatoriano, el cual establece lo siguiente: "Artículo 246.- Estafa. Aquel que obtenga beneficio ilícito para sí mismo o para un tercero, causando perjuicio a terceros, al inducir o mantener en error a otro mediante artificios o engaños, será sancionado con una pena privativa de libertad de dos (2) a ocho (8) años y una multa que oscilará entre cincuenta (50) y mil (1.000) salarios mínimos legales mensuales vigentes. La existencia de la estafa resulta innegable en situaciones en las que el agente logra ilícitamente obtener beneficios mediante el uso de mecanismos que posibilitan la conexión no autorizada a través de la computadora". (Delito Informático. Procedimiento Penal en Ecuador , 2019)

### 1.5.3. España

La regulación interna de los delitos informáticos se encuentra en el Código Penal español, en distintos títulos según el bien jurídico protegido. Para efectos de su categorización y estudio utilizaremos la clasificación de los delitos informáticos empleada por el Observatorio Español de Delitos Informáticos, especificando para aquello las disposiciones aplicables y los elementos pertinentes en materia de ciberdelincuencia respecto de cada una de las siguientes categorías:

- Interferencia en los datos y en el sistema: Arts. 263 a 267 Se regula principalmente el daño grave a datos o programas informáticos; la interrupción grave a un sistema informático y la comercialización de dispositivos electrónicos para aquello, contemplando incluso la responsabilidad de personas jurídicas en la comisión de estos delitos.
- Fraude informático: Arts. 248 a 251. Se enmarca plenamente en la regulación del delito de estafa, donde se pena además la utilización indebida de tarjetas bancarias.
- Falsificación Informática: Arts. 390 a394 que regulan la falsificación documental en general, contemplando la hipótesis de falsificación telegráfica por medio de servicios de telecomunicación. Además; el Art. 399 bis regula la falsificación de tarjetas bancarias y el Art. 400 sanciona la comercialización de programas informáticos para cometer las falsificaciones descritas.

España concurrió a la firma del Convenio de Budapest con fecha 23 de noviembre de 2001. Contando con la autorización interna de las Cortes Generales (Congreso) según lo dispuesto por el artículo 94 de la Constitución Española y se procedió a su promulgación en el año 2010, publicado en el Boletín Oficial de Estado (BOE) número 226 de 17 de septiembre de 2010. (Gomezjurado Gomezjurado, 2023)

Al ratificar el instrumento internacional; con fecha 3 de junio de 2010, España se limitó a realizar una Declaración consistente en reconocer a Gibraltar como un territorio no autónomo, dependiente del Reino Unido y en proceso de descolonización. Esta declaración fue introducida a su vez en el convenio de adhesión al Marco BEPS de la UCDE y va en la línea de reiterar lo dispuesto por el tratado de Ultrecht de

1713121 con especial consideración al actual proceso de autonomía en discusión. España no reservó ninguna disposición del Convenio. (Padilla, MENCION EN DERECHO FINANCIERO, BURSATIL Y DE SEGUROS, 2022)

Dado que España promulgó el Convenio ya en el año 2010, las medidas de adecuación adoptadas se encuentran incorporadas plenamente en su legislación, lo que ha sido expuesto en el punto i) del presente acápite. Sin perjuicio de aquello, actualmente se estudia una gran reforma a su sistema procesal penal, la que se encuentra pendiente a partir de un borrador elaborado por el Ministerio de Justicia en 2013 con el objetivo de sustituir la ley de Enjuiciamiento Criminal de 1882. (pág. 15)

### 1.5.4. Uruguay

En materia criminal el Código Penal uruguayo dispone en su artículo 277 bis la tipificación del contacto o influencia a menores de edad con intención de cometer delitos contra su integridad sexual por cualquier medio. Fuera de esta materia no hay regulación específica sobre delitos cometidos mediante medios informáticos. Cabe señalar que Uruguay tiene actualmente una regulación sobre la protección de datos personales mediante Ley 18.331 de 2008 que fue complementada por la Ley 19.670 de 2018 con el objetivo de reforzar las obligaciones y responsabilidad de los encargados de base de datos. (DÍAZ GÓMEZ, 2010)

En materia procesal, Uruguay realizó una reforma mayor en el año 2017 mediante la Ley 19.293 de nuevo Código Procesal Penal, que estableció un sistema oral acusatorio, separando las funciones de investigación y acusación de las funciones jurisdiccionales, dejando las primeras en el nuevo Ministerio Público. Este Código establece algunas medidas pertinentes al presente estudio: en su sección XIV “de la interceptación e incautación postal y electrónica”; en los artículos 205 y siguientes, consagra la facultad de solicitar judicialmente por parte del Ministerio Público la interceptación, incautación y apertura del correo electrónico o comunicaciones similares del imputado y la medida de intervención de comunicaciones (de contenido) en el artículo 209. En materia probatoria; además, se establece la filmación como medio de presentar el testimonio además de considerar al video dentro del concepto de documento. (López Quizhpi, 2022)

## 1.6. BIEN JURÍDICO PROTEGIDO

Los actos delictivos en el ámbito informático son catalogados como ofensas pluridimensionales, ya que su principal foco de interés recae en la salvaguardia de la información, ya sea almacenada, comprimida o transmitida mediante sistemas informáticos. (Villavicencio Terreros, 2014 p. 288); la protección de la información alojada en bases de datos, sistemas o redes de computadoras, así como la seguridad en la circulación legal de la información que atraviesa estos entornos, son aspectos cruciales a considerar.(Peña Cabrera Freyre, 2008, p. 501). El segundo aspecto resguardado legalmente abarca tanto el patrimonio como la privacidad. Sin embargo, es innegable que el elemento fundamental en términos de bienes jurídicos recae en aquellos directamente relacionados con los sistemas informáticos.. (Arrimadas Abogados, 2021)

Villavicencio Terreros (2014) refiere que en los delitos informáticos: No se puede considerar exclusivamente a la información como el único bien jurídico afectado, dado que no solo es el más significativo sino que también afecta a un conjunto de bienes, como consecuencia de las características de la conducta típica en esa modalidad delictiva, la cual entra en conflicto con diversos intereses colectivos. (p. 288)

Bajo esta premisa, compartimos la perspectiva de Pérez López (2019), quien señala que debido a la universalización de la tecnología, las oportunidades para la delincuencia informática han aumentado considerablemente. En este contexto, resulta difícil limitar a un autor específico a una tipología particular, ya que la sociedad ha superado las barreras sociales para el uso de la tecnología, democratizando constantemente sus recursos y posibilidades. (p. 96)

## 1.7. ANÁLISIS DE LAS DISTINTAS POSICIONES TEÓRICAS DE LOS DELITOS COMETIDOS A TRAVÉS DE REDES SOCIALES

Según el Sociólogo Requema Santos (2011) “una red social es una serie de vínculos que existen entre varias personas que tienen como capacidad principal la

interpretación de una o varias conductas sociales dentro de los miembros que componen los vínculos" (Requena Santos, 2011, pág. 2)

Por otro lado, para Cacales Martínez, "Las redes sociales en internet son conformados por un grupo de amigos que al ingresar a el portal seleccionado, tienen la oportunidad de hacer partícipes a sus propios contactos y al mismo tiempo ser puesto a consideración a otro mientras de la red de tal manera que permiten el acceso a una ampliación dentro del mismo grupo" (Cacales Martínez, Real García, & Benedicto Marcos, 2011), él consideraba que los integrantes iban aumentando conforme a más miembros se unían, es decir si un usuario ingresa consigo trae a más usuarios conforme permite el acceso a sus contactos por ende el portal se expande. (Rodas Soto, 2022)

Según el IWGDPT (2018) "algunos sistemas de redes sociales vulnera el concepto de la comunidad, puesto que estas redes de una u otra manera comparte información personal basado en que está disponible para otros miembros de la red solo por el hecho de aceptar una amistad" (Internacional Working Group on Data Protección in Telecommunications, 2018), en donde se sugiere que no existe una seguridad en sí de los datos de terceros al ser proporcionado por sus amigos dentro de sus perfiles por lo que dichas redes no pueden responsabilizarse. (Rendón, 2022)

En el Ecuador, la legislación acerca de las redes sociales es reducida, en sentido que netamente se lo puede encontrar en el Reglamento General de la Ley Orgánica de Comunicación, en su segundo artículo donde establece una exclusión de la regulación y control administrativo dentro de la información que sea emitida por medio de redes sociales, blogs y páginas web. (FISCALIA GENERAL DEL ESTADO, 2023)

## 1.8. NATURALEZA JURÍDICA Y CARÁCTERÍSTICAS DEL DELITO DE ESTAFA

En la naturaleza jurídica encontramos la identificación de los bienes jurídicos que son lesionados por las actividades ilegales tipificadas en las diversas legislaciones de carácter penal, Según Von Liszt (1981) "La naturaleza parte de intereses vitales, tanto del individuo o colectivo, parte de la protección jurídica que

eleva los derechos indispensables para la convivencia pacífica que se encuentra precautelado bajo normativas de constante cambio conforme a las necesidades".

En las normativas vigentes el bien jurídico es el objeto de protección de la Ley como el carácter fundamental del buen vivir, es decir, si no se protegiera los diversos bienes jurídicos, se violentarían diversos tratados y convenios internacionales, iríamos contrarios a la constitución, por tanto, contrarios a los derechos humanos dejando una vida sin opciones y vacías, de ahí la importancia del debido cuidado de los diversos bienes jurídicos, estos en algunos casos son intrínsecos e inalienables. (Los ciberdelitos como estafas en línea y promociones falsas se disparan hasta en un 35% en diciembre, 2022)

Una vez definido qué objetivo de la naturaleza de los delitos es proteger los intereses de las diversas comunidades, podemos establecer que el bien jurídico dentro del delito de estafa es el patrimonio, por tanto, este debe protegerse según lo establecido en diversas normas que amparan este derecho como fundamental para la correcta supervivencia del ser humano. Conforme se desarrolla la sociedad los delincuentes buscan la manera de violentar este derecho mediante las ventajas que proporcionan las ciencias jurídicas y nuevas tecnológicas. (FRAUDE, CORRUPCIÓN Y UTILIZACIÓN INDEBIDA DE LOS RECURSOS, 2022)

# CAPITULO II

# METODOLOGÍA DEL PROCESO INVESTIGACIÓN

## 2.1. Enfoque de la investigación

### 2.1.1. Enfoque cualitativo

El presente trabajo de investigación fue elaborado bajo el enfoque cualitativo debido a que es el que Opta por ajustarse de manera más adecuada a las particularidades y requisitos del estudio en cuestión.

El enfoque cualitativo se refiere a la recolección y análisis de datos no numéricos que permitan la comprensión de conceptos, opiniones y demás que contribuyen las personas, teniendo un sentido más amplio. Una porción de un concepto se va precisando a medida que se acota, y una vez claramente definida, se deducen metas y cuestionamientos de investigación. Posteriormente, se examina la documentación existente y se desarrolla un marco o enfoque teórico. (Nizama y Nizama, 2020, pp. 69-90)

## 2.2. Período y lugar de investigación

La presente investigación se desarrolló en la ciudad de Guayaquil en el periodo 2020-2022 con el fin de analizar la estafa a través de las redes sociales, titulados como delitos electrónicos hacia las víctimas examinando la búsqueda de una reparación total hacia el sujeto afectado.

## 2.3. Método de Investigación:

### 2.3.1. Investigación Descriptiva

La elección de la investigación descriptiva se valida como un enfoque adecuado para explorar temas o sujetos particulares, sirviendo como preludio a investigaciones más cualitativas.

> A pesar de que existen algunas inquietudes legítimas acerca de la validez de los conceptos, siempre y cuando el investigador tenga pleno conocimiento de las limitaciones, este tipo de investigación se presenta como una herramienta científica sumamente valiosa. (Shuttleworth, 2020)

Respecto al método aplicado, se escogió como el método más pertinente, las entrevistas aplicadas a profesionales del derecho especialistas en el campo de estudio, todo con el objetivo de recopilar información acerca de la problemática establecida, el conocimiento que poseen y la perspectiva acerca de la problemática permite que la información obtenida sea de gran relevancia para el análisis de la problemática.

## 2.4. Universo y Muestra de la Investigación

El universo de esta investigación son los profesionales del derecho especializados en el objeto de estudio, a los cuales se les realizara entrevistas para recopilar información y conocer su perspectiva.

La muestra se establece en recopilar información de las personas a las cuales se les aplicara las entrevistas, los cuales se encuentran especializados en el ámbito penal direccionados a los comentarios expuestos por los abogados especializados del tema en cuestión, los cuales se han visto envueltos en delitos electrónicos, específico en estafa por medio de las redes sociales. Debido a esto se decidió definir a las entrevistas como el método de recopilación de información.

Según los datos del Consejo de la Judicatura, en el Sistema Informático del Foro de Abogados se encuentra registrados un total de 20.714 abogados en la Provincia del Guayas, siendo estos la población de la presente investigación.

Por tanto, con un nivel de confianza del 95% estableciendo que la población de estudio son los 20.714 abogados registrados en el Consejo de la Judicatura y con un margen de error del 47% que se justifica con los abogados que no son

especialistas en las materias mencionadas, así como aquellos que han fallecido o ya no ejercen la profesión, pero no han dado de baja su registro, el tamaño de la muestra es 5, número que represente al 0,024% de la población.

## 2.5. Métodos empleados

### 2.5.1. Métodos empíricos

### 2.5.2. Entrevistas

La entrevista constituye un método para recopilar información que posibilita conocer las perspectivas de especialistas en el campo de estudio. Al interactuar con profesionales expertos en derechos vinculados al tema de investigación, se busca adquirir la información esencial para alcanzar los objetivos de esta investigación. (Bertomeu, 2019)

Según señala José Brunner (Gauna, 2020) “La interacción entrevistadora nos conecta con individuos de importancia en nuestras vidas, brindándonos la oportunidad de sumarnos a sus diálogos. A partir de este proceso, podemos formular una premisa inicial acerca de la función de las entrevistas. Podemos afirmar que contribuyen a enriquecer los intercambios sociales que constantemente se desarrollan en la sociedad, ampliando la influencia de ciertos interlocutores destacados”.

En la exploración de cuestiones particulares, resulta fundamental identificar individuos expertos o reconocidos como 'autoridades' que puedan ofrecer opiniones fundamentadas. De este modo, se genera la imperiosa tarea de conectar a los lectores con los actores clave de la noticia o con especialistas, propiciando un diálogo social que contribuirá en última instancia a fortalecer o ajustar ciertos patrones presentes en el debate público. (Vera, 2015)

En este estudio en particular, se empleará la entrevista a profundidad como herramienta principal para recopilar información. Este método facilita la comprensión de las perspectivas del entrevistado con respecto al problema propuesto desde una perspectiva cualitativa. De esta manera, se obtendrá información directamente relacionada con su experiencia profesional, sus conceptos, opiniones jurídicas y evaluaciones acumuladas a lo largo de su carrera como abogado.

### 2.6. Procesamiento y análisis de la información

Para llevar a cabo la investigación, se adoptará un enfoque cualitativo con el objetivo de comprender y analizar en detalle las particularidades de la problemática en cuestión. Inicialmente, se llevará a cabo la recopilación de información mediante la consulta de fuentes bibliográficas, como artículos científicos, libros de derecho y normativas tanto nacionales como internacionales.

Después de recopilar la información, se aplicará el enfoque empírico para obtener datos directos mediante la realización de entrevistas a expertos en el ámbito de los adolescentes infractores. Estos especialistas, basándose en su experiencia y conocimientos, proporcionarán información crucial y fundamental para llevar a cabo la investigación actual.

# CAPITULO III

## ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

## 3.1. Análisis e interpretación de resultados

**PRIMERA ENTREVISTA**

**Abg. Alex López Ávila.**

Magister en Derecho Constitucional; en Criminalística y Ciencias forenses, Victimología, delincuencia y criminología

Abogado; Fiscal y Docente en Derecho Penal, Procesal Penal y Criminalística de la Universidad Tecnológica Ecotec.

1. **¿Qué comentario puede usted aportar referente a la estafa a través de las redes sociales?**

Es un tema que ha sido común dentro de la materia de propiedad, la estafa se ha ido amoldando a los cambios de tecnología por ser antes realizadas de forma presencial, era lo más común como el cambiazo o el cheque; sin embargo, hoy en día existe un sin número de estafas vía internet como el pharming, hay más variedades por sustracción de dinero que se encasilla en estafa, pero son relaciones exclusivamente por computadoras o en muchos casos por cajeros digitales.

2. **¿Cuál es su criterio respecto a que Ecuador no sea partícipe del Convenio de Budapest?**

Hay que tomar un punto muy importante, hace un tiempo atrás se reconsideraba importante para irse adaptando a la tecnología e impartiendo por los soportes de Budapest, incluyendo sus protocolos por destacar, lo cual hoy en día se interesa porque en cierta parte la legislación del convenio de Budapest se ha hecho con las reformas del 12 de mayo en el Código Orgánico, algunos puntos del convenio como la mayor relevancia es la adaptación de la realidad jurídica a los tipos de protocolos que nos otorga la ayuda de manera internacional.

3. **Desde su experiencia ¿Podría ser reconsiderada la reforma dentro de la normativa penal buscando una reparación económica hacia la víctima?**

La reparación es de acuerdo a la sentencia, por no ser determinado un culpable ante dicho caso expuesto que se llegue a presentar, el mismo sería vulnerar el principio de inocencia si no ha existido una sentencia dictaminada como tal, es así, que no se encuentra posible interponer una reparación económica hasta que no se dictamine la sentencia de la misma.

4. **Desde su punto de vista ¿Qué situación podría generar que exista la implementación de la propuesta mencionada en el sistema judicial?**

El artículo 78 del COIP determina reparaciones integrales, incluyendo los materiales si llega a ser el caso en buscar un adelanto de la reparación total hacia la víctima debe ser reconsiderada una conciliación en el artículo 663 para llegar a un acuerdo, por superar los 5 años solicitando una anticipación.

5. **Desde su criterio ¿Qué otra opción sería considerada con el fin de obtener la reparación total de la víctima, por los delitos de estafa por medio de las redes sociales?**

A partir de los comentarios anteriores, se determina que no se encuentra otro tipo de reparación en lo que respecta a la víctima por encontrarse ya tipificado en la norma, no se verifica una nueva recomendación a la misma.

**SEGUNDA ENTREVISTA**

**Abg. Galo Monroy Oñate**

Abogado en la materia penal graduado en la Universidad Guayaquil.

1. **¿Qué comentario puede usted aportar referente a la estafa a través de las redes sociales?**

El problema que ha llegado a surgir a partir se ve involucrado el avance de la tecnología, de ese mismo modo se ha determinado nuevos métodos con el fin de delinquir y vulnerar el bien jurídico protegido siendo en este caso, el patrimonio de la víctima, cabe destacar que al ser un delito un poco reciente la normativa penal la

tipifica por lo que hoy en día, sin embargo, al momento de buscar un culpable ante dicha problemática no es posible hallarlo, siendo los casos donde los mismos cometen dichas acciones en diferentes partes del mundo.

2. **¿Cuál es su criterio respecto a que Ecuador no sea partícipe del Convenio de Budapest?**

Referente al tema de Budapest, es una discusión que ha sido determinada en base a los últimos años y aunque el protocolo no es nuevo a la fecha, Ecuador no ha buscado ser partícipe al mismo por el cual se ha buscado determinar el propósito del mismo, siendo una opción fáctica al momento de hacer cara ante dichos problemas jurídicos modernos.

3. **Desde su experiencia ¿Podría ser reconsiderada la reforma dentro de la normativa penal buscando una reparación económica hacia la víctima?**

Lo comparto, dentro del artículo 186 del COIP debe ser considerada en el mismo delito la reparación económica buscando la totalidad de la misma víctima, aparte de buscar el bienestar y salvaguardar los derechos de la víctima que en su momento fueron violentados.

4. **Desde su punto de vista ¿Qué situación podría generar que exista la implementación de la propuesta mencionada en el sistema judicial?**

Si, al mencionar el comentario anterior es de menester comprender la infinidad de perjuicios que se llega a cometer referente al delito en mención debe ser reconsiderado dicha propuesta para solución de la misma.

5. **Desde su criterio ¿Qué otra opción sería considerada con el fin de obtener la reparación total de la víctima, por los delitos de estafa por medio de las redes sociales?**

Volvería a reiterar la propuesta del convenio de Budapest como tal, siendo la misma primordial para la obtención de resultados.

**TERCERA ENTREVISTA**

**Ab. José Alberto Garcés Solá**

1. **¿Qué comentario puede usted aportar referente a la estafa a través de las redes sociales?**

Con el avance de la tecnología, las personas tienen acceso a eventos actuales en diferentes hechos, es por lo que, el comercio ha tenido un gran avance en posicionar las mercaderías o negocios a disposición directa de la sociedad, acto que ha generado también el incremento masivo en el delito de estafa, y, por medio de las redes sociales se ha visto que se han creado mecanismos para confundir, persuadir y perjudicar por medio de un aparente acto comercial; en este sentido es necesario indicar que, la tecnología es buena pero la sociedad sigue siendo ingenua por falta de conocimiento en dar información personal.

**2.- ¿Cuál es su criterio respecto a que Ecuador no sea partícipe del Convenio de Budapest?**

El convenio de Budapest es estrictamente relacionado con los delitos electrónicos o más bien informáticos, este convenio es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente en delitos informáticos y el Ecuador debe efectuar la suscripción del Convenio de Budapest para estar a la vanguardia en la defensa de los intereses de sus ciudadanos con la finalidad de precautelar y salvaguardar los derechos de todo el país.

**3.- Desde su experiencia ¿Podría ser reconsiderada la reforma dentro de la normativa penal buscando una reparación económica hacia la víctima?**

Debería reformarse la norma penal considerando que esta busca como objetivo primario establecer un ejercicio punitivo y preventivo en el que se entiende conocida por los ciudadanos que ciertos actos efectuados son considerado ilícitos y su castigo es con una pena privativa de libertad y el resarcimiento económico hacia la víctima quien es la persona que recibió de manera directa la acción o en su defecto la omisión del hecho ilícito; por ende, el resarcimiento de daños y perjuicios va íntimamente arraigado con la pena impuesta o determinada en los grados de participación penal.

**4.- Desde su punto de vista ¿Qué situación podría generar que exista la implementación de la propuesta mencionada en el sistema judicial?**

Precautelaría a los sistemas informáticos de las personas tanto naturales como jurídicas, públicas o privadas, generando un mayor aseguramiento en la prevención y/o sanción en el evento de vulneración de estos sistemas.

**5.- Desde su criterio ¿Qué otra opción sería considerada con el fin de obtener la reparación total de la víctima, por los delitos de estafa por medio de las redes sociales?**

En realidad, cualquier delito sea o no por redes sociales necesita que la víctima sea reparada, de la misma manera hay que tener presente el daño ocasionado mediato e inmediato considerando que en este obrar no podemos establecer solo culpa si no que lleva implícito un acto doloso y al ser doloso se debe no solo contemplar los hechos acaecidos si no las consecuencias a futuro de este obrar que fue perjudicada la víctima.

## Cuarta entrevista

**Ab. Anghelo Armijos Romero, abogado en UTPL y maestría en Derecho Procesal en la Universidad ECOTEC.**

1. **¿Qué comentario puede usted aportar referente a la estafa a través de las redes sociales?**

Con el progreso tecnológico, las personas pueden acceder a información actualizada sobre diversos eventos. Como resultado, el ámbito comercial ha experimentado un notable avance al colocar productos y negocios directamente al alcance de la sociedad. Sin embargo, esta evolución también ha propiciado un aumento significativo en los casos de estafa. A través de las redes sociales, se observa la creación de estrategias destinadas a confundir, persuadir y perjudicar mediante tácticas que simulan ser transacciones comerciales legítimas. En este contexto, es crucial señalar que, si bien la tecnología aporta beneficios, la sociedad sigue siendo vulnerable debido a la falta de conocimiento al proporcionar información personal.

2. **¿Cuál es su criterio respecto a que Ecuador no sea partícipe del Convenio de Budapest?**

El Convenio de Budapest guarda una estrecha relación con los delitos electrónicos o, más precisamente, los delitos informáticos. Este acuerdo internacional tiene como objetivo combatir el crimen organizado transnacional, centrándose específicamente en las infracciones relacionadas con la informática. Es imperativo que Ecuador firme el Convenio de Budapest para posicionarse en la vanguardia en la protección de los intereses de sus ciudadanos, con el propósito de precautelar y salvaguardar los derechos de toda la nación.

3. **Desde su experiencia ¿Podría ser reconsiderada la reforma dentro de la normativa penal buscando una reparación económica hacia la víctima?**

La reforma de la normativa penal debería contemplar su objetivo principal de establecer tanto un castigo como una medida preventiva. Es esencial que los ciudadanos estén conscientes de que ciertos actos son considerados ilegales y conllevan sanciones, como la privación de libertad y la obligación de compensar económicamente a la víctima, quien ha sufrido directamente el acto ilícito. Por lo tanto, la compensación por daños y perjuicios está estrechamente vinculada a la pena impuesta o determinada en los diferentes grados de participación penal.

4. **Desde su punto de vista ¿Qué situación podría generar que exista la implementación de la propuesta mencionada en el sistema judicial?**

Protegería los sistemas informáticos de individuos y entidades, ya sean de naturaleza pública o privada, con el objetivo de fortalecer la seguridad y facilitar medidas preventivas o sanciones en caso de violación de dichos sistemas.

5. **Desde su criterio ¿Qué otra opción sería considerada con el fin de obtener la reparación total de la víctima, por los delitos de estafa por medio de las redes sociales?**

En verdad, cualquier infracción, ya sea a través de plataformas digitales o no, requiere que se repare el daño causado a la víctima. Asimismo, es fundamental tener en cuenta tanto las repercusiones inmediatas como las a largo plazo de dicha conducta

delictiva. En este contexto, resulta insuficiente atribuir únicamente culpa, ya que el acto conlleva elementos dolosos. Al tratarse de un comportamiento doloso, es esencial considerar no solo los eventos pasados, sino también las consecuencias futuras de la afectación sufrida por la víctima.

## QUINTA ENTREVISTA

**Abg. José Sanchez Vallejo, maestría en Derecho Constitucional y Derecho de investigación.**

1. **¿Qué comentario puede usted aportar referente a la estafa a través de las redes sociales?**

Con el avance tecnológico, las personas pueden acceder fácilmente a información actualizada sobre una variedad de eventos, lo que ha llevado a un notable progreso en el ámbito comercial al poner productos y negocios directamente al alcance de la sociedad. Sin embargo, esta evolución también ha dado lugar a un aumento significativo en los casos de estafa. A través de las redes sociales, se observa la implementación de estrategias diseñadas para confundir, persuadir y perjudicar mediante tácticas que simulan ser transacciones comerciales legítimas. Es esencial destacar en este contexto que, aunque la tecnología ofrece beneficios, la sociedad sigue siendo vulnerable debido a la falta de conocimiento al proporcionar información personal.

2. **¿Cuál es su criterio respecto a que Ecuador no sea partícipe del Convenio de Budapest?**

El Convenio de Budapest está directamente vinculado a los delitos electrónicos, específicamente a los delitos informáticos. Su finalidad es abordar el crimen organizado a nivel transnacional, poniendo un énfasis particular en las violaciones vinculadas a la informática. Es esencial que Ecuador ratifique el Convenio de Budapest para situarse en la vanguardia en la protección de los intereses de sus ciudadanos, con el objetivo de resguardar los derechos de un país.

3. **Desde su experiencia ¿Podría ser reconsiderada la reforma dentro de la normativa penal buscando una reparación económica hacia la víctima?**

La modificación de la legislación penal debe tener como objetivo principal la instauración tanto de una sanción como de una medida de prevención. Resulta fundamental que los ciudadanos estén conscientes de que ciertos comportamientos son considerados ilícitos y conllevan consecuencias legales, como la privación de libertad y la obligación de resarcir económicamente a la víctima que ha sufrido directamente el acto ilegal. De este modo, la compensación por daños y perjuicios está estrechamente ligada a la pena impuesta o establecida en los diferentes niveles de participación delictiva.

4. **Desde su punto de vista ¿Qué situación podría generar que exista la implementación de la propuesta mencionada en el sistema judicial?**

Garantizaría la seguridad de los sistemas informáticos tanto en el ámbito público como privado, con la finalidad de reforzar su protección y facilitar la implementación de medidas preventivas o sanciones en caso de que se produzca una infracción en dichos sistemas.

5. **Desde su criterio ¿Qué otra opción sería considerada con el fin de obtener la reparación total de la víctima, por los delitos de estafa por medio de las redes sociales?**

Realmente, cualquier transgresión, ya sea a través de medios digitales o no, demanda la reparación de los perjuicios causados a la persona afectada. Además, es crucial tener en cuenta tanto las repercusiones inmediatas como las de largo plazo de dicha conducta ilegal. En este contexto, asignar exclusivamente culpabilidad resulta insuficiente, dado que la acción involucra elementos intencionales. Al tratarse de un comportamiento con intenciones dañinas, es esencial considerar no solo los eventos pasados, sino también las consecuencias futuras de la afectación sufrida por la víctima.

## 3.2. Interpretación de resultados

En base a las entrevistas realizadas a profesionales del derecho especializados en las áreas penal y constitucional, se llevó a cabo un análisis considerando sus perspectivas, opiniones y experiencias. El objetivo fue obtener información significativa sobre el tema investigado, la cual es conocida por ellos gracias a su trayectoria, formación y experiencia en dichas áreas.

En la primera pregunta realizada, todos los entrevistados mostraron conocimiento acerca de la estafa por medio de las redes sociales, llegando a observar que definen como la consecuencia de un avance tecnológico que genera cada vez más controversia respecto al tema, la misma que ha sido determinada a partir de los conocimientos en los distintos conocimiento que poseía cada profesional sobre el tema dando un resultado del amplio conocimiento que llega a la misma interrogativa referente al estudio del tema, verificando cada respuesta llega a una conclusión al encontrar inconvenientes sobre dicha práctica la falta de conocimiento que tiene la Sociedad referente al tema a tratar . En la pregunta número 2, los entrevistados expusieron estar en total acuerdo la suscripción que debe ser impuesta por Ecuador para ser partícipe del protocolo que tiene como fin combatir el crimen organizado, transnacional, específicamente en delitos informáticos dando como resultado una alianza internacional. Sin embargo, el entrevistado número 1 indicó que la norma reformas del 12 de mayo en el Código Orgánico, algunos puntos del convenio como la mayor relevancia es la adaptación de la realidad jurídica. A diferencia de los 4 entrevistados acordar encontrarse en concertación sobre la pregunta en cuestión.

Según la 3 pregunta, el entrevistado 1 tuvo indiferencia indicando que dicha propuesta se encuentra sujeta al artículo 78 del COIP como referencia a dicha solución, no obstante, los 4 entrevistados encontraron una conclusión indicando que en dicha pena privativa debe ser reconsiderada en la misma la reparación total de la víctima. Según la cuarta pregunta la autora observa que todos los entrevistados manifestaron comentarios similares indicando precautelar los sistemas informáticos de las personas tanto naturales como jurídicas, públicas o privadas, generando un mayor aseguramiento en la prevención.

En la pregunta número cinco, se pudo observar opiniones divididas entre los entrevistados donde el entrevistado 1 manifestó dicha solución en los artículos 78 del COIP o llegar a la conciliación por medio del artículo 663 de la misma norma, a diferencia de los entrevistados 2, 3 y 4 resguardando sus opiniones anteriores en torno a la problemática hay que tener presente el daño ocasionado mediato e inmediato considerando que en este obrar no podemos establecer solo culpa si no que lleva implícito un acto doloso y al ser doloso se debe no solo contemplar los hechos acaecidos si no las consecuencias a futuro de este obrar que fue perjudicada la víctima.

## 3.3. Interpretación de las entrevistas

Los participantes han reconocido la vulnerabilidad que presenta las víctimas por estafa por redes sociales, se afirma que van más allá del alcance de la normativa penal aquellos sistemas informáticos que, en lugar de las cerraduras convencionales, desempeñan simplemente una función de protección. Esto se aplica a los mecanismos electrónicos de apertura y cierre, que a veces operan mediante tarjetas magnéticas. La mención de estas barreras tecnológicas no implica, por lo tanto, un beneficio injusto por parte del agente, sino que simplemente facilita la posibilidad de llevar a cabo acciones agresivas contra la propiedad ajena.

Adicionalmente, se identifican la aceptación en base a la coordinación de las respuestas por la suscripción de Ecuador en el Convenio de Budapest siendo una vía óptima con el objetivo de disminuir la presencia de estos nuevos delitos electrónicos, promoviendo la cooperación entre países extranjeros.

En resumen, las entrevistas enfatizan la complejidad que existe dentro del caso en mención donde está en revisión la vulnerabilidad de la víctima a su patrimonio, sin embargo, existen desafíos que necesitan ser abordados para garantizar un crecimiento equitativo y eficaz en la ciudad.

# CAPÍTULO IV
# PROPUESTA

## Propuesta

### “RESTAURACIÓN ECONÓMICA COMO MEDIDA DE REPARACIÓN”

La estafa gracias a los progresos en la ciencia informática, la observación de conductas podrá llevarse a cabo de manera sencilla, evitando que se convierta en un

procedimiento imposible o, al menos, que dificulte al máximo su implementación. Con el objetivo de encontrar una mejora a la solución que conlleva dicha problemática, se propone la revisión del artículo 186 del Código Orgánico Integral Penal adecuando el mismo con su verificación una reparación total, en dicho caso económica una vez dictaminada la sentencia por prisión preventiva.

En Ecuador, la investigación enfrenta desafíos significativos debido a la ausencia de acuerdos internacionales que permitan el intercambio fluido de datos informáticos, como los existentes entre Estados Unidos y Europa. Se presenta dificultad para identificar las cuentas o direcciones IP asociadas a delitos o la apropiación indebida de información personal, y los procedimientos legales pueden demorarse debido a la falta de rapidez en la tramitación.

En mención al anterior párrafo, se propone la suscripción inmediata de Ecuador al Convenio de Budapest, en términos generales, el Convenio ha sido bien recibido a nivel global, aunque ciertos Estados han optado por no unirse debido a su preferencia por la regulación de la cooperación internacional y los temas de ciberdelincuencia a través de tratados regionales que se adapten a las particularidades y necesidades de cada región. En este contexto, la incidencia y progreso de la ciberdelincuencia en América Latina se considera menor en comparación con algunos países de Asia o Europa.

En relación con la propuesta legislativa, la promulgación de una ley posibilitaría la inclusión en nuestro sistema jurídico de las atribuciones y procesos mencionados previamente, con el fin de garantizar una ejecución eficiente de las operaciones en beneficio de la población afectada.

Finalmente, se destaca la necesidad de tener una firme determinación política para llevar a cabo la ejecución de este proyecto de investigación, con el propósito de impulsar la legislación correspondiente que aplique eficientes estrategias contra las organizaciones delictivas, que perjudican extensamente a nuestra población desprotegida mediante estafas masivas.

La propuesta final de reforma al artículo 186 del Código Orgánico Integral Penal tiene como objetivo consolidar un marco legal sólido que promueva la reparación total de la víctima por el delito de estafa. Al poner énfasis en la precisa definición de principios, la asignación específica de recursos, la participación activa de los ciudadanos, la evaluación de los resultados, el fortalecimiento de las habilidades y el establecimiento de medidas de rendimiento, se busca asegurar un manejo equitativo, transparente y eficaz de los recursos públicos para promover el desarrollo.

## JUSTIFICACIÓN DE LA PROPUESTA

En razón a lo observado dentro del presente trabajo de investigación se ha determinado la existencia de la reparación total incluyendo la económica hacia la víctima, confirmando el problema al no existir un resguardo total en mención a la problemática por justificar, la afectación al bien jurídico que se presenta es alarmante en cuanto al patrimonio por la aplicación a ella.

Por otra parte, es necesario examinar otras alternativas que permitan evitar encontrar la compensación de la persona afectada ante el delito de estafa por medio de las redes sociales, por ende, el objetivo general se enfoca en establecer una propuesta relación a la información obtenida y analizada.

Dentro de esta orden de ideas, la cual permitirá disminuir la vulnerabilidad del derecho de la víctima el cual se encuentra vulnerado su patrimonio afectado por el cometimiento de este tipo de delitos.

# Conclusión

En el transcurso de la investigación, he obtenido diversas conclusiones que puedo exponer de la siguiente manera: A lo largo de la historia, el delito de estafa ha experimentado una evolución hacia su autonomía, ya que desde sus inicios se ha visto inmerso en una serie de artimañas engañosas que se han reducido con el paso de los años, configurándose como un delito que se distingue de otras infracciones que también definen un tipo penal que castiga acciones contrarias a la propiedad.

La comisión del delito de estafa, al ser fundamentalmente intencional, requiere que se demuestre la intención de obtener beneficios por parte del perpetrador, lo que resulta en un enriquecimiento a expensas del patrimonio de la víctima, quien, al incurrir en un error, cedió su propiedad.

En consecuencia, puede deducirse que la infracción, al incorporar el componente de engaño de manera restringida para abarcar solo casos pertinentes y conductas específicas que sean verdaderamente de último recurso, debería ser definida de manera más precisa y específica por parte del legislador. Esto resultaría en una tipificación del delito que se centre únicamente en describir conductas en las que el engaño sea apropiado, dando lugar a un artículo más sólido y menos susceptible a interpretaciones amplias.

## Recomendaciones

Dada la evolución histórica del delito de estafa y su autonomía creciente, se recomienda que los legisladores la revisión y actualización de las leyes correspondientes para garantizar una adecuada tipificación y sanción de las conductas fraudulentas. Esto permitirá adaptar la legislación a las nuevas formas de estafa que puedan surgir con los avances tecnológicos y sociales.

A partir de la naturaleza transnacional de muchas estafas en la era globalizada, se sugiere fomentar la cooperación internacional entre los sistemas judiciales y las fuerzas del orden. Acuerdos de colaboración e intercambio de información podrían facilitar la persecución de estafadores que operan más allá de las fronteras nacionales.

Con el fin de fortalecer la capacidad de las autoridades en la lucha contra la estafa, se recomienda implementar medidas que incentiven a las víctimas a denunciar estos delitos. Esto podría incluir garantías de protección a los denunciantes y la simplificación de los procesos para reportar casos de fraude.

## BIBLIOGRAFIA

## Bibliografía

*Los delitos informáticos con pena de prisión.* (2021). Obtenido de https://dplnews.com/ecuador-los-delitos-informaticos-con-pena-de-prision/

(2022)., C. N. (s.f.). *Cámara Nacional de Acuacultura*. Obtenido de Estadísticas Camarón Ecuatoriano.: https://www.cna-ecuador.com/estadisticas/

Abarca., L. D. (2020). Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales.

Altamirano, A. (s.f.). *La estafa como un instrumento de la corrupción social.* Fiscalía Provincial de Tungurahua, DGPP, Tungurahua.

*Arrimadas Abogados.* (2021). Obtenido de https://www.arrimadasabogados.es/blog/el-delito-de-estafa-y-la-evolucion-del-engano-arrimadas-abogados-logrono/

*ASOBANCA.* (2021). Obtenido de https://asobanca.org.ec/cuidado-con-el-phishing-no-muerda-el-anzuelo/

Banco Central del Ecuador Subgerencia de Análisis de Productos y Servicios. (2020). *Camarón Ecuatoriano en el Mundo.*

Bertomeu, P. F. (2019). Obtenido de https://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

Briceño, J. B. (2023). *La evolución histórico-dogmática de la estafa procesal en España y Alemania*. Obtenido de https://indret.com/la-evolucion-historico-dogmatica-de-la-estafa-procesal-en-espana-y-alemania/

Caeiro, R. E. (2021). *Documentación de impactos y el método Eslabones de Incidencia. Posibilidades de aplicación INTA.* Buenos Aires: Ediciones INTA; Estación Experimental Agropecuaria Catamarca. Recuperado el 30 de mayo de 2022, de http://hdl.handle.net/20.500.12123/10324

CAROLINA, A. Z. (2023). *EL DELITO DE ESTAFA EN REDES SOCIALES Y EL IMPACTO EN LA SOCIEDAD ECUATORIANA.* Obtenido de https://dspace.uniandes.edu.ec/bitstream/123456789/16548/1/USD-DER-EAC-032-2023.pdf

Carrasco, J. B. (2011). *Gestión de procesos (Alineados con la estrategia).*

Casillas, L. (8 de noviembre de 2022). *El poder del miedo: El auge del fraude relacionado con la pandemia.* Obtenido de https://es.clear.sale/blog/el-poder-del-miedo-el-auge-del-fraude-relacionado-con-la-pandemia

CFN - Subg. De Análisis de Productos y Servicios. (2020). *EXPLOTACIÓN DE CRIADEROS, PREPARACIÓN Y CONSERVACIÓN, ELABORACIÓN DE PREPARADOS Y VENTAS AL POR MAYOR DE CAMARÓN Y LANGOSTINOS.* GUAYAQUIL.

CÓDIGO ORGÁNICO INTEGRAL PENAL, C. (2023). *LEXIS.* Obtenido de https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

Crespo, H. F. (30 de junio de 2021). *El delito de estafa en el Código Orgánico Integral Penal.* Obtenido de file:///C:/Users/1/Downloads/17095.pdf

Crespo, H. F. (s.f.). Análisis del tipo penal y las reformas del 2019. En H. F. Crespo. Revista Derecho Penal Central.

Crespo, H. F. (s.f.). *El delito de estafa en el Código Orgánico Integral Penal. Breve análisis del tipo penal y las reformas del 2019.* Obtenido de https://revistadigital.uce.edu.ec/index.php/derechopenal/article/view/3341

Cuatrecasas, L. (2017). *Ingeniería de Procesos y de Planta. Ingeniería Lean.* Barcelona: Profit Editorial I. S.L. .

CUNICH, J. A. (2021). *Fases de desarrollo del delito de estafa con atención a sus elementos típicos, especialmente el perjuicio, a la luz de la Jurisprudencia de la Corte Suprema.* Obtenido de https://repositorio.uchile.cl/bitstream/handle/2250/189630/Fases-de-desarrollo-del-delito-de-estafa-con-atencion-a-sus-elementos-tipicos-especialmente-el-perjuicio-a-la-luz-de-la-jurisprudencia.pdf?sequence=1

*Delito Informático. Procedimiento Penal en Ecuador* . (2019). Obtenido de file:///C:/Users/1/Downloads/Dialnet-DelitoInformaticoProcedimientoPenalEnEcuador-5761561.pdf

DÍAZ GÓMEZ, A. (2010). *El Convenio de Budapest.* Obtenido de https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

diciembre, C. s. (2023). *PRIMICIAS*. Obtenido de https://www.primicias.ec/noticias/sucesos/ciberdelitos-suben-navidad-ecuador-guia/

DONNA, E. A. (2021). *Bien jurídico protegido*. Obtenido de http://historico.juridicas.unam.mx/publica/rev/revlad/cont/1/art/art3.htm

Equipo editorial, E. (5 de agosto de 2021). *Concepto*. Obtenido de Concepto: https://concepto.de/conclusion/

FGE. (2015). Obtenido de https://www.fiscalia.gob.ec/secciones/boletines/2015-boletines/page/68/

*FISCALIA GENERAL DEL ESTADO.* (2023). Obtenido de https://www.fiscalia.gob.ec/fiscalia-obtiene-sentencia-por-los-delitos-de-acceso-no-consentido-a-un-sistema-informatico-telematico-o-de-telecomunicaciones-y-revelacion-ilegal-de-base-de-datos/

*FRAUDE, CORRUPCIÓN Y UTILIZACIÓN INDEBIDA DE LOS RECURSOS*. (2022). Obtenido de https://weareallin.iom.int/es/fraude-corrupcion-y-utilizacion-indebida-de-los-recursos

Fresneda, S. C. (2022). *DEXIA ABOGADOS.* Obtenido de https://www.dexiaabogados.com/blog/estafa/

Gauna, W. R. (2020). Obtenido de https://perio.unlp.edu.ar/catedras/graficadepor/wp-content/uploads/sites/166/2020/07/2-La-entrevista-Mego-Romeo-Gauna.pdf

Gómez, D. B. (11 de junio de 2022). *Estafas virtuales: cuáles son los delitos más comunes y cómo prevenirlos.* Obtenido de https://www.infobae.com/economia/2022/06/12/estafas-virtuales-cuales-son-los-delitos-mas-comunes-y-como-prevenirlos/

Gomezjurado Gomezjurado, J. D. (2023). *ESTAFA;MEDIOS ELECTRÓNICOS;AUTORIA;CIBERDELINCUENCIA*. Obtenido de https://repositorio.uide.edu.ec/handle/37000/5790

GUSQUI, V. S. (2020). *ANÁLISIS DEL DELITO DE ESTAFA EN REDES SOCIALES EN MEDIOS ELECTRÓNICOS.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/53108/1/Tenesaca%20Vanesa-Cede%c3%b1o%20Italo%20BDER-TPrG%20040-2021.pdf

H., B. R. (2004). *Logística. Administración de la cadena de suministro.* . México: Pearson Educación.

Harán, J. M. (2020). *Crece el ecommerce y aumentan las estafas y los incidentes de seguridad.* Obtenido de https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

hernánfartocrespo. (2019). *El delito de estafa en el Código Orgánico Integral Penal.* Obtenido de https://revistadigital.uce.edu.ec/index.php/derechopenal/article/view/3341/4121

Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. (2020). En I. N. Toledo, & L. V. Cruz..

Institute, L. I. (2022). Obtenido de https://www.law.cornell.edu/wex/es/fraude_cibern%C3%A9tico_e_inform%C3%A1tico

INTERPOL. (2020). *Evolución de las tendencias y amenazas en materia de ciberdelincuencia durante la COVID-19.* Obtenido de file:///C:/Users/1/Downloads/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Jácome, A. I., & Briones, M. J. (2022). *La aplicación de la teoría de la imputación objetiva en el delito de estafa en el Ecuador.* Obtenido de https://repositorio.uotavalo.edu.ec/xmlui/handle/52000/792

La responsabilidad bancaria frente a los delitos informáticos . (2021). Quito.

León Felipe, G. (24 de septiembre de 2020). *Delincuencia en tiempos de coronavirus. Estafas y ciberdelitos.* Obtenido de https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delincuencia-en-tiempos-de-coronavirusbr-estafas-y-ciberdelitos-2020-09-24/

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

Los ciberdelitos como estafas en línea y promociones falsas se disparan hasta en un 35% en diciembre. (21 de diciembre de 2022). pág. 12.

Mundo, B. N. (2021). *3 nuevos fraudes y estafas surgidos por la pandemia del coronavirus.* Obtenido de https://www.bbc.com/mundo/noticias-55927424

Novik, M. (2021). *Fraudes digitales: cuenteros y estafadores operan con redes sociales*. Obtenido de https://www.planv.com.ec/historias/sociedad/fraudes-digitales-cuenteros-y-estafadores-operan-con-redes-sociales

Padilla, M. P. (2022). *La responsabilidad bancaria frente a los delitos informáticos* . Obtenido de file:///C:/Users/1/Downloads/T1631-MDE-Martinez-La%20responsabilidad.pdf

Padilla, M. P. (2022). *MENCION EN DERECHO FINANCIERO, BURSATIL Y DE SEGUROS.* Obtenido de file:///C:/Users/1/Downloads/T1631-MDE-Martinez-La%20responsabilidad.pdf

pandemia, A. a. (7 de junio de 2021). *COMERCIO Y JUSTICIA.* Obtenido de https://comercioyjusticia.info/tecnologia/advierten-aumento-de-estafas-electronicas-a-traves-de-las-redes-sociales-en-pandemia/

PAÚL, Y. R. (2023). *LA NO ADHESIÓN AL CONVENIO DE BUDAPEST* . Obtenido de https://dspace.uniandes.edu.ec/bitstream/123456789/16740/1/UT-DER-EAC-001-2023.pdf

*Pena máxima aplicada en los tipos delictivos.* (2015). Obtenido de file:///C:/Users/1/Downloads/famayorga,+Gestor_a+de+la+revista,+ART+6_La+estafa+como+un+instrumento+de+la+corrupci%C3%B3n+social.pdf

PENAL, G. (2022). *Estafas a través de Medios Informáticos*. Obtenido de https://www.garberipenal.com/3-tipos-de-estafas-comunes-a-traves-de-medios-informaticos/

Penal., E. d. (2019). Obtenido de file:///C:/Users/1/Downloads/17095.pdf

Pereyra Maita, L. A. (2020). Obtenido de https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3579/Luz%20Pereyra_Jessy%20Turpo_Trabajo%20de%20Investigacion_Bachiller_2020.pdf?sequence=1&isAllowed=y

Rendón, A. D. (2022). *DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR.* Obtenido de http://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

Roberto Hernández Sampieri, Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la Investigación. En *Metodología de la investigación* (pág. 91). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Rodas Soto, P. E. (2022). *El delito de apropiación fraudulenta por medios electrónicos en la ciudad de Guayaquil*. Obtenido de https://repositorio.ug.edu.ec/items/2a57af8c-04ff-40e0-bf4b-41bf9c0c1ce6

Ron, A. M. (2019). *DerechoEcuador.com*. Obtenido de https://derechoecuador.com/estafa-informatica/

Rosso Pérez, M. E. (29 de abril de 2022). *LegalToday*. Obtenido de https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delito-de-estafa-informatica-2022-04-29/

Sánchez, A. S. (2022). *LA ESTAFA INFORMÁTICA.*

Servicios, B. C. (2020).

Shuttleworth, M. (2020). *Diseño de Investigación Descriptiva*. Obtenido de https://explorable.com/es/diseno-de-investigacion-descriptiva

Superintendencia de Compañias Subgerencia de Análisis y Productos y servicios. (2020). *Análisis Sectorial Camarón.*

Tamaulipeca. (30 de junio de 2022). *Tamaulipeca*. Obtenido de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692022000100021

*Teoría general del delito de estafa.* (2020). Obtenido de https://dspace.uazuay.edu.ec/bitstream/datos/4725/1/08798.pdf

UNIVERSO, E. (2021). Conozca cuáles son los delitos informáticos con pena de prisión en Ecuador. pág. 15.

Vera, M. B. (2015). Obtenido de http://metabase.uaem.mx/bitstream/handle/123456789/1580/OP_324.pdf?sequence=1

W. Edwards Deming. (1982). *Out of the Crisis. Quality, productivity and Competitive Position.* Ediciones Díaz de Santos, S.A.