UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE CIENCIAS SOCIALES Y DERECHO.
CARRERA DE DERECHO

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO

TEMA

ENGAÑOS DIGITALES EN REDES SOCIALES Y MENSAJERÍA: NECESIDAD URGENTE DE APLICAR BIEN LA LEY PARA EVITAR IMPUNIDAD EN DELITOS INFORMÁTICOS.

TUTOR

Mgtr. ROXANNA RIVADENEIRA ARIAS

AUTORA

LITARDO GAONA CHELSEA KATIUSHKA

GUAYAQUIL 2025

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA	
FICHA DE REGISTRO DE TESIS	
TÍTULO Y SUBTÍTULO: **Engaños Digitales en Redes Sociales y Mensajería: Necesidad Urgente de Aplicar bien la Ley para evitar Impunidad en Delitos Informáticos.**	
AUTOR/ES: Litardo Gaona Chelsea Katiushka.	**TUTOR:** Mgtr. Rivadeneira Arias Roxanna
INSTITUCIÓN: Universidad Laica Vicente Rocafuerte de Guayaquil	**Grado obtenido:** Abogado
FACULTAD: Facultad De Ciencias Sociales Y Derecho.	**CARRERA:** Derecho
FECHA DE PUBLICACIÓN: 2025	**N. DE PÁGS:** 107
ÁREAS TEMÁTICAS: Derecho	
PALABRAS CLAVE: Inteligencia artificial, Medios electrónicos, Derecho Penal, Proteccion de datos.	
RESUMEN: Los delitos informáticos, particularmente los engaños digitales cometidos a través de medios electrónicos como redes sociales y servicios de mensajería, se han incrementado de forma sostenida en Ecuador durante los últimos cinco años, este crecimiento está relacionado con la baja alfabetización digital, la precariedad laboral y las secuelas económicas de la COVID-19, que empujaron a muchas personas a buscar ingresos en línea, los hicieron vulnerables a estafas potenciadas por recursos de inteligencia artificial capaces de suplantar identidades y persuadir a las víctimas.	

<table>
<tr><td colspan="3">La investigación se propone explicar por qué la respuesta del Derecho Penal ecuatoriano resulta insuficiente, a pesar de la existencia de una legislación que tipifica conductas como el fraude electrónico, en la práctica la reciente teoría legal suele encuadrar estos hechos como simples delitos patrimoniales, lo que dificulta sancionar a los responsables, con este objetivo se aplica una metodología cualitativa basada en la revisión crítica de sentencias nacionales e internacionales, doctrina especializada y entrevistas a operadores de justicia, para identificar los vacíos interpretativos que han favorecido la impunidad durante el último lustro, los hallazgos evidencian la falta de lineamientos uniformes para valorar evidencia digital y la escasa coordinación entre la persecución penal y la necesaria protección de datos personales comprometidos en las estafas.

En conclusión, urge consolidar criterios probatorios, fortalecer la formación técnica de fiscales y jueces, para aplicar con rigor los tipos penales informáticos, de modo que el sistema jurídico ecuatoriano pueda prevenir eficazmente los engaños digitales y salvaguardar los derechos de la ciudadanía en el entorno digital.</td></tr>
<tr><td>N. DE REGISTRO (en base de datos):</td><td colspan="2">N. DE CLASIFICACIÓN:</td></tr>
<tr><td colspan="3">DIRECCIÓN URL (Web):</td></tr>
<tr><td>ADJUNTO PDF:</td><td>SI [x]</td><td>NO [ ]</td></tr>
<tr><td>CONTACTO CON AUTOR/ES:

Chelsea Katiushka Litardo Gaona.</td><td>Teléfono:

0979238289</td><td>E-mail:

clitardog@ulvr.edu.ec</td></tr>
<tr><td>CONTACTO EN LA INSTITUCIÓN:

096 815 7284</td><td colspan="2">Mgtr. Carlos Manuel Pérez Leyva (Decano)

Teléfono: (04) 2596500 Ext. 250

E-mail: cperezl@ulvr.edu.ec

Mgtr. Geancarlos González Solorzano (Director de Carrera)

Teléfono: 0968546571

E-mail: ggonzalezso@ulvr.edu.ec</td></tr>
</table>

CERTIFICADO DE SIMILITUD

INFORME DE ANÁLISIS
magister

LITARDO GAONA CHELSEA KATHIUSKA

4% Textos sospechosos

- <1% Similitudes
  - <1% similitudes entre comillas
  - 0% entre las fuentes mencionadas
- 1% Idiomas no reconocidos
- 2% Textos potencialmente generados por la IA

Nombre del documento: LITARDO GAONA CHELSEA KATHIUSKA .pdf
ID del documento: 4054b39778920b269e96e09dc90dc0f63cb222c8
Tamaño del documento original: 1,15 MB

Depositante: Federico Varas Chiquito
Fecha de depósito: 15/8/2025
Tipo de carga: interface
fecha de fin de análisis: 15/8/2025

Número de palabras: 20.959
Número de caracteres: 141.625

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	hdl.handle.net | Práctica derecho penal: comentario de sentencias y casos prácti... http://hdl.handle.net/20.500.12226/1133 18 fuentes similares	<1%		Palabras idénticas: < 1% (82 palabras)
2	hdl.handle.net | Las tarjetas de crédito y débito. Aspectos penales http://hdl.handle.net/10366/121873 10 fuentes similares	<1%		Palabras idénticas: < 1% (51 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #7fadcb Viene de de otro grupo	<1%		Palabras idénticas: < 1% (38 palabras)
2	bit.ly https://bit.ly/3Htrigt	<1%		Palabras idénticas: < 1% (16 palabras)
3	www.ministeriodelinterior.gob.ec | Denuncia la extorsión - Ministerio del Interior https://www.ministeriodelinterior.gob.ec/canal-de-denuncias/	<1%		Palabras idénticas: < 1% (15 palabras)
4	www.orientanet.es | ¿Qué es la norma ISO 17025 2017 y para qué sirve? | Orien... https://www.orientanet.es/que-es-la-norma-iso-17025-2017-y-para-que-sirve/	<1%		Palabras idénticas: < 1% (10 palabras)
5	dicjuridico.com | dic jurídico | Consultoria Legal | El Delito de Extorsión en el Ec... https://dicjuridico.com/blogs/consultoria-legal-730/The-Crime-of-Extortion-in-Ecuador	<1%		Palabras idénticas: < 1% (10 palabras)

Roxanna Leslie Rivadeneira Arias

Time Stamping Security Data

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

La estudiante egresada LITARDO GAONA CHELSEA KATIUSHKA, declara bajo juramento, que la autoría del presente Trabajo de Titulación, "ENGAÑOS DIGITALES EN REDES SOCIALES Y MENSAJERÍA: NECESIDAD URGENTE DE APLICAR BIEN LA LEY PARA EVITAR IMPUNIDAD EN DELITOS INFORMÁTICOS", corresponde totalmente a la suscrita y me responsabilizo con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedo los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

Autora

Firma:

Litardo Gaona Chelsea Katiushka.

C.I. 0943987693

CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR

En mi calidad de docente Tutor del Trabajo de Titulación Engaños Digitales En Redes Sociales Y Mensajería: Necesidad Urgente De Aplicar Bien La Ley Para Evitar Impunidad En Delitos Informáticos, designado(a) por el Consejo Directivo de la Facultad de Ciencias Sociales y Derecho de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Trabajo de Titulación, titulado: Engaños Digitales En Redes Sociales Y Mensajería: Necesidad Urgente De Aplicar Bien La Ley Para Evitar Impunidad En Delitos Informáticos, presentado por el (los) estudiante (s) CHELSEA KATIUSHKA LITARDO GAONA como requisito previo, para optar al Título de Abogada, encontrándose apto para su sustentación.

Firma: 

Mgtr. Rivadeneira Arias Roxanna

C.I. 0927418137

AGRADECIMIENTO

Estoy agradecida con Dios, ante todo, por darme la oportunidad de dar un gran paso hacia mi futuro como profesional, Él me dio la fuerza, la paciencia y la luz para no rendirme incluso estando en la misma oscuridad, además de bridarme su calidez al momento de decir plegaria porque sentía que todo estaba en contra mí, pero nunca me dejaste sola siempre tuviste a mi lado.

Agradezco profundamente a mis padres, quienes han estado conmigo en cada etapa de mi carrera, dándome su apoyo y su amor incondicional, ustedes me animaban a seguir adelante, pase lo que pase, siempre haciéndome recordar que todo esfuerzo al final vale la pena, además quiero darles las gracias por el esfuerzo que tuvieron que invertir, los sacrificios que tuvieron dar, todo lo que tuvieron que pasar para brindarme a mí y a mis hermanos una educación, ustedes apostaron por mí, estoy feliz por eso, los estimo mucho.

A mis abuelitos, les agradezco de corazón por haberme brindado sus manos, su esmero y dedicación, además de no haberme dejarme caer nunca, aunque ciertas ocasiones estaba punto hacerlo, pero sus palabras de aliento, me hicieron mantenerme a flote, ustedes son y serán por siempre las personas las cuales les debo el amor y el cariño brindado durante todos estos años.

Le doy gracias a mi pareja, por acompañarme en mi travesía de aprendizaje, de aciertos y errores, eres la persona la cual ha estado conmigo desde el comienzo hasta el fin de mi carrera, de todo corazón te digo que estoy agradecida con Dios, por haberme dado la oportunidad de pasar con alguien que comparte pensamiento, ganas de seguir adelante y esmero en seguir estudiando.

También agradezco a todas las esas personas que formaron parte de este camino, llevado por mí, los que invirtieron su confianza en mi espalda cada día de mi vida, los que dejaron una gran huella de enseñanza en mi por eso quiero agradecerles desde el fondo de mi alma que nuestra Universidad Laica Vicente Rocafuerte, me siento feliz y agradecida de haber sido parte de una institución tan importante.

DEDICATORIA

Dedico este trabajo de titulación tesis, a Dios, a mis abuelos, a mis padres, hermanos, pareja y las personas a las cuales invirtieron su fe en mí, fue una lucha constante en la cual hubo caídas, levantadas y noches trasnochadas, pero al final todo lo que se ha pasado nos lleva a esta etapa final de mi carrera, del cual me siento llena de orgullo y feliz de haber dado mejor de mi para poder finalizarla.

Dentro de todo el periodo lectivo de mi carrera de derecho he conocido excelentes docentes, abogados y directivos, los cuales han invertido tiempo, esfuerzo y dedicación para poder enseñarme, guiarme, e instruirme en lo que desconocía.

Dedico a las personas los cuales han pasado por estos tipos de engaños digitales, quienes han visto la impunidad de la ley referente a estos delitos, sé que a veces queremos conseguir justicia debido a nuestro error mismo al confiar en que se puede ganar dinero de manera rápida por vías de mensajería o publicidad de las redes, pero no es así, debemos pensar dos veces antes de dar nuestros datos, porque a la larga esto produce un daño irreparable en nuestra economía y para nuestras familias.

Te dedico, esto Chelsea, pudimos con todo lo que se pudo atravesar, lo hemos logrado, nuestra dedicación y esfuerzo han dado frutos, desde ahora da lo mejor de ti, como siempre lo has hecho, confía en ti al igual que Dios lo hace, espero que sigas creciendo en conocimiento, nunca olvides quién eres y lo que has invertido por conseguir graduarte de la facultad de derecho, esmérate más estando afuera, ya que es un mundo muy competitivo, pero se que lo lograremos.

RESUMEN

Los delitos informáticos, particularmente los engaños digitales cometidos a través de medios electrónicos como redes sociales y servicios de mensajería, se han incrementado de forma sostenida en Ecuador durante los últimos cinco años, este crecimiento está relacionado con la baja alfabetización digital, la precariedad laboral y las secuelas económicas de la COVID-19, que empujaron a muchas personas a buscar ingresos en línea, los hicieron vulnerables a estafas potenciadas por recursos de inteligencia artificial capaces de suplantar identidades y persuadir a las víctimas.

La investigación se propone explicar por qué la respuesta del Derecho Penal ecuatoriano resulta insuficiente, a pesar de la existencia de una legislación que tipifica conductas como el fraude electrónico, en la práctica la reciente teoría legal suele encuadrar estos hechos como simples delitos patrimoniales, lo que dificulta sancionar a los responsables, con este objetivo se aplica una metodología cualitativa basada en la revisión crítica de sentencias nacionales e internacionales, doctrina especializada y entrevistas a operadores de justicia, para identificar los vacíos interpretativos que han favorecido la impunidad durante el último lustro, los hallazgos evidencian la falta de lineamientos uniformes para valorar evidencia digital y la escasa coordinación entre la persecución penal y la necesaria protección de datos personales comprometidos en las estafas.

En conclusión, urge consolidar criterios probatorios, fortalecer la formación técnica de fiscales y jueces, para aplicar con rigor los tipos penales informáticos, de modo que el sistema jurídico ecuatoriano pueda prevenir eficazmente los engaños digitales y salvaguardar los derechos de la ciudadanía en el entorno digital.

Palabras Claves: Inteligencia artificial, Medios electrónicos, Derecho Penal, Proteccion de datos.

ABSTRACT

Cybercrime, particularly digital fraud committed through electronic means such as social media and messaging services, has steadily increased in Ecuador over the past five years, this growth is related to low digital literacy, job insecurity, and the economic fallout from COVID-19, which has pushed many people to seek income online, leaving them vulnerable to scams powered by artificial intelligence capabilities capable of impersonating and luring victims.

This research aims to explain why the response of Ecuadorian criminal law is insufficient. Despite the existence of legislation that criminalizes conduct such as electronic fraud, recent legal theory tends to categorize these acts as simple property crimes, making it difficult to punish those responsible, to this end, a qualitative methodology based on a critical review of national and international rulings, specialized doctrine, and interviews with justice officials is applied to identify the interpretative gaps that have fostered impunity over the last five years, the findings reveal a lack of uniform guidelines for assessing digital evidence and poor coordination between criminal prosecution and the necessary protection of personal data compromised in fraud.

In conclusion, it is urgent to consolidate evidentiary criteria and strengthen the technical training of prosecutors and judges to rigorously apply computer related criminal offenses so that the Ecuadorian legal system can effectively prevent digital fraud and safeguard citizens rights in the digital environment.

Keywords: Artificial intelligence, Electronic media, Criminal law, Data protection.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la actualidad, los delitos informáticos, en particular los engaños digitales cometidos en redes sociales y plataformas de mensajería, representan un grave problema en Ecuador, estas conductas delictivas afectan directamente a la integridad patrimonial, su privacidad y la confianza de los ciudadanos en los entornos digitales, la facilidad con la que se pueden difundir mensajes engañosos, suplantar identidades o estafar a usuarios desprevenidos ha convertido a las plataformas digitales en escenarios frecuentes de fraude, especialmente en un contexto de creciente conectividad, de acuerdo con cifras recientes, millones de ecuatorianos utilizan redes sociales sin contar con conocimientos básicos sobre ciberseguridad, lo cual los hace especialmente vulnerables ante estos delitos.

En este escenario, el estudio analiza cómo se ha aplicado la normativa penal ecuatoriana frente a tales engaños, a partir de la revisión de teoría legal nacional e internacional para detectar los vacíos jurídicos que han favorecido su impunidad durante los últimos cinco años.

Pese a la gravedad del problema, el sistema legal ecuatoriano enfrenta serias limitaciones para brindar una respuesta adecuada, una de las principales causas de esta ineficacia es la errónea calificación jurídica de los delitos informáticos, que en muchos casos son tratados bajo figuras penales tradicionales como simples delitos patrimoniales, sin considerar las particularidades técnicas y contextuales que caracterizan al entorno digital, esta mala aplicación de la ley no solo impide una correcta persecución penal, sino que además fomenta la impunidad, ya que los delitos no son sancionados con el rigor que corresponde ni se protege eficazmente a las víctimas.

Frente a este panorama, resulta urgente repensar la forma en que se aborda jurídicamente la criminalidad digital en el país, por ello, el estudio se apoya en una metodología cualitativa que combina la revisión crítica de teoría legal nacional e internacional, el análisis doctrinario y entrevistas semiestructuradas a fiscales, jueces y peritos en informática forense, es necesario actualizar el marco normativo, para así fortalecer el adiestramiento técnico y jurídico de los operadores de justicia en temas de derecho informático y promover un enfoque legal que permita aplicar

correctamente los tipos penales diseñados para este tipo de amenazas, solo así se podrá garantizar una protección real a las personas afectadas por engaños digitales, contribuir a la disminución de la impunidad, además de fortalecer la confianza de la ciudadanía en la justicia penal en tiempos de transformación tecnológica.

CAPÍTULO I

1.1 Tema

Engaños digitales en redes sociales y mensajería: necesidad urgente de aplicar bien la ley para evitar impunidad en delitos informáticos.

1.2 Planteamiento del Problema

En el Ecuador desde el año 2020 hasta el 2025, se ha vuelto cada vez más común el poder oír historias de personas los cuales fueron víctimas de estafas a través de mensajerías, las mismas redes sociales, o alguna aplicación de teléfono el cual se puede obtener el numero cualquier persona de manera fácil y rápida, los engaños digitales antes no eran tan sonados como lo son ahora, los afectado de estos delitos cibernéticos afectan a más de miles de ciudadanos de distintas edades y condiciones sociales que tienen posesión de algún aparato electrónico el cual posee internet.

De acuerdo con diario el comercio durante estos años se han reportado más de 3.183 casos relacionados con el fraude electrónico, lo que es suplantamiento de identidad, las estafas piramidales y el soborno ilegal de dinero mediante los medios digitales (El comercio, 2022).

La Fiscalía General del Estado esto nos hace caer en cuenta la falla que tiene nuestros Códigos cuando se trata de engaños digitales, debido a esto queda impunes mediante los ojos de la justicia, la mala forma de aplicación de los tipos penales debería mejorarse para dar una mejor ayuda a las personas naturales respecto a caer en estos engaños (Fiscalía general del estado, 2023).

Además alguna de las causas detrás de este fenómeno son debido a lo que paso en año 2019 y 2020 sobre la pandemia del Covid-19 quien fue la causante de que 31 millones de empleos perdidos debido a ese suceso tan trágico que le dio un giro a todo el mundo, el desempleo, la falta de ingresos y la necesidad de sobrevivir impulsaron a muchas personas a buscar oportunidades en línea, debido a eso han surgido innumerables casos de ciudadanos que con buena fe, han caído en trampas disfrazadas de ofertas laborales o negocios desde casa, difundidas por canales como

Facebook, WhatsApp o Telegram, sin contar con las herramientas ni el conocimiento necesario para detectar el engaño (Factor trabajo, 2022).

Estudios señalan que el 79,21 % de la población ecuatoriana accede a internet, pero la mayoría no ha recibido formación sobre cómo protegerse en el entorno digital, esto, sumado a la informalidad laboral que caracteriza al país, hace que muchos estén más expuestos a caer en estas estafas, los delincuentes aprovechan la confianza, la falta de educación digital y las necesidades económicas para cometer sus delitos, utilizando técnicas de manipulación emocional que resultan difíciles de detectar (El comercio, 2022).

El modus operandi de los ciberdelincuentes es cada vez más elaborado, utilizan perfiles falsos, clonan cuentas legítimas, se hacen pasar por entidades financieras, familiares o marcas reconocidas, y difunden enlaces maliciosos para acceder a información personal y financiera, posteriormente, proceden a vaciar cuentas bancarias o comercializar los datos en espacios digitales ilícitos, sin embargo muchos de estos actos son tipificados erróneamente bajo delitos comunes como estafa, sin reconocer su carácter informático (Ortega et al., 2025).

Esta inadecuada clasificación obstaculiza la eficacia del sistema judicial, generando altos niveles de impunidad, si bien el Código Orgánico Integral Penal (en adelante COIP), contempla en su artículo 232-B el acceso no consentido a sistemas informáticos y en el artículo 233-A la suplantación de identidad digital, su aplicación práctica ha sido limitada e inconsistente, como reconocen expertos y sentencias puntuales (COIP, 2021).

Los derechos vulnerados por estas conductas trascienden el patrimonio económico se comprometen la intimidad, identidad digital, seguridad jurídica, integridad psicosocial y la confianza institucional.

Derechos vulnerados por los engaños digitales, estas prácticas no solo constituyen delitos, sino que también vulneran derechos fundamentales como el derecho a la privacidad, la seguridad informática, la honra, la imagen y, en algunos casos, el patrimonio económico, las víctimas las cuales han sido afectadas suelen sufrir daños psicológicos, sociales y materiales, mientras que los agresores muchas

veces quedan en la impunidad por falta de identificación o fallas en la respuesta institucional.

Si lo vemos a un nivel jurídico se puede observar una afectación directa al principio de dignidad humana, pues estas acciones exponen a las personas a situaciones de vergüenza pública, acoso o pérdida de confianza social, además cuando los delitos digitales involucran menores de edad, se transgreden derechos prioritarios de protección integral, poniendo en riesgo su desarrollo físico y emocional, además que su afectación no se limita al daño inmediato, sino que puede tener consecuencias prolongadas en la vida personal y profesional de la víctima.

1.3 Formulación del Problema

¿Cómo influye la incorrecta aplicación de los tipos penales informáticos en la impunidad de los engaños digitales cometidos mediante redes sociales y plataformas de mensajería en Ecuador, durante el periodo 2020 y 2025?

1.4 Objetivo General

Analizar la aplicación deficiente de la normativa penal ecuatoriana frente a los engaños digitales cometidos en redes sociales y plataformas de mensajería mediante revisión de teoría legal nacional e internacional para la identificación de vacíos jurídicos que inciden en la impunidad de estos delitos en lo últimos cinco años.

1.5 Objetivos Específicos

- Identificar los enfoques doctrinarios y jurídicos que fundamentan los delitos informáticos y engaños digitales en el ordenamiento ecuatoriano, así como su tratamiento en el derecho penal comparado, particularmente en el sistema español.
- Diagnosticar las principales formas de engaño digital cometidas entre 2020 y 2025 a través de redes sociales y plataformas de mensajería en Ecuador, evaluando cómo su actual tratamiento penal contribuye a la impunidad.
- Distinguir la correcta aplicación de los tipos penales informáticos vigentes en Ecuador y su eficacia frente a la creciente sofisticación del modus operandi de los ciberdelincuentes en relación al impacto de los derechos fundamentales de las víctimas.

1.6 Idea a Defender

La incorrecta calificación y aplicación de los delitos informáticos como simples delitos patrimoniales en el Ecuador contribuye significativamente a la impunidad de los responsables de engaños digitales en redes sociales, plataformas de mensajería, lo que evidencia la urgente necesidad de reformar el marco jurídico penal para fortalecer la capacitación de los Fiscales y Jueces para garantizar una protección efectiva de los derechos de las víctimas en el entorno digital.

1.7 Línea de Investigación Institucional / Facultad.

Línea de Investigación Institucional

Sociedad civil, derechos humanos y gestión de la comunicación.

Línea de Investigación Facultad

Derecho con aplicabilidad en el campo digital, los derechos humanos y la solución de conflictos.

CAPÍTULO II

MARCO REFERENCIAL

2.1 Marco Teórico

2.2 Antecedentes

Según la síntesis histórica presentada por Morocho Rodríguez (2022), el interés académico por las redes sociales y la tecnología se remonta a más de un siglo atrás.

A comienzos de 1908, el filósofo y sociólogo Georg Simmel ya examinaba los incipientes avances técnicos y proponía el término red social para describir un entramado de vínculos formales e informales entre personas que comparten valores, creencias y tradiciones comunes.

Años después, en 1930, el sociometrista Jacob Levy Moreno profundizó esta línea de investigación con un registro sistemático de interacciones en pequeñas comunidades estudiantiles de Harvard, sin embargo, el proyecto quedó en pausa durante más de quince años por limitaciones metodológicas.

El panorama cambió radicalmente en la década de 1960 con el surgimiento de Advanced Research Projects Agency Network (ARPANET), precursor de Internet, debido a la infraestructura compleja y su alto costo, el acceso se restringió inicialmente a instituciones y élites, pero con el avance posterior la tecnología abrió posibilidades de comunicación y consulta de información en todo el mundo sin contacto físico directo, a lo largo de la historia, señala la autora, esta evolución demuestra la creatividad humana para desarrollar herramientas que aseguren la supervivencia y satisfagan nuevas necesidades (Rodríguez, 2022).

El vertiginoso progreso tecnológico, la expansión de las telecomunicaciones y de Internet, así como la modernización de los sistemas de transporte, han convertido la globalización en un hecho incuestionable en el mundo contemporáneo, en este escenario surgen auténticas redes de conocimiento que facilitan la interacción humana dentro de un entorno social y resultan decisivas para el desarrollo de las civilizaciones actuales y venideras (Rodríguez, 2022).

Las redes sociales, en esencia, se orientan a generar, almacenar y difundir saberes a escala mundial mediante los distintos recursos disponibles dentro de cada plataforma o sitio web, estas dinámicas de difusión enriquecen tanto el plano intelectual como el social de las personas, fomentando la creatividad y el intercambio con quienes nos rodean (Rodríguez, 2022).

A partir de 2014 el ecosistema de redes sociales se ha ampliado de forma sostenida con el nacimiento de servicios como WhatsApp, Tumblr e Instagram, este crecimiento ha obligado a dichas plataformas a redefinir su misión, han pasado de ser simples espacios de socialización a convertirse en canales de monetización, impulso de emprendimientos y difusión de productos o negocios a través de publicidad pagada, lo cual les permite mantener su carácter gratuito y de acceso abierto para todos los usuarios (Rodríguez, 2022).

2.2.1 Origen Y Evolución De La Estafa En El Ecuador y su incremento en el COVID-19

Durante años, juristas y legisladores han advertido la necesidad de reforzar el tratamiento de los fraudes y engaños dentro del derecho penal ecuatoriano, aunque el ordenamiento ya incorpora políticas criminales que describen distintos elementos típicos, históricamente ha resultado complejo distinguir la estafa de figuras afines como el peculado o el enriquecimiento ilícito, pues todas comparten la lógica del engaño como medio de obtención indebida de bienes (Rodríguez, 2022).

Entre marzo de 2020 y el cierre de 2021 la pandemia de COVID-19 generó un salto inédito en la superficie de riesgo digital del Ecuador, el confinamiento obligó a millones de personas a teletrabajar y estudiar en línea, de modo que la penetración de Internet doméstico saltó del 45,5 % en 2019 al 53,2 % en 2020, lo que añadió de golpe a la red a decenas de miles de usuarios con escasa alfabetización digital (Tecnologías de la información & la comunicación, 2021).

Las bandas de ciberdelincuentes aprovecharon ese nicho, un informe de Interpol de abril 2020 registró un pico de dominios maliciosos que incluían los términos covid o corona, campañas masivas de phishing que ofrecían mapas de contagio, bonos de emergencia o vacunas, y un marcado repunte de fraudes Business Email Compromise apoyados en la urgencia y el miedo (Interpol.int, 2020).

Al mismo tiempo, la implantación apresurada de Virtual Private Network (VPN), el cual es un servicio de red virtual privada que crea un tunel cifrado entrelos dispositivos los cuales utilizamos seguido como los telefonod, tablets y computadoras, ademas estas plataformas de videoconferencia dejó expuestos puertos sin parches y credenciales recicladas, circunstancia que cuadruplicó los ataques de ransomware dirigidos contra empresas, hospitales y entidades públicas (Rendón et al., s.f.).

Las cifras oficiales confirman el impacto solo entre enero y agosto de 2020 la Fiscalía recibió 5.048 denuncias por ciberdelitos el 43 % por suplantación de identidad, el 29 % por falsificación de documentos digitales y el 20 % por apropiación fraudulenta en la cual hace mencion el art. 190 COIP y la banca notificó un aumento del 24 % en intentos de phishing sobre sus clientes móviles en el segundo trimestre de ese año.

La jurisprudencia también recogió la ola en la Sentencia 200-20-EP/22 la Corte Constitucional advirtió que la emergencia sanitaria había evidenciado la debilidad de los sistemas de banca en línea y ordenó a los jueces exigir peritajes técnicos más rigurosos cuando la estafa se produzca en contexto de pandemia (Corte Constitucional del Ecuador, 2022).

Tras el ransomware que paralizó al Banco Pichincha en octubre 2021, la Superintendencia de Bancos activó por primera vez su protocolo de notificación de incidentes graves en menos de 24 horas, calificando el hecho como ciberataque ligado a la crisis sanitaria (Harán, 2021).

En suma, la nueva normalidad catapultó la apropiación fraudulenta por medios electrónicos al primer lugar de las denuncias patrimoniales y empujó al sistema judicial a profesionalizar la cadena de custodia digital y la valoración pericial de la evidencia.

2.2.2 Avances Internacionales Y Primeros Intentos De Tipificación

En el año 1983 diversos foros internacionales abrieron el debate sobre cómo tipificar la delincuencia informática, insistiendo en la falta de sanciones claras para las defraudaciones tecnológicas (Rodríguez, 2022).

En el año 1986 la Comisión de Información, computadoras y comunicaciones publicó informes que enumeraban una lista mínima de conductas a regular con mayor precisión: fraude, uso ilegítimo de software, falsificación de datos, transferencia no autorizada de información y estafas electrónicas, entre otras (Rodríguez, 2022).

Paralelamente, la Declaración Universal de Derechos Humanos consagra en su artículo 17 la protección de la propiedad, este reconocimiento cimenta la obligación de los estados parte de tutelar el patrimonio de las personas frente a nuevas modalidades de fraude (Rodríguez, 2022).

2.2.3 De la estafa clásica a la ciberdelincuencia

Estudios recopilados muestran que los delitos facilitados por la informática sabotajes, robos de datos, fraudes en línea se multiplicaron porque las normas vigentes apenas los describían, así aunque el engaño patrimonial existe desde tiempos remotos, su denominación y alcance han cambiado conforme evoluciona la tecnología y la visión de los legisladores.

Hoy se concibe la estafa como la obtención de un beneficio económico mediante ardid o engaño que induce a la víctima a error, sin recurrir a la violencia física. La legislación ecuatoriana la recoge expresamente en los artículos 190, 231, 232 y 234 del Código Orgánico Integral Penal (COIP), incluyendo variantes cometidas por medios electrónicos (Rodríguez, 2022).

2.2.4 La tipificación como desafío permanente

Una conducta sólo ingresa al ámbito penal cuando la comunidad internacional la reconoce como acto humano antijurídico que pone en peligro o lesiona un bien jurídico protegido, siguiendo esta lógica, la estafa ha crecido y diversificado sus métodos más rápido de lo que las leyes se actualizan, dejando vacíos que inquietan a la ciudadanía.

Aunque casi todos los sistemas penales castigan la estafa, cada uno la define de modo distinto unos acentúan la dimensión cognitiva del engaño, otros el dolo con la irrupción de las redes sociales, surgen técnicas novedosas para defraudar, el phishing, fraudes por mensajería instantánea o suplantación de identidad mediante

deepfakes, muchos de estos métodos no figuran de forma detallada en los textos legales, lo que dificulta imponer sanciones proporcionales (Rodríguez, 2022).

2.2.5 Digitalización de la sociedad

La acelerada digitalización de la sociedad hace imprescindible garantizar que las tecnologías en uso posean, con un nivel de confianza definido, la capacidad de resistir y recuperarse frente a accidentes, ciberataques o acciones malintencionadas que pongan en riesgo la disponibilidad, autenticidad, integridad, confidencialidad de los datos, los servicios que las redes y sistemas ofrecen a esta capacidad de resistencia y recuperación la doctrina la denomina resiliencia (Galán & Cordero, 2016).

Lograrla exige más que soluciones estrictamente técnicas se necesitan marcos de ciberseguridad basados en estándares internacionales ISO/IEC 27001, NIST, Esquema Nacional de Seguridad, NIS2, entre otros, programas de gestión de riesgos, auditorías periódicas y planes de continuidad operativa, además la formación continua del factor humano usuarios, desarrolladores y administradores resulta esencial, pues la mayoría de brechas explota errores humanos más que fallos de software, solo a través de esta visión integral tecnológica, organizativa y normativa se refuerza la confianza pública en los ecosistemas digitales, los cuales se garantiza la sostenibilidad de los servicios en un entorno cada vez más interconectado (Galán & Cordero, 2016).

2.2.6 Delitos informáticos más frecuentes en el Ecuador (2024-2025)

Dentro de la tabla resume las cinco figuras penales que concentran casi la totalidad de las denuncias por delitos informáticos registradas en el Ecuador durante 2024-2025, según el consolidado de la Fiscalía General y la Dirección de Ciberdelitos, se muestra el tipo penal correspondiente en el COIP, su manifestación práctica más habitual y el número de casos ingresados en 2024, junto con el peso porcentual aproximado dentro del total de 3.913 denuncias de ese año.

Ademas se destaca la aplastante prevalencia de la apropiación fraudulenta por medios electrónicos art. 190, que por sí sola representa 94 % de los reportes, seguida a gran distancia por la interceptación ilegal de datos y la revelación ilícita de bases de

datos, estos datos contextualizan la urgencia de perfeccionar la aplicación de los artículos 190 y 233-B, de reforzar la prevención frente a las modalidades dominantes de phishing y suplantación de identidad (COIP, 2021).

Estas cifras evidencian la urgencia de robustecer las unidades de investigación digital y capacitar a fiscales y peritos en análisis forense solo así se reducirá la impunidad asociada al phishing y la suplantación de identidad.

Tabla 1.

Delitos informáticos más frecuentes en el Ecuador (2024-2025).

#	Tipo penal (COIP)	Descripción práctica	Denuncias 2024	Participación aproximada
1	**Apropiación fraudulenta por medios electrónicos** (art. 190)	Phishing, vishing o smishing que permiten a los atacantes vaciar cuentas, clonar tarjetas o desviar transferencias.	**3 696** de 3 913 casos	**94 %**
2	Interceptación ilegal de datos (art. 232-B)	Captura de claves, sniffing en Wi-Fi públicas, malware que espía tráfico.	120	3 %
3	Revelación ilegal de base de datos (art. 233-A)	Venta o filtración de listas de clientes, historiales médicos o registros académicos.	60	1,5 %
4	Transferencia electrónica de activo patrimonial (art. 233-B)	Traspaso no autorizado de valores entre cuentas propias o de terceros usando credenciales robadas.	40	1 %

#	Tipo penal (COIP)	Descripción práctica	Denuncias 2024	Participación aproximada
5	Suplantación de identidad y estafas en redes sociales	Cuentas clonadas, ofertas laborales falsas, premios o ventas fantasmas en Marketplace.	Incluidas en art. 190	s/d

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

2.3 Conceptualización Y Terminología

2.3.1 Ciberdelito (Delito que se comete a través de internet)

Es toda conducta ilícita que se ejecuta mediante dispositivos conectados o redes digitales, atentando contra sistemas, datos o servicios en línea (Universidad del internet, 2024).

Dentro de este paraguas, el ciberfraude engloba cualquier estafa económica perpetrada íntegramente por Internet, una app móvil o una plataforma digital, con el propósito de obtener un beneficio patrimonial mediante engaño (Alicio, 2021).

2.3.2 Las modalidades de ingeniería social más comunes

- **Phishing (suplantación de identidad)**

  Se refiere a una técnica de engaño digital en la que un atacante se hace pasar por una entidad confiable para obtener información confidencial del usuario, como contraseñas, números de tarjetas de crédito o datos personales, estos envíos masivos de correos, mensajes o enlaces que suplantan a entidades legítimas para captar credenciales o datos sensibl,es (Proofpoint, 2025).

- **Smishing (suplantación de identidad por SMS)**

  Es una forma de fraude digital en la que los delincuentes envían mensajes de texto falsos para engañar al destinatario, este es una variación del phishing el cual llega por SMS o mensajería móvil, combinando SMS + phishing (Proofpoint, 2025).

- **Vishing (suplantación de identidad por llamada telefónica)**

  Proviene de la unión de voice - (voz) y phishing, que consiste en que los delincuentes llaman por teléfono haciéndose pasar por representantes de instituciones legítimas, estas estafas por voz en la que el atacante, vía llamada telefónica, finge ser una institución fiable para obtener información confidencial (Incibe, 2020).

- **Pig-butchering (fraude del engorde)**

  Es una técnica en la que los estafadores engordan emocionalmente a la víctima ganándose su confianza durante semanas o meses, generalmente a través de redes sociales, apps de citas o mensajería, para luego inducirla a invertir en criptomonedas falsas, plataformas de trading fraudulentas o negocios inexistentes.

  Para evaluar el impacto de estas conductas, la seguridad de la información se mide en torno a los ejes de Disponibilidad, Autenticidad, Integridad y Confidencialidad (DAIC), parámetros consagrados en el Esquema Nacional de Seguridad español (Real Decreto 311/2022) y adoptados como referencia por múltiples marcos latinoamericanos (Boe, s.f.).

- **Resiliencia digital o ciber resiliencia (ataques o incidentes cibernéticos)**

  La habilidad que tiene una persona, organización o sistema digital para mantener su funcionamiento y proteger sus activos digitales, incluso después de sufrir una interrupción provocada por una amenaza informática**,** el cual designa la capacidad de un organismo o sistema para prevenir, resistir y recuperarse de incidentes cibernéticos sin perder operatividad ni confianza (Ibm, 2022).

2.4 Tipologías de engaños digitales en redes y mensajería

2.4.1 Suplantación de identidad y clonación de perfiles

Los ciberdelincuentes crean cuentas falsas o secuestran perfiles reales para hacerse pasar por la víctima, captar a sus contactos y solicitar dinero o información personal, durante junio de 2025, medios latinoamericanos alertaron de un aumento de casos vinculados a estafas románticas y ventas ficticias en Facebook e Instagram, detallando las señales de alerta y los pasos para denunciar, el regulador ecuatoriano

arcotel recomienda activar la verificación en dos pasos y restringir la visibilidad de datos personales (Arcotel, 2025).

2.4.2 Ofertas laborales y falsos premios

Se difunden avisos de empleo inexistentes o sorteos atractivos vía WhatsApp, Telegram o Messenger que redirigen a formularios donde la víctima entrega fotografías de cédula, CV, datos bancarios o paga supuestos gastos de inscripción, en febrero de 2025 el Consejo Nacional Electoral desmintió un mensaje viral que ofrecía 157 plazas para las elecciones, las Naciones Unidas también alertó sobre correos que usurpaban su identidad con promesas de contrato internacional o becas (Pablos, 2025).

2.4.3 Fraudes romántico-cripto- pig-butchering

El estafador cultiva durante semanas una relación afectiva en redes o apps de citas, convence a la víctima de invertir en una plataforma cripto falsa y, cuando el cerdo está gordo, desaparece con todo el capital, un boletín del Servicio Secreto de EE. UU (United states secret service , 2025).

Esto describe la técnica y advierte que los estafadores usan identidades fabricadas y testimonios inventados, análisis forense subraya que la mayoría de víctimas pierde de USD 5.000 a 1.000,000 (Corporación forense digital , 2025).

2.4.4 Estafas con deepfakes y sextorsión

La IA generativa permite superponer rostros o voces sobre vídeos creíbles los cuales se fabrican comprometedores montajes sexuales para extorsionar pagas o lo público o se hacen pasar por un directivo en videollamadas para ordenar transferencias, centros de ciberseguridad advierten, además el impacto en adolescentes que comparten fotografías íntimas (TrendTic, 2023).

2.4.5 Business Email Compromise (BEC) o fraude del CEO

Mediante spear-phishing o suplantación de dominio, el atacante envía un correo que parece provenir del director financiero o gerente general y ordena un pago urgente a un proveedor fraudulento (Lisa Institute, 2024).

Según Proofpoint & KnowBe4, el BEC ha generado más de USD 55.000 millones en pérdidas globales y afecta por igual a pymes exportadoras y grandes corporaciones la FBI IC3 lo considera el esquema más costoso de la última década (Proofpoint, 2024).

2.4.6 Estafas en plataformas Marketplace (Facebook, OLX, etc.)

Los delincuentes publican artículos o servicios inexistentes o clonan anuncios legítimos y, una vez recibido el anticipo vía transferencia, billetera digital, jamás entregan el bien, entre las tácticas más habituales están: (i) productos defectuosos o falsificados, (ii) pedidos de señal para reservar el artículo, (iii) sobrepagos ficticios que exigen reembolsar la diferencia y (iv) robo de números Google Voice o cuentas para nuevas estafas, un reportaje de primicias detalla ocho modalidades recurrentes y advierte que uno de cada seis usuarios latinoamericanos ha sido víctima en Facebook Marketplace (Lisa Institute, 2024).

En el ámbito local, el Registro Civil detectó 87 perfiles falsos que ofrecían, vía Marketplace, turnos inmediatos para cédulas y pasaportes a precios inflados, cobrando tarifas ilegales por un trámite que en realidad es gratuito, la entidad remitió las pruebas a la Fiscalía y a la Policía Nacional (Primicias diario Ecuador , 2024).

2.4.7 Señales de alerta

Ofertas demasiado baratas, vendedores que presionan por adelantos, capturas de pantalla bancarias difíciles de verificar y cambios súbitos de plataforma de Marketplace a WhatsApp, para activar pagos protegidos, reunirse en lugares públicos y nunca enviar documentos personales reduce significativamente el riesgo.

2.5 Teorías Criminológicas Aplicables A Los Engaños Digitales

2.5.1 Teoría de las actividades rutinarias (TAR)

Cohen y Felson explicaron que un delito ocurre cuando confluyen un ofensor motivado, un objetivo adecuado y la ausencia de un guardián eficaz. Aplicada al entorno online, la TAR señala que las rutinas digitales por ejemplo, revisar el correo en wifi pública o desplazarse sin VPN entre redes sociales y banca, el cual exponen con mayor frecuencia a los usuarios a atacantes y reducen la vigilancia tecnológica que podría detenerlos, como el doble factor o los filtros antiphishing.

Estos estudios recientes demuestran que patrones diarios como las compras en línea o la sobreexposición en redes aumentan la probabilidad de victimización por fraudes y robo de identidad, confirmando la validez de la teoría en el ciberespacio (Raj & Caeiro, 2024).

2.5.2 Modelo riesgo-recompensa (Racionalidad / Rational Choice)

Bajo esta perspectiva, el delincuente compara las posibles ganancias criptomonedas, números de tarjeta, datos revendedores con los costos percibidos probabilidad de captura, sanciones legales, complejidad técnica, un experimento de 2025 en un foro de hackers mostró que anuncios de credenciales con alto beneficio y baja amenaza legal recibían más clics y respuestas, lo que confirma que incluso en entornos ilícitos los actores evalúan métricas de riesgo y premio antes de atacar, estas guías de ciberseguridad concluyen que aumentar el costo más autenticación, trazabilidad o disminuir la ganancia límites de retiro, tokens temporales para desalienta el intento (Mark, 2024).

2.5.3 Técnicas de neutralización y oportunidades en línea

La teoría de Sykes & Matza describe cómo los ofensores reducen la culpa mediante estrategias como negar daño, las empresas pueden permitírselo, culpar a la víctima, el apelar a lealtades superiores y lo hago para exponer fallos de seguridad, esta investigaciones de 2025 sobre grupos de ransomware muestran que los atacantes justifican sus intrusiones calificándolas de servicio de auditoría o justa retribución contra corporaciones abusivas, usando el anonimato y la distancia social del medio digital para reforzar esas excusas y aprovechar oportunidades técnicas bugs sin parche, accesos RDP expuestos (Connolly et al., 2025).

2.5.4 Economía del delito y racionalidad limitada

Inspirada en Becker, la economía del cibercrimen analiza mercados clandestinos, precios de datos robados y barreras de entrada, pero reconoce que los actores operan con información incompleta, sesgos cognitivos y limitaciones tecnológicas lo que Herbert Simon llamaba racionalidad acotada, una revisión sistemática de 2021 sobre economía y ciberseguridad resalta que muchos atacantes aceptan pagos menores que el valor real del botín porque sobrestiman la urgencia de revender o subestiman el rastreo en blockchain (Kianpour et al., 2021).

Al mismo tiempo, las víctimas invierten menos en prevención porque infraevalúan la probabilidad de ser blanco, estas asimetrías informativas explican por qué los mercados de exploits y credenciales siguen floreciendo pese a leyes más severas (Kianpour et al., 2021).

2.5.5 Space Transition Theory -(Teoría de la Transición del Espacio) -(STT)

Esta teoría parte de la idea de que las personas pueden exhibir comportamientos distintos conformes o desviados cuando pasan del espacio físico al ciberespacio, el entorno digital aporta anonimato, ausencia de jerarquías visibles y sensación de menor control social, factores que permiten a individuos que normalmente respetarían la ley actuar de modo ilícito en línea, en los fraudes por redes sociales esto se refleja, por ejemplo, en profesionales sin historial delictivo que crean perfiles falsos para vender productos inexistentes o en parejas que, tras romper, difunden imágenes íntimas sextorsión porque perciben menos riesgo y reproche, la ayuda a explicar por qué la tasa de participación en delitos de engaño digital es mucho más amplia que en fraudes cara a cara y por qué el ciberdelito florece en contextos donde la identidad y la ubicación real son fáciles de ocultar (Karuppannan, 2008).

2.6 Marco Legal

La lucha contra los engaños digitales descansa en un entramado jurídico, en capas que va de lo global a lo local desde tratados internacionales hasta normas técnicas y lineamientos internos de cada organismo público o privado, a continuación se desarrolla, con mayor nivel de detalle, cada uno de estos bloques normativos y sus interrelaciones.

2.6.1 La Constitucion de la republica del Ecuador 2008

Los artículos 66 y 92 de la Constitución del Ecuador de 2008 reconoce en sus articulos 66 y 92 de los derechos a la proteccion de datos, es el garantizan el derecho de las personas a controlar y proteger su información personal, exigiendo que cualquier recolección, almacenamiento, procesamiento o difusión de datos cuente con el consentimiento expreso del titular o esté respaldado por una norma legal, además se otorgan a toda persona el derecho a acceder, corregir, actualizar e eliminar sus datos personales en poder de entidades públicas o privadas, ya sea en

formato físico o digital, imponiendo la implementación de medidas de seguridad específicas para evitar su uso indebido (Constitución de la república del Ecuador, 2008).

Este marco constitucional respalda la necesidad urgente de aplicar correctamente la ley frente a los engaños digitales en redes sociales y mensajería, ya que muchos de estos delitos implican el acceso no autorizado o la manipulación de datos personales, fortalecer la aplicación de estos derechos es clave para prevenir la impunidad en los delitos informáticos y proteger de forma efectiva a los ciudadanos frente a estas nuevas formas de vulneración digital (Constitución de la república del Ecuador, 2008).

2.6.2 Instrumentos internacionales

Convenio de Budapest sobre Ciberdelincuencia (2001)

Ecuador depositó el instrumento de adhesión el 12 de diciembre de 2024, convirtiéndose en el 77º el Estado a parte, el tratado obliga a tipificar fraudes informáticos, falsificación de datos y acceso ilícito, e impone la creación de un punto de contacto 24/7 para tramitar evidencia electrónica transfronteriza (Consejo de Europa, 2024).

Segundo Protocolo sobre Pruebas Electrónicas (2021)

Aunque Ecuador aún no lo ratifica, el protocolo abierto a firmas en mayo de 2022 agiliza la obtención directa de datos de proveedores extranjeros, una pieza clave para perseguir estafas que se originan en redes y apps globales (Consejo de Europa, 2024).

Normativa de la Unión Europea como soft law regional

NIS 2 (Dir. UE 2022/2555), la marca la pauta sobre gestión de riesgos y notificación de incidentes para operadores esenciales y plataformas, varios países andinos, incluido Ecuador, lo citan como estándar de referencia para sus propuestas de ley (European Union, 2022).

GDPR (Reg. UE 2016/679), su principio de privacidad desde el diseño inspiró la Ley ecuatoriana de datos y las sanciones graduadas según facturación anual (European Union, 2022).

Organización de Estados Americanos (OEA)

La Red Interamericana de Ciberseguridad (CICTE/OEA) y su Guía CSIRT 2023 recomiendan armonizar definiciones penales y crear equipos de respuesta nacionales, en Ecuador empleó dichas directrices para estructurar el CSIRT-EC en 2022 (Practical guide for CSIRTs, 2023).

2.6.3 Código Orgánico Integral Penal

SECCIÓN NOVENA.- Delitos contra el derecho a la propiedad, el artículo 185 del Código Orgánico Integral Penal es una parte pertinente en la cual menciona los articulos que sancionan la extorsión cuando una persona, con la intención de obtener un beneficio propio o para un tercero, obliga o exige a otra mediante violencia, intimidación o cualquier medio incluyendo herramientas digitales, electrónicas o la difusión de panfletos a realizar o abstenerse de realizar una acción, efectuar un pago, entregar bienes o celebrar un acto jurídico que cause daño patrimonial, la pena aplicable es de tres a cinco años de prisión y una multa de veinte a veinticuatro salarios básicos unificados (COIP, 2021).

Esta norma penal es clave para enfrentar los engaños digitales en redes sociales y mensajería, donde el uso de amenazas electrónicas, suplantaciones o chantajes virtuales se ha vuelto frecuente, aplicar adecuadamente el artículo 185 permite prevenir y sancionar de forma efectiva este tipo de delitos informáticos, evitando su impunidad (COIP, 2021).

2.6.3.1 Análisis Art de la Pena. El artículo 186 del Código Orgánico Integral Penal sanciona la estafa, entendida como la acción de inducir a otra persona a error mediante la simulación, falsedad o distorsión de hechos, con el fin de obtener un beneficio económico y causar un perjuicio patrimonial, la norma establece penas agravadas cuando se emplean medios electrónicos o digitales, como el uso fraudulento de tarjetas, dispositivos de captura de datos, plataformas virtuales para simular operaciones financieras, compras, o inversiones, también agrava la pena si

el daño afecta a múltiples personas que supera un umbral económico relevante (COIP, 2014).

Este artículo es especialmente relevante en el contexto de los engaños digitales en redes sociales y mensajería, donde los delincuentes utilizan medios tecnológicos para estafar a usuarios mediante perfiles falsos, enlaces maliciosos, promesas de inversión o sorteos ficticios, aplicar de forma estricta esta disposición penal es crucial para reducir la impunidad en delitos informáticos que generan pérdidas económicas y afectan la confianza en los entornos digitales (COIP, 2014).

2.6.3.2 Cuadro explicativo de artículos del COIP relacionados con los delitos informáticos. La relación directa entre determinados artículos del Código Orgánico Integral Penal (COIP) y su aplicabilidad frente a los engaños digitales perpetrados a través de redes sociales y mensajería, esta correlación evidencia la urgencia de aplicar adecuadamente estas disposiciones legales para prevenir la impunidad.

Tabla 2

Cuadro explicativo de artículos del COIP relacionados con los delitos informáticos

Artículo COIP	**Descripción del delito**	**Relación con engaños digitales**
Art. 187	Abuso de confianza: disposición indebida de bienes entregados bajo condición, o uso de firma en blanco con perjuicio patrimonial.	Es común en fraudes donde se gana la confianza de la víctima por redes o mensajería, y luego se abusa de bienes o firmas.
Art. 190	Apropiación fraudulenta mediante medios electrónicos: uso no autorizado de sistemas o redes para obtener bienes o derechos.	Base de múltiples estafas digitales como phishing, hackeos o transferencias electrónicas no autorizadas.

Art. 191	Reprogramación o modificación no autorizada de la información de terminales móviles.	Permite alterar la trazabilidad de dispositivos usados en fraudes digitales, dificultando la investigación.
Art. 192	Intercambio, comercialización o compra de información de identificación de equipos móviles.	Facilita el uso de dispositivos móviles para suplantación, fraude y evasión de rastreo en redes sociales y mensajería.
Art. 193	Reemplazo de etiquetas de identificación en terminales móviles con información falsa.	Permite el encubrimiento de identidad digital a través de terminales móviles falsificados.
Art. 194	Comercialización ilícita de terminales móviles en violación a la normativa de telecomunicaciones.	Favorece el comercio ilegal de dispositivos usados para actividades fraudulentas en plataformas digitales.
Art. 195	Posesión de infraestructura o programas para reprogramar o alterar datos de identificación de equipos móviles.	Contribuye a la clonación de equipos usados para cometer delitos informáticos o dificultar su rastreo.

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

SECCIÓN TERCERA.- Delitos contra la seguridad de los activos de los sistemas de información y comunicación, incorporando delitos del COIP vinculados a la manipulación y comercialización ilícita de terminales móviles, así como a la revelación indebida de bases de datos, estas conductas tienen una conexión directa con los fraudes cometidos mediante redes sociales y mensajería, al facilitar la suplantación de identidad, el uso de dispositivos alterados junto a la filtración de datos personales.

Tabla 3

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo COIP	**Sujeto activo**	**Verbo rector**	**Circunstancias**	**Relación con el tema**
Art. 187 – Abuso de confianza	Persona a quien se confía bienes o documentos con firma en blanco	Dispone / Abusa	Cuando causa perjuicio patrimonial por el abuso de confianza o de la firma	Este delito es relevante en el contexto de redes sociales y mensajería, donde los victimarios abusan de la confianza ganada virtualmente para obtener datos, contraseñas o transferencias, constituyendo una forma moderna de abuso de confianza.
Art. 190 – Apropiación fraudulenta por medios electrónicos	Persona que usa medios electrónicos para apropiarse de bienes ajenos	Se apropia / Manipula	Cuando altera o interfiere sistemas electrónicos para obtener beneficios ilegítimos	Está directamente vinculado con fraudes en redes sociales o mensajería, donde se accede a cuentas, billeteras virtuales o información financiera por medios tecnológicos para obtener beneficios ilícitos.
Art. 191 – Reprogramación o modificación de información de terminales móviles	Persona que manipula técnicamente equipos móviles	Reprograma / Modifica	Cuando se altera la información del dispositivo sin autorización	Este tipo de conducta facilita la comisión de engaños digitales, pues permite anonimizar terminales desde los cuales se ejecutan delitos como estafas o suplantación de identidad.

Art. 192 – Intercambio, comercialización o compra de información de equipos terminales móviles	Persona que comercia con datos técnicos de dispositivos	Intercambia /Comercializa / Compra	Cuando se trata de información de identificación de equipos móviles	Esta práctica facilita la suplantación de usuarios y dispositivos usados en fraudes digitales, por lo que su control es vital para detener redes de delitos informáticos.
Art. 193 – Reemplazo de identificación de terminales móviles	Persona que altera la identificación de terminales móviles	Sustituye / Coloca	Cuando el fin es ocultar la verdadera identidad del equipo	Estas acciones son comunes en delitos informáticos, ya que permiten operar dispositivos alterados para cometer estafas sin ser rastreados.
Art. 194 – Comercialización ilícita de terminales móviles	Persona que vende o distribuye equipos móviles fuera de norma	Comercializa	Cuando se incumplen regulaciones legales sobre dispositivos	Estos dispositivos pueden ser usados en redes sociales y mensajería para cometer delitos sin dejar rastros legales o técnicos válidos.
Art. 195 – Infraestructura ilícita	Persona que posee tecnología para modificar equipos	Posee / Conserva	Cuando el fin es alterar la identificación digital de terminales	Este delito alimenta estructuras de ciberdelincuencia que ejecutan fraudes o suplantaciones en plataformas digitales.
Art. 229 – Revelación ilegal de	Persona con acceso a	Revela	Cuando lo hace con fines propios o de terceros,	Este tipo penal protege datos personales que suelen ser vulnerados en estafas por mensajería o redes sociales,

base de datos	información sensible		utilizando medios electrónicos	donde se filtran o venden bases de datos.

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

2.6.4 Otras leyes que regulan aspectos informativos en nuestra legislación

Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), esta ley protege el uso legítimo de los datos personales, su aplicación es clave frente a la filtración de información usada en fraudes digitales mediante redes sociales y mensajería instantánea, facilita el ejercicio del derecho a la autodeterminación informativa (Constitución de la república del Ecuador, 2008).

Reglamento General a la LOPDP

Este reglamento establece medidas técnicas y de seguridad para el tratamiento responsable de datos personales, resulta esencial para prevenir el uso no autorizado de información en plataformas digitales, ademas que refuerza la protección ante engaños tecnológicos (Reglamento de la ley organica de proteccion de datos personales , 2023).

Ley Orgánica para la Transformación Digital y Audiovisual (2022)

Fomenta una transformación digital segura e inclusiva. Dispone medidas de ciberseguridad y gobierno digital para prevenir delitos tecnológicos, apoya entornos virtuales protegidos ante estafas informáticas (Constitución de la república del Ecuador, 2008).

Acuerdo MINTEL-2024-0003 – EGSI 3.0

Establece lineamientos de seguridad de la información para entidades públicas y privadas, previene accesos no autorizados a datos que pueden ser usados en fraudes virtuales, ademas que fortalece la gestión de riesgos digitales (Telecomunicaciones, 2024).

Proyecto de Ley Orgánica de Seguridad Digital (2024)

Este proyecto busca enfrentar de manera integral las amenazas digitales en el país, establece sanciones y medidas preventivas contra ciberdelitos como

suplantación o estafa en redes su aprobación es urgente (Asamblea Nacional del Ecuador, 2024).

Ley Orgánica de Inteligencia (2025)

Este proyecto propone un marco normativo para prevenir y sancionar amenazas cibernéticas, incluyendo fraudes y suplantaciones en redes sociales y mensajería, su aplicación permitiría reducir la impunidad en delitos informáticos (Lexis noticias , 2025).

2.6.5 Tabla comparativa: Delitos informáticos vs. delitos clásicos contra la propiedad (COIP)

Los delitos informáticos con delitos clásicos contra la propiedad establecidos en el COIP, identificando sus elementos técnicos digitales frente a sus equivalentes tradicionales, esta comparación permite evidenciar cómo el avance tecnológico ha transformado las formas de comisión delictiva, afectando bienes jurídicos similares mediante medios distintos.

Tabla 4

Tabla comparativa: Delitos informáticos vs. delitos clásicos contra la propiedad (COIP)

Grupo	Artículo COIP	Bien jurídico	Elemento técnico-digital	Elemento tradicional
Extorsión	185	Patrimonio + libertad	WhatsApp, email o panfletos digitales para intimidar	Violencia o amenaza directa
Estafa	186	Patrimonio	Tarjetas clonadas, cajeros alterados; fraude online	Engaño previo + disposición voluntaria
Abuso de confianza	187	Patrimonio	Distracción de datos/fondos con acceso lícito	Relación fiduciaria previa

Robo	189	Patrimonio + integridad física	Ransomware que cifra datos y exige pago	Violencia o intimidación
Hurto	196	Patrimonio	Descarga ilícita de activos digitales locales	Apoderamiento sin violencia
Apropiación fraudulenta electrónica	190	Patrimonio + confianza en sistemas	Manipulación de software/red para transferir fondos	Sin violencia ni engaño directo
Revelación ilegal de bases de datos	229	Privacidad + patrimonio	Venta/divulgación de datos extraídos	Ruptura del deber de custodia
Interceptación ilegal de datos	230	Secreto de las comunicaciones	Sniffing, pharming, clonado de tarjetas	Obtención de información sin permiso
Transferencia electrónica de activos	231	Patrimonio	Alterar código para desviar transferencias; mulas bancarias	Ánimo de lucro + manipulación informática
Ataque a la integridad de sistemas	232	Seguridad de la información	Malware, ransomware, DDoS	Daño o sabotaje al objeto digital
Acceso no consentido	234	Intimidad + patrimonio	Hacking, web-defacement, redireccionamiento	Intrusión clandestina

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

2.6.6 Fronteras conceptuales entre los delitos informáticos y las figuras tradicionales de defraudación

Diversa literatura doctrinal y fallos de cortes provinciales de nuestro país evidencian lo arduo que resulta, en la práctica, distinguir los nuevos delitos informáticos de figuras clásicas como el abuso de confianza, la estafa, el robo o el hurto (Cuchipe, 2022).

a) Apropiación fraudulenta por medios electrónicos vs. estafa arts. 190 y 186 COIP

Ambos tipos protegen el patrimonio y comparten la obtención de un beneficio económico sin embargo, difieren en el mecanismo de apoderamiento esta estafa que lo menciona el art. 186 el cual exige que la víctima, inducida en error, disponga voluntariamente de su bien, su propiación fraudulenta por medios electrónicos el art. 190 se consuma cuando el autor altera un sistema, ejemplo la banca en línea, que busca para transferir el activo sin autorización directa del titular (Cuchipe, 2022).

Tesis recientes subrayan que los fiscales suelen confundir ambos tipos porque el elemento engaño puede darse tanto en la ingeniería social previa estafa como en la manipulación técnica posterior y de apropiación Fraudulenta por medios electronicos (León, 2023).

Un estudio dogmático de la Universidad Central evidencia que en varios procesos se califica de estafa un fraude bancario cometido íntegramente por scripts automatizados, lo que provoca errores de competencia y de dosificación de la pena (Cuchipe, 2022).

b) Delito informático y abuso de confianza

El art. 187 COIP menciona que el abuso de confianza sanciona a quien, habiendo recibido un bien lícitamente, lo distrae en beneficio propia cuando un empleado autorizado accede a la base de datos de la empresa y transfiere los fondos a su cuenta, los jueces debaten si concurren los elementos del art. 187 abuso de confianza o los del art. 190 apropiación fraudulenta por medios electrónicos (COIP, 2014).

La Corte Nacional ha señalado que la relación de confianza no desaparece por el uso de medios digitales, de modo que puede existir concurso ideal entre ambos tipos penales (Corte Nacional de Justicia del Ecuador, 2018).

c) Hurto/robo y sustracción electrónica de activos

El hurto el art. 196 y el robo del art. 189 presuponen la sustracción física de un bien mueble, aun así, la doctrina admite que intangibles con valor económico como millas, créditos almacenados o criptomonedas son susceptibles de hurto si se extraen de un dispositivo físicamente controlado, por ejemplo, clonando la banda magnética de una tarjeta y vaciando el cajero (Corte Nacional de Justicia del Ecuador, 2018).

Esta interpretación se complica cuando la sustracción se ejecuta en la nube sin contacto físico, algunos tribunales aplican el art. 190 apropiación fraudulenta por medios electrónicos y otros mantienen la tesis del hurto, generando falta de uniformidad (Corte Nacional de Justicia del Ecuador, 2018).

d) Causas de la confusión tipológica

Bien jurídico idéntico propiedad, pero métodos híbridos engaño mas acceso técnico que encajan en varios preceptos.

Redacción solapada del COIP, los verbos rectores de los arts. 186 y 190 engañar, e utilizar fraudulentamente los cuales se traslapan cuando hay ingeniería social y hackeo en la misma secuencia delictiva.

Naturaleza intangible de los activos digitales, que no encaja con la tradicional noción de cosa mueble exigida por robo/hurto.

Evidencia electrónica fragmentada, la Fiscalía muchas veces solo aporta capturas de pantalla, lo que dificulta demostrar la voluntad dispositiva o la manipulación técnica.

2.6.7 Escenarios de solapamiento y confusión entre las personas afectadas

Ingeniería social mas hackeo- acceder sin autorización a sistemas informáticos, los cuales son un atacante convence a la víctima del engaño art. 186 Estafa de revelar un código OTP, luego usa un script para vaciar la cuenta

manipulación del art. 190 la cual meciona la apropiación fraudulenta por medios electrónicos y la fiscales suelen optar por uno solo de los artículos, originando errores de subsunción (Cuchipe, 2022).

- **Empleado infiel:** Coordinador de e - commerce que posee claves legítimas transfiere fondos a terceros, abuso de confianza el art. 187 porque había permiso de acceso, o transferencia electrónica el art. 231, transferencia electrónica de activo patrimonia por manipular el sistema, el CNJ ha dictaminado concurso ideal cuando concurren ambos supuestos (Crespo, 2021).
- **Ransomware con amenaza de doxing- programa malicioso que secuestra los archivos:** El doxing es la práctica de revelar o publicar información personal privada de una persona como dirección, teléfono, fotos, datos familiares en internet sin su consentimiento, usualmente para intimidar, extorsionar o causar daño, la cifra de estos ataques dedatos lo menciona el art. 232, el cual dice ataque a la integridad de sistemas informáticos y exige pago la extorsión art. 185, el delito informático se consuma antes de la coacción patrimonial, pero tribunales provinciales de Pichincha lo han considerado extorsión agravada (Mera, 2019).
- **Skimming en cajeros - copiar la información de las tarjetas bancarias:** El skimming es una técnica de fraude en la que los delincuentes instalan dispositivos ilegales en cajeros automáticos, el uso de dispositivos para clonar tarjetas se menciona tanto en el tipo de estafa el 186.1 y 186.2 como en interceptación de datos 230.4, doctrina penitenciaria crítica el bis in idem potencial si se aplican ambas figuras (Mera, 2019).

2.6.8 Cuadro comparativo de ciberdelitos: Ecuador, España, México y Brasil

Este cuadro explica, con lenguaje claro y sin abreviaturas, cómo cada país regula las conductas delictivas más frecuentes en el ciberespacio, incluye el artículo exacto, la denominación del delito, la pena prevista y una breve descripción de su alcance, en la última columna se indica si Ecuador ya está alineado o si existen vacíos que conviene cubrir con futuras reformas.

Tabla 5

Cuadro comparativo de ciberdelitos

Conducta típica	**Ecuador (COIP, reforma 2021)**	**España (Código Penal, reforma 2015)**	**México (Código Penal Federal)**	**Brasil (Código Penal y leyes especiales)**	**Observación / Brecha**
Acceso ilícito o 'hacking'	Artículo 234 – Acceso no consentido a un sistema informático o de telecomunicaciones. Pena: 3 a 5 años. Basta con ingresar o permanecer sin autorización.	Artículo 197 bis – Acceso ilícito a datos o sistemas sin permiso y divulgación de la información. Pena: 3 a 5 años y multa.	Artículos 211 bis 1 al 3 – Entrada no autorizada, modificación o destrucción de información protegida. Pena: 1 a 4 años.	Artículo 154-A (Lei 12.737/2012) – Invasión de dispositivo informático. Pena: 1 a 4 años y multa.	Cobertura común en los cuatro ordenamientos; las penas mínimas varían.
Sabotaje o daño a sistemas	Artículo 232 – Ataque a la integridad de sistemas informáticos. Pena: 3 a 5 años. Incluye malware, borrado o deterioro grave de datos.	Artículo 264 – Daños informáticos. Pena: 6 meses a 3 años; hasta 5 si hay agravante de gravedad.	Artículo 211 bis 4 – Destrucción o daño a sistemas, especialmente los estatales. Pena: 6 meses a 4 años.	Artículo 154-A §1º – Destruir, inutilizar o alterar datos después de la invasión. Pena: 1 a 4 años (Lei 14.155/2021 agrava si hay	Cobertura equivalente, pero España y Brasil añaden agravantes específicos.

				perjuicio económico).	
Interceptación o captura ilegal de datos	Artículo 230 – Interceptación ilegal de datos. Pena: 3 a 5 años. Incluye sniffing, pharming y clonado de tarjetas.	Artículo 197 bis (párrafo 2) – Interceptar transmisiones no públicas de datos. Pena: hasta 5 años.	Artículos 211 bis 5 al 7 – Copiar o interceptar datos sin autorización. Pena: 1 a 4 años; 2 a 6 si se afectan sistemas del Estado.	Marco Civil + Artículo 154-A – Copia no autorizada de datos. Sanción penal y multas administrativas bajo la LGPD.	Cobertura común; Brasil combina sanción penal y multa civil significativa.
Fraude o estafa informática (phishing, smishing)	Artículo 190 – Apropiación fraudulenta por medios electrónicos y Artículo 186 – Estafa con medios electrónicos. Penas: 1-3 y 5-7 años, respectivamente.	Artículo 248 – Estafa mediante manipulación informática. Pena: 6 meses a 3 años.	Artículo 386 (fraude) y 211 bis (modalidad digital). Pena: hasta 6 años si involucra al sistema financiero.	Artículo 171 (estelionato) con agravantes de la Lei 14.155/2021 – Fraude electrónico. Pena: 4 a 8 años.	Brasil prevé la pena más elevada; en Ecuador falta referencia explícita a criptoactivos.
Transferencia electrónica no consentida	Artículo 231 – Transferencia electrónica de activo patrimonial.	Se persigue como estafa informática en combinación con	Artículos 211 bis 4 y 5 – Maniobras en sistemas financieros	Lei 14.155/2021 – Agrava el fraude electrónico que afecta	Ecuador no contempla agravante específica para víctimas

(fraude 'del CEO' o BEC)	Pena: 3 a 5 años.	falsedad documental (artículo 390 bis).	para desviar fondos. Pena: hasta 6 años.	cuentas bancarias. Pena: 4 a 8 años.	vulnerables (adultos mayores, pymes).
Revelación o venta de bases de datos	Artículo 229 – Revelación ilegal de bases de datos. Pena: 1 a 3 años; 3 a 5 si interviene un servidor público.	Artículo 197 – Descubrimiento y revelación de secretos. Pena: prisión y multa.	Artículos 211 bis 2 y 3 – Difusión de información reservada. Pena: hasta 4 años.	Ley General de Protección de Datos Personales (LGPD) – Multa administrativa de hasta 50 millones de reales y sanción penal.	Solo Brasil combina multa civil alta con sanción penal; Ecuador y los demás solo contemplan la vía penal.
Conductas emergentes (deepfakes sexuales, fraude cripto-romántico)	No hay artículo específico: se procesa por estafa o delitos contra la intimidad.	Proyecto de Ley Orgánica enviado al Congreso el 25 de marzo de 2025 crea un tipo penal para deepfakes sexuales y grooming mediante IA.	Se tramita como fraude genérico; no existe figura autónoma.	Debate parlamentario (PL 4719/2019) para penalizar la creación y difusión de deepfakes; aún sin aprobación.	Vacío normativo general; España lleva ventaja con su proyecto de 2025.

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

2.6.9 Políticas criminales empleadas por los países considerados en el derecho comparado para su debida prevención de los delitos cibernéticos

Los engaños digitales en redes sociales y mensajería requieren algo más que la mera tipificación penal, los estados han aprobado políticas públicas de ciberseguridad que combinan educación, gestión de incidentes y coordinación con proveedores de Internet (International telecommunication Union, 2020).

Ecuador publicó la Estrategia Nacional de Ciberseguridad 2022 y 2025, que reserva un eje completo a la prevención de fraudes en plataformas sociales, allí se exige a las operadoras móviles difundir alertas sobre perfiles falsos y phishing en whatsapp y facebook (Ministerio de telecomunicaciones y de la sociedad de la informacion, 2021).

En España, el plan nacional de ciberseguridad es proveer de 150 actuaciones, entre ellas el programa Generación D, que creará hasta 1.500 espacios de capacitación donde la ciudadanía aprende a reconocer estafas en Instagram, tiktok y telegram, la ejecución corre a cargo del Instituto nacional de ciberseguridad de España (NCIBE) y del foro nacional de ciberseguridad (Departamento de seguridad nacional , 2022).

México actualizó su marco preventivo con la Política Nacional de Ciberseguridad 2023, que obliga a bancos, fintech y operadoras móviles a emitir alertas sobre smishing y deep-fake cuando surgen nuevas campañas de fraude en redes sociales y mensajería (Estrategia nacional de ciberseguridad, 2017)

En Brasil, la Estratégia Nacional de Segurança Cibernética E-Ciber, decreto una encomienda al Computer Emergency Response Team de Brasil, este al publicar guías trimestrales sobre fraudes románticos y clonación de cuentas de WhatsApp Business, distribuidas a escuelas y empresas (E-ciber , 2020).

Estos ejemplos muestran que la prevención es transversal: los países combinan legislación penal, educación digital temprana y alertas masivas para reducir la impunidad en los engaños digitales (International telecommunication Union, 2020).

2.7Jurisprudencia y casos emblemáticos en materia de ciberdelito (2020-2025)

2.7.1 Ataque al Banco Pichincha (octubre 2021): Primera reacción regulatoria formal

Hecho un ransomware inhabilitó parte de la banca en línea y los cajeros de la mayor entidad financiera del país.

Actuación la superintendencia de bancos declaró el incidente como acto delictivo y activó su protocolo de ciberseguridad, obligando al banco a aislar servidores y reportar indicadores de continuidad.

Relevancia en este caso inauguró la obligación de notificar incidentes graves a la Superintendencia y evidenció la falta de una Ley de seguridad digital que exija plazos homogéneos de reporte (Superintendencia de bancos , 2021).

2.7.2 Allanamiento a la Corte Provincial del Guayas (junio 2021): Interceptación ilegal de datos

Hecho la Fiscalía y la Policía allanaron oficinas judiciales para investigar la supuesta manipulación del sistema de sorteos electrónicos de causas mediante interceptación y desvío de datos.

Etapa procesal se abrió una investigación previa por el artículo 230 COIP, por interceptación ilegal, seis funcionarios fueron retenidos para pericias forenses.

Aporte marcó el primer uso del art. 230 contra funcionarios públicos y subrayó la necesidad de cadena de custodia digital dentro de la propia Función Judicial (Diario primicias Ecuador, 2021).

2.7.3-. Registro Civil vs tramitadores de turnos (julio 2023)

Hecho la dirección general del registro civil denunció ante la fiscalía a once páginas web y perfiles de Facebook Marketplace que cobraban entre USD 5 y 25 por turnos rápidos para cédulas y pasaportes.

Calificación jurídica la fiscalía abrió indagación por estafa y apropiación fraudulenta arts. 186 y 190 COIP, se incautaron dominios, se bloqueó la pasarela de cobro usada en línea.

Importancia del caso fijó un precedente su venta de citas gubernamentales, aunque el servicio sea gratuito, lesiona el patrimonio de la víctima y la fe pública digital (Primicias, 2023).

2.7.4 Sentencia 200-20-EP/22 de la Corte Constitucional (mayo 2023)

Supuesto de hecho el Tribunal Penal del Azuay había condenado por apropiación fraudulenta por medios electrónicos, la defensa alegó violaciones al debido proceso, esta ecisión de la Corte Constitucional dejó sin efecto un auto que había archivado la apelación, ordenó retrotraer el proceso y envió lineamientos sobre la motivación cuando se juzgan delitos informáticos, subrayando la necesidad de peritajes técnicos imparciales.

Valor doctrinal en primer pronunciamiento constitucional menciona explícitamente el art. 190 COIP y la obligación de capacitar a jueces en materia digital (Ecuador C. C., 2023).

2.7.5 Ciberdelincuencia y rezago judicial — informe Expreso (julio 2025)

El contenido del reportaje recoge datos oficiales 20602 denuncias por ciberdelitos entre 2022 mayo y 2025del mismo mes, el cual pone un 57 % que corresponde a apropiación fraudulenta, esto analiza fallos contradictorios en estafas con criptomonedas y señala la demora del legislativo para tipificar deepfakes y pig butchering.

Este impacto aunque no es una sentencia, el artículo cita entrevistas con magistrados y académicos y se ha convertido en lectura obligada para el debate parlamentario sobre la nueva ley de seguridad digital (Mera, 2025).

Por lo antes mencionado podemos observar lo siguiente:

- El predominio del art. 190 COIP, casi todas las sentencias firmes se fundamentan en apropiación fraudulenta, aun cuando la conducta combina engaño previo estafa y manipulación técnica esto confirma el problema de solapamiento tipológico (COIP, 2021).
- Evidencia digital insuficiente en varios fallos la Corte anula procesos por peritajes incompletos o falta de cadena de custodia, como recordó la sentencia 200-20-EP/22.

- Escasa persecución de estafas con IA y cripto, la inteligencia artificial y las criptomonedas, el IA es una rama de la informática que se enfoca en crear sistemas y programas capaces de realizar tareas que normalmente requieren inteligencia humana y las cripto son una moneda digital o virtual que utiliza criptografía para asegurar las transacciones, controlar la creación de nuevas unidades y verificar la transferencia de activos, en esto no existe, a la fecha un caso con condena firme por deepfakes o pig butchering, lo que demuestra el vacío normativo.
- Rol creciente de la vía administrativa la Superintendencia de Bancos y Arcotel han dictado medidas cautelares bloqueo de dominios, protocolos de notificación que sirven de base para futuras tipificaciones penales (Superintendencia de bancos , 2021).

2.8 Dimensión técnico-tecnológica

Los engaños digitales combinan ingeniería social con herramientas avanzadas de software malicioso y obligan a perfeccionar la trazabilidad forense de la evidencia a continuación, procedo a describir los cuatro ejes técnicos que hoy definen el ciberdelito en Ecuador y la región.

2.8.1 Ingeniería social y patrones de ataque

El pilar operativo de la mayoría de fraudes sigue siendo convencer al usuario de que entregue sus credenciales, en 2025 Latinoamérica padece 1.925 ciberataques semanales por organización, un aumento interanual del 108 %; las campañas de phishing protagonizan el repunte (Peralta, 2025).

El CSIRT-EC ha documentado oleadas de correos que suplantan cuentas internas de Microsoft 365 y sortean filtros mediante envío directo, además de malspam que distribuye falsos comprobantes de pago en PDF (CNT, 2025).

Estas campañas refuerzan la validez de la Teoría de las Actividades Rutinarias los cuales explotan la rutina diaria de revisar correo y redes sociales sin verificación de remitente.

2.8.2 IA generativa y deepfakes como multiplicador del engaño

La Inteligencia Artificial ya permite clonar voces en tiempo real y crear vídeos hiperrealistas a bajo coste, un informe del Innovation Lab de Europol alerta de que los deepfakes facilitan el fraude financiero y la extorsión sexual al borrar la línea entre contenido real y fabricado (Europol, 2022).

Interpol por su parte, reporta el uso de IA para generar anuncios de empleo falsos que captan víctimas de trata y alimentan centros de estafa en Asia, África y ahora también Centroamérica (Interpol, 2025).

En México, los ataques con voces sintéticas y vídeos manipulados elevaron un 220 % los casos de phishing entre 2022 y 2023, tendencia que se replica en Ecuador según la Superintendencia de Bancos (Rodríguez, 2024).

Relación de IA y engaños digitales

La inteligencia artificial potencia los engaños digitales porque permite generar mensajes y deepfakes muy convincentes, personalizar automáticamente cada ataque según la víctima y dirigir botnets que adaptan su malware en tiempo real, con ello aumentan la eficacia del phishing, el malspam y el malware bancario, y se vuelve más difícil para los sistemas de seguridad detectar y bloquear las amenazas (Analytic exchange program , 2024).

2.8.3 Botnets, malspam y malware bancario

La infraestructura criminal se apoya en redes de dispositivos zombis para distribuir troyanos bancarios y ransomware el cual es un programa malicioso que secuestra y bloquea los archivos en este panorama de amenazas 2024 de Kaspersky es las empresas internacionales de ciberseguridad, el cual revela que América Latina recibió más de 1,1 billones de intentos de infección entre junio 2023 y julio 2024, es decir, unos 2,2 millones de ataques por minuto los troyanos más detectados apuntan a aplicaciones de banca móvil (kaspersky, 2024).

Una variante del botnet Mirai cuál es la red de dispositivos infectados, este sigue aprovechando routers domésticos y cámaras IP sin parchear, superando los 1.700 millones de intentos de explotación en un año (kaspersky, 2024).

Estas cifras explican por qué el art. 232 COIP, que sanciona el sabotaje a sistemas, es cada vez más invocado para perseguir ataques de denegación de servicio y ransomware.

2.8.4 Trazabilidad y cadena de custodia digital

La solidez de un proceso penal depende de preservar la integridad de los logs, hashes y metadatos que prueban el ataque, la norma ISO/IEC 27037:2012 el cual adoptada como referencia por el esquema gubernamental de seguridad de la información (EGSI 3.0) detalla las fases de identificación, recolección, adquisición y preservación de evidencia, exigiendo documentar quién accede a cada artefacto, en qué momento y con qué herramienta (Hux, 2024).

2.8.5 Conclusión de los cuatros ejes antes mencionados

El delito informático actual no depende solo de códigos maliciosos se nutre de psicología del usuario, IA generativa y ecosistemas de botnets que automatizan ataques a escala continental, paralelamente, la prueba electrónica debe recogerse bajo estándares confiables para ser admisible sin una comprensión integral de estos cuatro ejes, las reformas legales y la estrategia de persecución penal quedarán siempre un paso atrás de la tecnología criminal.

2.9 Impacto socio-económico y victimología

Los ciberdelitos ya no representan solo un problema tecnológico, actualmente erosionan la economía, afectan la salud mental y golpean con más fuerza a determinados colectivos, la cual describiré los hallazgos más sólidos para Ecuador y el contexto global reciente.

2.9.1 Costos económicos directos

Pérdidas globales récord, el Internet Crime Complaint Center (IC3) del FBI registró en 2024 USD 16.600 millones de daños un 33 % más que en 2023 pese a que las denuncias totales descendieron levemente a 859.532 desde 2000 el acumulado supera USD 50.500 millones (Sabin & Rubin, 2025).

En el Ecuador el fraude financiero informal ha crecido y la Superintendencia de Bancos detectó 38 pseudo financieras entre enero y junio de 2025 algunas movieron

más de USD 50 millones prometiendo duplicar capitales a través de redes sociales y WhatsApp (Universo, 2025).

Carga para el sector productivo. Un estudio académico de 2025 calcula que las pymes ecuatorianas destinan ya el 2,1 % de sus ventas a mitigar fraudes online software, seguros y contracargos y que uno de cada cuatro negocios paralizó operaciones al menos 24 horas por un ataque (Morales et al., 2025).

2.9.2 Costos sociales y de salud mental

El estrés, ansiedad y depresión según la Universidad de Cambridge, halló que las víctimas de fraude financiero muestran niveles de ansiedad y depresión comparables a los de sobrevivientes de delitos violentos, el 45 % deja de usar el banco implicado y el 17 % cierra su cuenta tras el incidente (Freitas, 2024).

Pérdida de confianza un análisis forense argentino documenta que el golpe emocional incluye quiebre de la confianza institucional y retraimiento social prolongado (Santos, 2025).

Psicólogos clínicos citados por Bio Catch señalan que la culpa y el estigma explican la baja tasa de denuncia: solo 1 de cada 9 víctimas formaliza la queja (Freitas, 2024).

2.9.3 Grupos más vulnerables

Las personas mayores, en especial las mujeres jóvenes y las micro empresas constituyen los blancos más frecuentes de los ciberdelitos patrimoniales en Ecuador.

En primer lugar, los adultos de 60 años o más concentran la mayor parte de las pérdidas: el informe 2024 del IC3 registró 147.127 víctimas sénior y USD 4.880 millones en daños, casi el 64 % del total global y un 43 % más que en 2023 el promedio individual supera los USD 83. 000, lo que confirma su exposición desproporcionada a fraudes de soporte técnico, romances y estafas de inversión, incluidos mecanismos pig butchering con criptomonedas (Justice, 2025).

Estados Unidos, FBI destaca el creciente número de casos de fraude a personas mayores denunciados antes del Día Mundial de Concientización sobre el Abuso a las Personas Mayores (FBI US, 2025).

En el caso de las mujeres de 15 a 29 años, los delitos de sextorsión y deepfakes sexuales han crecido con rapidez, un estudio del Taller de Comunicación Mujer y ONU Mujeres reveló que todas las denuncias por violación a la intimidad y extorsión sexual interpuestas entre 2019 y 2023 en Quito, Cuenca y Guayaquil terminaron sin sentencia condenatoria, mientras que buena parte de las víctimas desistió de continuar el proceso por desgaste emocional y estigma social, esta impunidad refuerza la percepción de riesgo y explica la baja tasa de denuncia efectiva (Carrillo, 2024).

Por último, las micro empresas y emprendimientos sufren un impacto crítico porque carecen de defensas técnicas y de personal especializado, el reporte Chequeo Digital 2022-2023 del Ministerio de Telecomunicaciones indica que más del 50 % de las microempresas ecuatorianas permanece en el nivel Inicial de madurez digital y apenas el 6 % alcanza el nivel experto esa brecha se traduce en falsos correos de pago, Business Email Compromise y ransomware que pueden paralizar operaciones durante días o forzar el cierre temporal del negocio (Telecomunicaciones M. d., 2023).

En conjunto, estas tres poblaciones muestran cómo la combinación de baja alfabetización digital, alta exposición en línea y recursos preventivos limitados multiplican la probabilidad de victimización en el ecosistema de engaños digitales.

2.9.4 Repercusiones macroeconómicas

- Erosión de la confianza financiera: Cada estafa masiva reduce en 0,3 puntos la intención de uso de banca móvil, según la Superintendencia esto obliga a las entidades a invertir más en autenticación robusta y eleva las tarifas al usuario final (Morales & Ramírez, 2025).
- Desvío de gasto público: El Registro Civil destinó USD 1,2 millones extra en 2023 para rediseñar su portal de citas tras la ola de tramitadores digitales (Internet crime complaint, 2024).
- Brecha de innovación: El 42 % de startups fintech ecuatorianas retrasó el lanzamiento de productos en 2024 por requisitos de certificación ISO 27001 exigidos por los inversores tras los incidentes de ransomware. (Morales et al., 2025).

2.9.5 Conclusiones para la victimología ecuatoriana

Por lo anteriormente analizado, podemos observar que el perfil típico de la víctima combina alta exposición digital y bajo dominio técnico, no necesariamente bajos ingresos; así mismo las pérdidas monetarias son solo la punta del iceberg, la ansiedad además del aislamiento y pérdida de confianza perduran por meses, sobre todo en adultos mayores (FBI US, 2025).

Además, que la cifra negra sigue siendo alta: la vergüenza y la sensación de autoculpa disuaden de denunciar, lo que subestima las estadísticas oficiales, por ende, las empresas asumen un coste añadido en servicios de soporte emocional y compensación, lo que se traslada vía tarifas al conjunto de consumidores (FBI US, 2025).

2.10 Factores humanos y cibercultura

Los engaños digitales prosperan cuando las brechas de alfabetización tecnológica se combinan con sesgos cognitivos, la autoridad, urgencia, prueba social con la desinhibición que brinda el anonimato en línea, en Ecuador, aunque el analfabetismo digital en la población de 15 a 49 años bajó al 5,4 % en 2024, la desigual capacidad para reconocer riesgos mantiene a muchos usuarios expuestos a tácticas de phishing, suplantaciones y fraudes por mensajería; comprender esta interacción entre personas y cibercultura es clave para diseñar estrategias de prevención y respuesta efectivas (Instituto nacional de estadistica y censos , 2024).

2.10.1 Alfabetización digital desigual

El INEC muestra que el analfabetismo digital cayó de 8,2 % en el 2022 a 5,4 % en el 2024, pero persiste una fuerte brecha geográfica, pero sólo el 12 % de los hogares rurales dispone de computador, frente al 61 % urbano (Proaño, 2025).

Esta combinación de mayor conectividad y baja capacitación crea una ventana de oportunidad que los estafadores aprovechan mediante phishing y ofertas falsas (Instituto nacional de estadistica y censos , 2024).

2.10.2 Sesgos cognitivos que facilitan el fraude

Un metaanálisis de 2025 identificó cinco sesgos decisivos en las víctimas: autoridad, urgencia, optimismo diciendo que a mí no me pasará, reciprocidad y prueba social, al introducir advertencias que neutralizan esos sesgos, la tasa de clics maliciosos se redujo 43 % (Radnaeva & Semenova, 2025).

Estudios de psicología aplicada confirman que incluso personas con alto nivel educativo caen en estafas cuando el mensaje combina miedo y escasez temporal (Cherry, 2024).

2.10.3 Efecto de desinhibición on-line

La sensación de anonimato, la falta de contacto visual y la asincronía comunicativa favorecen conductas que el usuario no exhibiría cara a cara unas investigaciones sobre desinhibición explican parte del auge de los comentarios llevan al fraude romántico (Wang et al., 2024).

2.10.4 Confianza cultural y desinformación

Latinoamérica registra altos niveles de desconfianza institucional, pero paradójicamente elevada confianza interpersonal en redes, un estudio en Nature Humanities and Social Sciences Communications halló que esta combinación favorece la viralidad de fake news y promociones fraudulentas, porque el usuario confía más en el reenvío de un conocido que en el desmentido oficial (López et al., 2025).

El fenómeno se intensifica en contextos de polarización política, como se vio en la campaña electoral mexicana de 2024, plagada de audios y vídeos generados por IA (klepper, 2024).

2.11 Persecución penal y cooperación internacional

Entre 2021 y 2025 la persecución penal de los engaños digitales en el Ecuador evolucionó desde unidades dispersas hacia una red especializada que ya opera, aunque con limitaciones en sincronía con los principales estándares y tratados internacionales.

La pieza de partida está en la Unidad de Investigaciones Tecnológicas de la Fiscalía, que desde 2024 dispone de un laboratorio forense con certificación ISO 17025:2018 para análisis de discos, móviles y cripto-billeteras esta acreditación, otorgada por el Servicio de Acreditación Ecuatoriano, garantiza la validez probatoria de los peritajes en juicio (Forenses, 2023).

En paralelo, la Dirección Nacional de Ciberdelitos de la Policía se conectó a la plataforma i-24/7 de Interpol y, con apoyo de Europol y Ameripol, desarmó en 2025 una red de phishing Iserver que operaba a la vez en Guayaquil y Madrid, primera operación conjunta que culminó con órdenes de registro en seis países (Ecuador P. N., 2024).

En el frente preventivo-técnico, el CSIRT-EC (GovCERT) asumió la coordinación nacional de incidentes y en agosto 2024 superó la auditoría de madurez SIM3 auspiciada por la OEA-CICTE, lo que lo coloca en el pelotón de los diez equipos latinoamericanos con ese nivel (Naciones, 2024).

A su alrededor ya funcionan CSIRT sectoriales energía (CELEC-EP) y telecomunicaciones (CNT-EP) que intercambian feeds de amenazas en tiempo real con la red CSIRTAmericas (Naciones, 2024).

Todos aplican el Esquema Gubernamental de Seguridad de la Información v 3.0 (EGSI), obligatorio desde marzo 2024 y alineado a ISO 27001-2022 e ISO 27037-27042 para cadena de custodia.

Incluso se pilotea un módulo blockchain que sella los hashes de la evidencia antes de subirlos al expediente digital, con el fin de cerrar discusiones sobre manipulación.

En el plano externo, el país dio un paso decisivo al depositar el instrumento de adhesión al Convenio de Budapest el 12 de diciembre de 2024, convirtiéndose en el Estado Parte n.º 77 (Europeo, 2024).

Ello obliga a contar con un Punto de Contacto 24/7: gracias al programa GLACY-e, fiscales y policías realizaron en noviembre 2024 una pasantía en Santo Domingo para replicar la estructura operativa dominicana y se comprometieron a responder solicitudes urgentes de otros países en menos de dos horas.

Además, Ecuador nutre su cooperación a través de MLAT bilaterales con España 2019 y Brasil 2022, que agilizan interrogatorios remotos y traslado de evidencias electrónicas sin la demora de las comisiones rogatorias clásicas (Gobierno, 2019).

2.12 Políticas públicas y prevención

Ecuador ha tejido en los últimos cuatro años un entramado de normas, campañas y alianzas que busca reducir la superficie de ataque y elevar la resiliencia digital del Estado, las empresas y la ciudadanía, aun así, el sistema sigue mostrando fragmentación regulatoria y brechas educativas que los estafadores aprovechan (Telecomunicaciones, 2024).

2.12.1 Marco estratégico y normativo

Esquema Gubernamental de Seguridad de la Información (EGSI v 3.0), el Acuerdo Ministerial MINTEL-2024-0003 volvió obligatorio para todas las entidades públicas un Sistema de Gestión de Seguridad alineado (ISO/IEC), el 27001:2022 e ISO 27037-27042 su cadena de custodia, el EGSI impone controles mínimos, auditorías anuales y reporte de incidentes críticos en 24 h (Telecomunicaciones, 2024).

Proyecto de Ley Orgánica de Seguridad Digital, aprobado para primer debate en junio 2024, crea un Sistema Nacional de Ciberseguridad, tipifica el incidente grave y fija multas de hasta 2 % de la facturación a quien no reporte brechas, el texto incorpora referencias a la Directiva europea NIS 2 y al Convenio de Budapest (Comisión Especializada Permanente de Soberanía, 2023).

Circular SB-IG-2024-0003-C, desde enero 2024 la Superintendencia de Bancos obliga a cada entidad financiera a notificar cualquier incidente que afecte un servicio crítico, enviar informe preliminar en 5 minutos y la causa raíz en 5 días se debe preservarse la evidencia digital por 5 años (Banco, 2024).

Ley Orgánica de Inteligencia en junio 2025, aunque pretende reforzar la lucha contra el crimen organizado, organizaciones civiles alertan de que habilita interceptaciones sin control judicial y puede erosionar la confianza ciudadana en la protección de datos.

2.12.2 Estructura operativa y cooperación

CSIRT-EC certificado SIM3. En agosto 2024 el equipo nacional fue certificado por la OEA como CSIRT de nivel básico de madurez, requisito para integrarse a la red CSIRTAmericas y recibir feeds de indicadores de compromiso.

Punto de Contacto 24/7, tras la ratificación del Convenio de Budapest en Octubre del 2024 la Fiscalía habilitó el punto de contacto permanente con apoyo del programa GLACY-e, con meta de responder solicitudes urgentes en menos de 2 h y preservar datos transfronterizos.

CSIRT sectoriales la energía (CELEC-EP) y telecomunicaciones (CNT EP) operan equipos propios que comparten alertas con el GovCERT, creando una malla vertical para infraestructuras críticas.

2.12.3 Prevención y cultura de ciberseguridad

Campaña Conectad@s Seguros, el Ministerio de Educación capacita a estudiantes de básica y bachillerato en reconocimiento de phishing, sextorsión y suplantación de identidad incluye guías pdf y protocolos frente a violencia digital.

Protocolos escolares de violencia digital publicados en 2023 los cuales establecen rutas de denuncia, primeros auxilios psicológicos y obligatoriedad de reportar a la Fiscalía cuando hay difusión no consentida de imágenes íntimas.

Sector financiero, la Asociación de Bancos (ASOBANCA) coordina simulacros de cibercrisis y campañas de doble autenticación; la Circular SB-IG-2024-0003-C consolidó el envío de reportes en tiempo real a la Superintendencia (Banco, 2024).

PYMES y sello Empresa Digital Segura, MINTEL y CAF lanzaron en 2025 un programa que subvenciona hasta el 70 % del costo de auditorías ISO 27001 para micro empresas exportadoras 112 compañías obtuvieron el sello en el primer semestre (Banco, 2024).

2.12.4 Errores de Subsunción (Tipificación)

El error de subsunción más frecuente en las investigaciones de ciberdelito ecuatorianas consiste en que las fiscalías formulan cargos por estafa del artículo 186

COIP cuando los hechos alteración de un sistema, uso de scripts o malware encajan en la apropiación fraudulenta por medios electrónicos del artículo 190, un estudio empírico de revista Lex revisó 62 sentencias dictadas entre 2022 y 2023 y comprobó que 41 % de las acusaciones aplicaban el artículo 186 aunque el peritaje acreditaba manipulación informática, error que terminó en nulidad o absolución en la mitad de los casos (Olivares, 2024).

Una tesis de la Universidad Técnica del Norte añade que los fiscales prefieren la estafa porque resulta más fácil de explicar al juez, aun cuando la conducta sea 100 % digital, lo que diluye la tipicidad y favorece la impunidad, la Corte Constitucional recordó en la Sentencia 601-18-EP/23 - 20-dic-2023 que el juez puede reconducir la figura jurídica sin violar el derecho de defensa, pero exigió a la Fiscalía describir con precisión los elementos técnicos y adjuntar peritajes imparciales de lo contrario, el proceso se anula por falta de motivación (Bonilla, 2025).

Revistas especializadas de la Corte Nacional, llamado ensayos penales #15, junio 2025 el cual denuncian que algunos fiscales mezclan artículos, por ejemplo formulan cargos por apropiación 190 y piden medidas precautelares con la lógica de transferencia 231, provocando autos de nulidad porque el juez no sabe qué pena graduar (Corte nacional de justicia , 2025).

Tres factores explican la confusión:

1. Brecha forense: Según el Informe 2024 de la Fiscalía, solo dos laboratorios policiales tienen acreditación ISO 17025, de modo que muchos expedientes carecen de peritajes que prueben la alteración o manipulación exigida por el artículo 190, y el fiscal se refugia en la estafa tradicional (Scielo , 2025).

2. Redacción solapada del COIP: Los verbos engañar el art. 186 e utilizar fraudulentamente un sistema el art. 190, aparecen sobrepuestos, generando inseguridad interpretativa aspecto subrayado por la investigación publicada en Invecom sobre estadística de ciberdelitos 2019 y 2024 (Scielo , 2025).

3. Presión estadística: Primicias reportó que de 412 incidentes críticos notificados por la banca en 2024, solo 35 llegaron a sentencia firme, lo que

incentiva a la Fiscalía a escoger la figura con mayor tasa histórica de condena, aun si no describe bien el medio comisivo (Primicias, 2024).

4. Consecuencias: Nulidades parciales, retrotracción a la audiencia de formulación, prescripción en algunos casos y desconfianza pública en la justicia digital, líneas de mejora ya propuestas en foros académicos y judiciales:

    - Manual interno que explique con ejemplos forenses cuándo corresponde estafa, apropiación, transferencia o interceptación.
    - Requisito de informe pericial mínimo hashes, logs, comparación de bases de datos para admitir la formulación de cargos por los artículos 190, 231 y 232.
    - Capacitación obligatoria en cibercrimen para fiscales de territorio mediante el programa GLACY-e y la Escuela de la Función Judicial.
    - Reforma puntual del COIP que separe claramente la estafa tradicional de la estafa informática modelo art. 248.2 del Código Penal español e incorpore tipos autónomos para deepfakes y fraudes cripto románticos, reduciendo así la ambigüedad subsuntiva (Primicias, 2024).
    - *…1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero…*

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Enfoque de la investigación

La metodología cualitativa se centra en comprender a fondo los fenómenos sociales, jurídicos y culturales a partir de datos no numéricos privilegia la reconstrucción de significados, percepciones y experiencias tal como los actores las viven, de modo que el investigador interprete la realidad en toda su complejidad y contexto (Creswell, 2019).

A diferencia de los enfoques cuantitativos sustentados en la medición estadística la investigación cualitativa adopta una mirada interpretativa y naturalista, el cual estudia las cosas en sus ambientes naturales para darles sentido desde la perspectiva de quienes las experimentan, por ende en la presente investigación no se usará la metología Cuantitativa (Hernández et al., 2014).

La metodología cualitativa resulta especialmente provechosa en la investigación jurídica porque permite examinar a fondo el contenido normativo, la aplicación práctica de las leyes y la interpretación que hacen jueces y fiscales, aspectos difíciles de capturar con simples estadísticas (Ian, 2002).

Dobinson & Johns explican que el investigador jurídico cualitativo estudia las normas en situción para descubrir cómo operan en la vida real y para detectar vacíos o contradicciones que los números por sí solos no muestran (Ian, 2002).

3.2 Alcance de la investigación: (Exploratorio, descriptivo o correlacional)

El presente trabajo tiene un alcance descriptivo con componentes exploratorios, en sentido descriptivo, su objetivo principal es caracterizar y explicar cómo se manifiestan los engaños digitales en redes sociales y servicios de mensajería instantánea dentro del contexto jurídico ecuatoriano, se detallan las modalidades de fraude, las disposiciones legales aplicables dentro del arts. 186 y 190 concordantes del COIP y las formas en que la práctica forense y judicial resuelve o no cada caso, tal como lo señalan (Hernández et al., 2014).

La investigación descriptiva busca especificar propiedades, rasgos y perfiles de personas, grupos o procesos para ofrecer un panorama preciso del problema (Hernández et al., 2014).

En su dimensión exploratoria, el estudio indaga un fenómeno emergente sobre el que existe escasa bibliografía jurídica nacional por tanto, requiere abrir camino para futuras investigaciones (Creswell, 2019).

Este componente exploratorio es pertinente porque las estafas basadas en phishing, deepfakes o cripto fraude se desarrollan con gran rapidez tecnológica, mientras la doctrina y los operadores de justicia aún no han analizado con profundidad sus implicaciones penales (Creswell, 2019).

Ambos alcances convergen en un estudio de caso múltiple se analizan expedientes concretos (ej. ataque a Banco Pichincha en 2021) para ilustrar la brecha entre el texto de la ley y su aplicación real.

Así se busca evidenciar cómo la subsunción errónea o la falta de peritajes especializados puede derivar en escenarios de impunidad y, simultáneamente, se identifican vacíos normativos y procesales que permitan proponer ajustes legales y buenas prácticas institucionales.

3.3 ESTUDIO DE CASO

3.3.1 Nombre del caso No.1 : Ciber ataque al Banco de Pichincha.

Introducción

En la madrugada del 10 de octubre de 2021, Banco Pichincha el más grande del sistema financiero ecuatoriano amaneció con todos sus cajeros automáticos fuera de servicio y su página de banca en línea declarada en mantenimiento, aún antes de que amaneciera, la entidad había detectado un ataque informático grave y decidió suspender todos sus servicios para evitar mayores problemas con los usuarios financieros.

¿Qué ocurrió exactamente?

El problema se originó cuando un empleado abrió un correo electrónico que parecía legítimo, ese mensaje instaló un programa maligno ransomware LockBit-software malicioso diseñado para bloquear el acceso de los usuarios a los sistemas informáticos a cambio del pago de un rescate que, como candado invisible, empezó a cifrar los archivos más importantes del banco, ante la alerta interna, los técnicos aislaron los servidores principales y desconectaron los cajeros, la app móvil para impedir que el candado se propagara, así se inició una caída de servicios que duró casi cuatro días.

Respuesta de las autoridades

A las ocho de la mañana de ese domingo la Superintendencia de Bancos ya tenía un informe preliminar en su mesa la misma Superintendencia calificó el hecho como ciber-evento sistémico y desplazó inspectores a las instalaciones del banco, esta experiencia terminó inspirando la circular SB-IG-2024-0003-C, que ahora obliga a todos los bancos a avisar a la autoridad en cinco minutos y a detallar la causa del incidente en un lapso de cinco días**.**

La investigación

Peritos de la Fiscalía y del CSIRT-EC (Centro de Respuesta a Incidentes de Seguridad Informática del Ecuador), analizaron los equipos y concluyeron que el ataque se dio por phishing y aprovechó una falla conocida de Windows PrintNightmare (vulnerabilidad de seguridad crítica que afecta al servicio de impresión de Windows), para tomar el control de los servidores, el banco no perdió dinero porque sus copias de seguridad estaban a salvo en otro centro de datos, pero la Fiscalía abrió un proceso penal por ataque a sistemas art. 232 COIP y tentativa de apropiación fraudulenta por medios electronicos art. 190.

El caso aún no llega a la etapa de juicio, debido a que aún faltan peritajes certificados y sólo existen dos laboratorios policiales con acreditación ISO 17025 estándar internacional que establece los requisitos para la competencia técnica de los laboratorios de ensayo y calibración para estos análisis.

Costos y daños colaterales

El banco calcula que dejó de ganar unos 980.000 dólares en comisiones y recibió más de cuatro mil reclamos de clientes indignados, además durante las dos semanas siguientes, las aplicaciones de bancos competidores se descargaron un 17 %, muchos usuarios prefirieron diversificar su dinero ante el susto.

Lecciones que dejó el caso

- Proteger las cuentas administrativas con doble verificación y desactivar accesos remotos que no se usan.
- Ensayar, cada trimestre, la restauración de los respaldos para comprobar que realmente funcionan.
- Contratar un seguro de ciberriesgo que cubra los gastos de recuperación y posibles rescates.
- Conservar todas las bitácoras y fijarlas con firmas digitales para que sirvan como prueba en el juicio.

Reflexión final de la investigadora sobre el caso

El episodio mostró que un simple correo engañoso puede paralizar a toda una institución financiera y que, sin una coordinación rápida entre el banco, la Superintendencia y la Fiscalía, el golpe habría sido mayor, también evidenció las tareas pendientes más laboratorios acreditados, tipos penales actualizados para los nuevos métodos de ataque y personal forense suficiente para que los procesos no se queden a medio camino.

3.3.2 Estudio del caso No.2

Nombre del caso No.2 : Apropiación fraudulenta por medios electrónicos: phishing 'Servicio Postal' (abril 2025)

Introducción

En abril de 2025, Andrea y Luis una pareja que esperaba un paquete importado, recibieron un correo y un mensaje de WhatsApp supuestamente enviados por Servicios Postales del Ecuador, el texto advertía que el envío estaba retenido por una dirección incorrecta y pedía pagar USD 0,36 a través de un enlace para regularizar la entrega, confiados los usuarios ingresaron los datos de su tarjeta de

crédito en menos de dos horas los delincuentes realizaron compras en el exterior por USD 2 000, la estafa se denunció ante la Fiscalía y fue tipificada como apropiación fraudulenta por medios electrónicos mencionado en el art. 190 COIP (Tapia, 2025).

Cronología del hecho

1. Correo/WhatsApp de phishing que clona la imagen del servicio postal Correos del Ecuador.
2. URL trampa con formulario para pagar la tasa.
3. Captura en tiempo real de número, CVV y token de la tarjeta de crédito de la víctima.
4. Compras internacionales con cargo inmediato antes de que el banco detecte el fraude.

Evidencia recabada durante su investigación

1. Capturas del correo y del chat de WhatsApp.
2. Registro de IP de origen (VPN europea).
3. Estado de cuenta que muestra transacciones no autorizadas.
4. Informe pericial que verifica el sitio falso y el phishing kit usado.

Tratamiento legal y dificultades

La Fiscalía inició la causa bajo el art. 190 Apropiación fraudulenta por medios electronicos, pero el banco tardó 45 días en entregar los registros de autenticación, además la defensa alegó que se trataba de una estafa art. 186 porque la víctima ingresó sus datos voluntariamente, el fiscal mantuvo la acusación al demostrar que existió manipulación de una plataforma electrónica para obtener el dinero.

conclusiones para la investigación

1. Error de subsunción recurrente: operadores confunden estafa clásica con apropiación electrónica.
2. Retardo probatorio: sin una orden de preservación rápida, los bancos tardan en remitir los logs (registros o bitácoras bancarias).
3. Necesidad de educación preventiva: la pareja desconocía la regla de no ingresar datos bancarios en enlaces externos.

Reflexión final de la investigadora sobre el caso

Este caso refleja, a pequeña escala, el corazón del presente trabajo un fraude que nace en la ingeniería social, se materializa en un medio electrónico y plantea el mismo problema de aplicar correctamente el tipo penal (Delito) para evitar la impunidad.

3.4 Técnica e instrumentos para obtener los datos

Para la presente investigación, usaré las siguientes técnicas de recolección de datos:

Tabla 6.

Técnica e instrumentos para obtener los datos

Técnica	Instrumento
Análisis documental	Revisión sistemática de normas jurídicas (COIP, Constitución), jurisprudencia, doctrina, informes oficiales y artículos académicos.
Estudio de caso	Guía de análisis para el estudio detallado de casos reales sobre delitos informaticos, donde se identifique cómo se aplicó la ley (Caso Banco Pichincha).
Entrevista semiestructurada	Cuestionario guía aplicado a abogados, fiscales o expertos en derecho penal o informático, con preguntas abiertas para conocer su interpretación de los delitos informáticos.

Fuente: COIP (2021)

Elaborado por: Litardo Gaona (2025)

3.4.1 Preguntas de la entrevistas

1. Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?
2. ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

3. ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?
4. ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?
5. ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?
6. ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?
7. Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador?

3.5 Población y Muestra

3.5.1- Población

La población está compuesta por abogados penalistas del Colegio de Abogados del Guayas, por usuarios de redes sociales y mensajería digital en Ecuador, quienes han sido o pueden ser víctimas de engaños digitales, esta definición permite un enfoque integral, tanto jurídico como social, de la problemática.

3.5.2- Muestra

La muestra se conformó por cinco abogados penalistas y una persona víctima de engaño digital, seleccionados mediante muestreo por conveniencia, a todos se les aplicó entrevistas como instrumento de recolección de información, esto permite analizar la aplicación legal desde la teoría, la práctica investigativa y la experiencia vivencial.

Tabla 7

Población

Población	Total	Porcentaje

Abogados en libre ejercicio afiliados al Colegio de Abogados del Guayas	15 138	100 %

Fuente: Colegio de Abogados del Guayas (2025)

Elaborado por: Litardo Gaona (2025)

Tabla 8.

Muestra

Grupo / Individuo	Tamaño de la muestra	Tipo de muestreo	Instrumento
Abogados especializados en Derecho Penal	5	Por conveniencia	Entrevista
Persona Afectada	1	Por conveniencia	Entrevista

Elaborado por: Litardo Gaona (2025)

CAPÍTULO IV

PROPUESTA O INFORME

Dentro de este capítulo se presentarán los resultados obtenidos, explicando cómo cada hallazgo se relaciona con los objetivos de la investigación y con la metodología aplicada. Asimismo, se ofrecerá un análisis crítico del problema abordado y se propondrán alternativas de solución basadas en la evidencia recopilada.

4.1 Presentación y análisis de resultados

Entrevista

Una vez realizadas las respectivas entrevistas a las y los abogados especialistas en materia penal, se presenta la descripción de sus respuestas, así como un análisis general de los datos que se hayan recogido.

Entrevistado No. 1

Mgtr. Kevin David García Coronel, Esp.

Perfil del Entrevistado: Abogado desde hace 6 años, ejerce la rama penal y ha patrocinado varias causas de conmocion social Caso Purga entre otros, posee titulos de Cuarto nivel a fin a la Materia. Posee estudios en Alemania y Colombia sobre Derecho Penal y tiene 6 años de experincia en materia Penal. Es Socio-Fundador del Estudio Jurídico Garcia Coronel

Títulos de 4to nivel

-Mgtr en Derecho Penal. (4to Nivel)

-Especialista En Cumplimiento Y Anticorrupcion (4to Nivel)

-Especialista En Garantias Jurisdiccionales Y Reparacion Integral(4to Nivel)

1.- Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?

Los casos que más veo involucran compras inexistentes en Marketplace o grupos de Telegram, seguidos por correos tipo ‘paquete retenido en Aduanas’ que conducen a enlaces de pago y roban la tarjeta. Últimamente se suman los fraudes con voz: llaman a adultos mayores en su mayoría imitando a un familiar y logran que transfieran dinero a cuentas de terceros.

2.- ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

Desde el ejercicio privado advierto que el 186 si funciona para fraudes simples, pero no abarca la complejidad de los actuales engaños en línea. Hoy el estafador combina ingeniería social con pequeñas rutinas de software que desvían pagos y borran huellas. Eso va más allá de ‘simular un hecho’ ante la víctima: hablamos de manipular todo un entorno digital. Para evitar vacíos, el COIP debería incorporar una figura autónoma de estafa informática, parecida al artículo 248.2 del Código Penal español

3.- ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?

Muchos casos se caen porque la policía judicial copia el contenido del celular o la computadora sin seguir el procedimiento o el protocolo correcto del peritaje, y esa prueba después es excluida. Además, pedir datos a empresas como Facebook o Google puede tomar meses; para cuando la información llega, el enlace ya no existe o la cuenta fue borrada, y nos quedamos sin prueba sólida para la audiencia de juicio.

4.- ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?

A mi parecer la legislación va un paso atrás: no menciona algunos fraudes informáticos de nueva generación ni fraudes con criptomonedas, y eso deja huecos que la defensa aprovecha. Con el marco actual se puede castigar, sí, pero el riesgo de impunidad sigue alto,

5.- ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?

Las plataformas extranjeras deberían estar obligadas a responder dentro de plazos cortos y en un formato estándar. Si Twitter o Telegram no entregan los registros de chat o de IP a tiempo, la Fiscalía se queda sin elementos de cargo y los responsables se aprovechan de ello.

6.- ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?

Para que la acusación prospere se necesitan principalmente los extractos bancarios, porque allí se ve la plata que salió y quién la recibió. A eso hay que sumarle la conversación completa (sin cortes) y un peritaje que explique con palabras simples cómo se engañó a la víctima

7.- Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador

Hace falta obligar a Facebook, WhatsApp o Telegram a nombrar un representante legal en Ecuador que responda en tiempo real a los pedidos de información. Mientras la asistencia internacional tarde meses, los culpables seguirán intocables.

Análisis de la entrevista:

La entrevista al Mgtr. Kevin García Coronel refuerza de forma directa la hipótesis central de la investigación: las estafas digitales que se ejecutan por redes sociales y mensajería avanzan más rápido que la legislación y que la práctica pericial ecuatoriana. En primer lugar, el jurista señala que los casos más frecuentes en sus expedientes son las ventas fantasma en Facebook Marketplace, los enlaces falsos de paquete retenido y las llamadas con voz clonada dirigidas sobre todo a adultos mayores; ello confirma que el fenómeno objeto de estudio no es marginal, sino la modalidad dominante de fraude patrimonial. En segundo término, advierte que el artículo 186 COIP sirve únicamente para engaños simples y que la complejidad actual como la ingeniería social combinada con software que desvía pagos y borra huellas¿

requiere un tipo penal autónomo de estafa informática, semejante al 248.2 español. Esta crítica respalda la necesidad de reformas específicas que la tesis plantea. El entrevistado también describe los principales obstáculos probatorios: extracción de datos de celulares sin protocolo adecuado, exclusión de esos elementos en juicio y demoras de meses para que Facebook o Google entreguen registros.

Entrevistada No. 2

Mgtr. Piedad Jacqueline Villacís Peña, Esp.

Perfil de la Entrevistada: Es abogada desde hace 28 años., ha ejercido la rama penal y laboral, patrocinó en el libre ejercicio varias causas en materia penal y actualmente ejerce el cargo de Jueza Penal en la Unidad del Cantón San Jacinto de Yaguachi, el cual lleva obstentando por el lapso de 10 años.

Títulos de 4to nivel :
-Mgtr en Derecho Laboral. (4to Nivel)

-Especialista En Consultoria Juridico Laboral (4to Nivel)

-Diploma Superior En Contratacion Laboral (4to Nivel)

1.- Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?

Normalmente al juzgado, nos llegan flagrancias o formulaciones de cargo ordinarias, por el delito de estafa, pero la fiscalía suele formular cargos por el delito antes mencionado, pero dentro de las instrucciones, piden reformular cargos al delito de apropiación fraudulenta por medios electrónicos o a veces por el delito de abuso de confianza.

2.- ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

El 186 fue concebido para el engaño tradicional cheques sin fondos, trampas cara a cara– y no recoge la rapidez ni la automatización de las estafas en redes sociales o apps de mensajería. He visto procesos en que la Fiscalía acusa por estafa,

pero las pruebas muestran claramente manipulación de sistemas, enlaces trampa y transferencias automáticas: eso encaja mejor en el 190 o incluso en el 231. Sin una reforma que especifique la modalidad digital corremos dos riesgos: absolver por falta de tipicidad o forzar la figura, vulnerando el principio de legalidad, por tanto, sí considero indispensable una reforma que describa la estafa electrónica, incluya agravantes por uso de tecnología avanzada y simplifique la prueba pericial para evitar la impunidad.

3.- ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?

Cuando llega la causa me encuentro con diligencias mal notificadas a proveedores extranjeros, discos duros clonados sin certificado y peritajes que no explican en términos sencillos cómo ocurrió la intrusión, esto complica la valoración de la prueba y, en ocasiones, obliga a devolverla para subsanar. También veo que la defensa aprovecha la falta de claridad entre los artículos 186 y 190 del COIP para alegar atipicidad, de modo que el proceso se dilata o en algunos casos se tiene que sobreseer a los procesados.

4.- ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?

La ley cubre básico todo, pero llega corta para los engaños más modernos. Cuando interviene inteligencia artificial o se mueve dinero en criptomonedas, el COIP no contempla agravantes ni reglas probatorias claras; esa brecha puede terminar en sobreseimientos o ratificaciones del estado de inocencia por falta de tipicidad.

5.- ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?

La asistencia internacional es clave para validar la prueba: si el chat o la transferencia provienen del exterior, solo con acuerdos firmes y formatos homologados puedo admitirlos en audiencia. Sin esa coordinación, la evidencia se vuelve impugnable y el caso se cae.

6.- ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?

Para mí los elementos más persuasivos son aquellos que encajan como piezas de un rompecabezas: primero, un informe pericial que certifique la autenticidad de los mensajes o correos donde se concreta el delito; segundo, el registro bancario que muestre la salida y la llegada del dinero; y, tercero, la confirmación del proveedor de Internet que vincule la dirección IP utilizada con el domicilio del procesado en algunos casos en los que se pueda obtener. Cuando estos tres elementos sin que haya contradicciones, la prueba resulta difícil de rebatir y la decisión judicial se vuelve mucho más clara.

7.- Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador

Necesitamos reglas claras de evidencia electrónica: que la ley diga cómo se captura, custodia y presenta un chat o un registro informático en estos casos. Así evitaríamos excluir pruebas por cadena de custodia deficiente. Además, convendría subir la pena con agravantes cuando las víctimas son adultos mayores o cuando el delito afecta servicios esenciales, como la banca en línea.

Análisis de la entrevista:

La jueza Piedad Villacís confirma el eje central de esta investigación: la norma y la práctica procesal no alcanzan a las estafas digitales actuales. Señala que la Fiscalía suele iniciar causas como estafa (art. 186) y luego reformular a apropiación fraudulenta por medios electrónicos (art. 190), generando retrasos y, a veces, sobreseimientos; ello evidencia el error de subsunción y respalda la propuesta de crear un tipo penal específico de estafa informática o por lo menos tener definiciones mas claras en la legislación. Entre los principales obstáculos destaca peritajes deficientes, discos clonados sin cadena de custodia y la tardanza de proveedores extranjeros en entregar datos, factores que obligan a excluir pruebas y favorecen la impunidad. Para una acusación sólida, la jueza prioriza tres piezas: peritaje que autentique los mensajes, registro bancario que trace el dinero y confirmación de la IP asociada al acusado. Finalmente, reclama reglas claras para capturar y presentar

evidencia electrónica y agravantes cuando la víctima sea adulto mayor o el ataque afecte servicios críticos, puntos que coinciden con las recomendaciones de esta tesis.

Entrevistado No. 3

Mgtr. German Alejandro Blum Espinoza, Esp.

Perfil del Entrevistado: Es Abogado desde hace 32 años, ha ejercido la rama penal desde que inicio como abogado y por ende ha patrocinado varias causas en materia penal cuando estaba en el libre ejercicio de su profesión. Actualmente ejerce el cargo de Juez del Tribunal de Garantías Penales en el cantón babahoyo, el cual lleva obstentando por el lapso de 16 años.

Títulos de 4to nivel :

-Mgtr en Derecho Penal y Criminología. (4to Nivel)
-Especialista En Derecho Penal Y Justicia Indigena (4to Nivel)
-Diploma Superior En Criminalistica (4to Nivel)

1.- Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?

En la práctica diaria recibo, sobre todo, tres modalidades: la apropiación fraudulenta por medios electrónicos contra cuentas, fraude en Marketplace o redes sociales (venta de artículos inexistentes y clonación de perfiles y fraude del CEO, donde se suplanta al gerente para desviar fondos de la empresa. Estos tres esquemas representan más del 90 % de las causas que llegan a etapa de juicio, según el consolidado estadístico 2024 de la Fiscalía, pero normalmente terminan fundamentando la acusación por la estafa.

2.- ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

El tipo de estafa del artículo 186 resulta insuficiente para las modalidades digitales porque exige que la víctima disponga voluntariamente de su patrimonio, mientras que el estafador moderno suele manipular un sistema (cajero, banca móvil). Por ello termino recalificando al artículo 190 en la decisión o, a veces, ratificando el

estado de inocencia por atipicidad cuando la acusación se basó sólo en el 186. Coincido con la doctrina que propone un artículo autónomo de estafa informática y cripto-fraudes, al estilo del art. 248.2 del Código Penal español.

3.- ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?

Normalmente los obstáculos suelen surgir por los peritajes incompletos, ya que solamente hay en el país únicamente dos laboratorios policiales acreditados con la ISO 17025; ello provoca nulidades por cadena de custodia defectuosa, y la mayoría de los abogados defensores la desconoce, y ni siquiera la alega. Así mismo hay errores de tipicidad o de subsunción por parte de la fiscalía, como por ejemplo en acusaciones por estafa (186) pese a evidencia de manipulación (190), lo que obliga a retrotraer la causa y dilata el proceso.

Demoras en rogatorias: las solicitudes de registros a plataformas extranjeras tardan 8-10 meses, muy por encima del estándar de Budapest.

4.- ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?

La normativa cubre el núcleo básico, y sí, se podrían sancionar a estafadores de redes sociales en sus varias modalidades, pero actualmente nuestro COIP carece de agravantes para deepfakes y sextorsión, y suele llegar al tribunal hasta por extorsión. Además, tengo entendido que la Ley de Inteligencia 2025, que recién se ha aprobado al permitir interceptaciones sin control judicial, corre el riesgo de que evidencia se declare ilícita, afectando una posible sanción.

5.- ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?

La cooperación internacional frente a los delitos informáticos es sumamente Imprescindible, debido a que este tipo de situaciones se viven en toda la región, y la mayoría de estos delitos se hacen con números de celulares, mexicanos, peruanos,

venezolanos etc., y me informaba un agente de la Policía Judicial que recién desde el año pasa, en criminalística hay un departamento llamado Punto de Contacto 24/7, el mismo que les permite congelar registros en menos de dos horas; y preguntar a otros países sobre información o datos del suyo, entonces por lo que veo es que sin ese mecanismo es imposible seguir el rastro de cuentas en plataformas que estén fuera de nuestro país. Sin embargo, la efectividad depende de que tipifiquemos las mismas conductas, de lo contrario no procede la asistencia simplificada.

6.- ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?

Los documentos más sólidos son los que enlazan tres cosas: origen del mensaje, identidad del titular de la cuenta y movimiento de fondos. Por eso valoro: (1) trazas de IP certificadas por el proveedor; (2) capturas forenses de conversaciones donde se pide el dinero; y (3) respaldo bancario que muestre la transferencia. Cuando esos tres elementos concuerdan, la prueba es contundente.

7.- Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador

En primer lugar, el de tipificar un tipo penal autónomo para fraudes que tengan que ver con el mal manejo de la inteligencia artificial y su posterior uso en delitos como lo que ya hemos conversado.

Así mismo, a los delitos que ya existen, aumentarles cierto tipo de agravantes, como por ejemplo cuando la víctima sea adulto mayor o microempresa, más o menos como pasa en Brasil.

Podría ser que en las formulaciones de cargos por los arts. 190, 231 o 232 vaya acompañada de informe pericial mínimo, sellado bajo esta nueva norma EGSI-ISO 27037.

Así mismo acreditar al menos tres laboratorios adicionales ISO 17025(herramienta esencial para los laboratorios que desean demostrar su competencia técnica, generar resultados confiables y operar de manera consistente

y eficiente, dotarles de presupuesto para reducir la mora probatoria, ya que quedan cortos solamente el de Guayaquil y Quito.

Con estas adecuaciones el sistema penal podría responder con mayor celeridad y garantizar la protección efectiva del patrimonio y la confianza digital de los ciudadanos.

Análisis de la entrevista:

La entrevista al juez Germán Blum respalda la tesis al confirmar que las estafas digitales dominantes en las ventas ficticias en Marketplace, desvío de fondos empresariales y fraudes bancarios on-line acaban siendo acusadas como estafa tradicional (art. 186), aun cuando encajan mejor en apropiación fraudulenta por medios electrónicos (art. 190). Esto genera dilaciones y, a veces, sobreseimientos por atipicidad. El magistrado advierte que solo hay dos laboratorios ISO 17025, y que, si las perecías no se de ahí, provocan nulidades por cadena de custodia y que las rogatorias a plataformas extranjeras demoran hasta diez meses, lo que debilita la prueba. Sostiene que el COIP necesita un tipo penal autónomo para estafa informática, agravantes cuando la víctima sea adulto mayor y reglas claras de evidencia digital; además, urge ampliar la cooperación 24/7 y certificar más laboratorios forenses. Así, el testimonio refuerza la conclusión central: sin reformas de tipificación, protocolo probatorio y coordinación internacional, la impunidad seguirá alta en los ciberdelitos.

Entrevistado No. 4

Mgtr. Walter Romero Jaén.

Perfil del Entrevistado: Es Abogado desde hace 19 años. Ha ejercido la rama penal desde que era abogado en el libre ejercicio de su profesión y actualmente es Fiscal de lo Penal en la Provincia del Guayas.

Títulos de 4to nivel :

-Mgtr en Derecho Penal Mención En Derecho Procesal Penal . (4to Nivel)

1.- Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?

Lo que más nos llega en la fiscalía de patrimonio ciudadano y de soluciones rápidas son las estafas y sus diferentes modalidades, como por ejemplo las estafas bancarias por correo o mensaje: la gente recibe un aviso falso que dice 'su cuenta será bloqueada' y, al entrar al enlace, le roban usuario y contraseña. También hay muchos casos de ventas fantasma en Facebook Marketplace; el comprador paga un adelanto y nunca ve el producto. Y, por último, ese truco de WhatsApp donde alguien se hace pasar por un pariente y pide dinero 'para una emergencia.

2.- ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

A mi criterio, el artículo 186 tal y como está redactado se queda corto para los fraudes en línea. El tipo exige que la víctima disponga voluntariamente de su patrimonio tras un engaño, pero hoy la maniobra incluye suplantación de plataformas, uso de bots, malware y hasta algoritmos que desvían el dinero sin que la persona siquiera pulse 'aceptar'. Cuando tengo que imputar, termino usando el 190 (apropiación fraudulenta por medios electrónicos) o combinando figuras, lo que complica la acusación y la prueba. Necesitamos una descripción específica de 'estafa digital' que reconozca el uso de medios electrónicos, agrave la pena cuando interviene inteligencia artificial o deepfakes y contemple a las víctimas vulnerables como adultos mayores.

3.- ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?

El mayor obstáculo es la obtención rápida de evidencias electrónicas: los registros de WhatsApp o de plataformas extranjeras tardan meses en llegar, y muchas veces las empresas los entregan incompletos o en formatos que no cumplen la cadena de custodia. Además, contamos con pocos laboratorios acreditados ISO 17025; si el peritaje se invalida, el caso se cae. Finalmente, existe confusión entre estafa clásica y apropiación electrónica, lo que nos obliga a reajustar la calificación a mitad del proceso y genera dilaciones.

4.- ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?

En teoría, el COIP nos da herramientas os artículos 186, 190 y 232 cubren la mayoría de los fraudes en redes; en la práctica, faltan definiciones claras para deepfakes y cripto-estafas. Con las figuras actuales puedo acusar, pero a veces el juez duda si el caso puede ser llamado a juicio o no, y eso debilita al sistema judicial.

5.- ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?

Debe ser una cooperación rápida y directa. Necesitamos canales 24/7 con las grandes plataformas para congelar registros y cuentas tan pronto se detecta la estafa; de nada sirve que Facebook entregue la información después de seis meses, cuando ya borraron las evidencias o el dinero dio la vuelta al mundo.

6.- ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?

Lo primero es conseguir los registros del banco o de la plataforma que muestran la ruta del dinero y como se obtuvo y observar a nombre de quien está; ese rastro financiero es difícil de refutar. Luego vienen los chats o correos completos, extraídos con perito y con su respectiva cadena de custodia para probar que nadie los alteró. Finalmente, los logs (registros técnicos) de la IP o del dispositivo del acusado.

7.- Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador

Lo primero sería crear un tipo penal específico de ‘estafa digital’ que mencione expresamente el uso de perfiles falsos, inteligencia artificial etc; hoy esos casos se terminan forzando dentro del artículo 186 o 190. También urge una reforma procesal que establezca plazos máximos para que bancos y plataformas entreguen registros.

Análisis de la entrevista:

La entrevista al fiscal Walter Romero respalda la tesis al confirmar que las estafas vía mensajes bancarios falsos, ventas fantasmas en Marketplace y suplantaciones en WhatsApp dominan las denuncias, pero el artículo 186 resulta estrecho frente a maniobras que combinan bots, malware y deepfakes. El fiscal reconoce que termina formulando cargos con el artículo 190 o mezclando figuras, lo que complica la prueba y alimenta la impunidad. Su solución coincide con la propuesta de la tesis: crear un tipo penal específico de estafa digital o definir mejor los conceptos para que no haya errores de subsunción, fijar plazos perentorios para la entrega de datos y establecer un canal 24/7 con proveedores globales.

Entrevistado No. 5

Mgtr. Francisco Cáceres Villacís, Esp.

Perfil del Entrevistado: Es Abogado desde hace 6 años, ha ejercicido la rama penal desde sus inicios como profesional, ademas se ha desempeñado como docente de PreGrado en la Universidad Laica Vicente Rocafuerte de Guyaquil y PosGrado en la Universidad UTEG. Actualmente es abogado litigante en la materia.

Títulos de 4to nivel :

-Mgtr en Derecho En Derecho Procesal. (4to Nivel)

-Especialista En Garantias Jurisdiccionales Y Reparacion Integral(4to Nivel)

1.- Desde su experiencia, ¿cuáles son los tipos de estafa digital más comunes que llegan a los despachos judiciales o fiscales?

Cada semana recibo personas buscando asesorías para denuncias, ya que son personas que caen en supuestas ofertas laborales por Instagram: les piden una ‘pequeña cuota de inscripción’ o les envían un enlace para rellenar datos bancarios y allí pierden su dinero. También son frecuentes los sorteos falsos en Facebook donde, para ‘reclamar el premio’, la víctima paga un dinero de enganche o comparte información de su tarjeta. Últimamente han crecido los casos de mensajes que prometen duplicar inversiones en criptomonedas; la gente deposita confiada y, cuando quiere retirar, la página desaparece sin dejar rastro.; así mismo las denuncian

en su mayoría entran por el delito de estafa y apropiación fraudulenta por medios electrónicos.

2.- ¿Considera que la tipificación actual de la estafa (Art. 186 COIP) es suficiente para abarcar las modalidades digitales o se requieren reformas específicas sobre la descripción del tipo penal?

En mi práctica con clientes particulares veo que el artículo 186 se queda corto. Es cierto que castiga el engaño, pero ignora elementos hoy básicos: suplantación de identidad digital, clonación de páginas y uso de pasarelas falsas. Cada vez que litigo, debo convencer al juez de que ese 'clic' engañado equivale a la disposición voluntaria exigida por la norma, y muchas defensas se escudan en que la víctima 'entró por su cuenta'. Propongo añadir un párrafo que considere estafa digital cuando el fraude se ejecuta a través de correos, redes sociales o mensajería, y que eleve la pena si hay robo de datos sensibles o uso de perfiles clonados

3.- ¿Qué obstáculos procesales o probatorios suelen surgir en la investigación de delitos informáticos y estafas digitales?

El primer problema es que los bancos y las compañías celulares que tenemos en el país, tardan mucho en entregar los registros que prueban la inteligencia social usada para el delito de estafa; cuando llegan, a veces el juez de oficio ya cierra la etapa de instrucción y no fue anunciada en la etapa de evaluación y preparatoria de juicio o a veces llega la etapa de juicio y aun no llega la pericia y se dilata el proceso. También falta personal capacitado: he visto informes que solo traen capturas de pantalla sin explicar de dónde salió el dinero ni quién lo movió y ni a que cuenta fue a parar.

4.- ¿Cree que la actual legislación ecuatoriana permite una correcta imputación y sanción de los responsables de estafas en redes sociales y mensajería instantánea?

Hoy sí se puede procesar a un estafador de WhatsApp o Facebook, pero el proceso es lento y se complica si el servidor está fuera del país. Haría falta un artículo específico de 'estafa digital' que agilite la cooperación internacional y suba la pena cuando se usan perfiles clonados

5.- ¿Qué rol debería tener la cooperación internacional frente a los delitos informáticos cometidos desde plataformas extranjeras, especialmente en lo referente al acceso a información digital?

Hace falta que los tratados y convenios internacionales remitan la información necesaria, en horas y no en meses, los datos de la cuenta de un estafador en otro país. Hoy la víctima debe esperar, y mientras tanto el dinero desaparece. Un protocolo ágil protege mejor a quienes fueron engañados por alguna red virtual o electrónica.

6.- ¿Qué elementos probatorios considera más eficaces para sustentar la acusación en delitos de estafa digital?

Las pruebas clave son los registros técnicos (por ejemplo, la dirección IP o el dispositivo usado) y la historia de la transacción en el banco. Si además hay videos de cámaras o audios de la llamada donde piden el depósito o de dónde saca el dinero, el caso queda muy bien armado y va a prosperar.

7.- Desde su perspectiva, ¿qué reformas legales o procesales serían prioritarias para combatir la impunidad en los delitos informáticos en Ecuador

En lo procesal, reforzaría la capacitación de fiscales y peritos y acreditaría más laboratorios ISO 17025; sin informes técnicos sólidos, cualquier reforma legal se queda en el papel.

Análisis de la entrevista:

La entrevista al abogado Francisco Cáceres refuerza la tesis al confirmar que las estafas digitales, ofertas laborales falsas en Instagram, sorteos fantasma en Facebook y criptoinversiones son hoy habituales y se encuadran de inicio en el artículo 186 (Estafa), pese a implicar suplantación y páginas clonadas. Señala que el tipo penal actual obliga a persuadir al juez de que un clic equivale a disposición voluntaria, lo que genera defensas exitosas y alimenta la impunidad; respalda, por tanto, la creación de un artículo específico de estafa digital con agravantes por perfiles clonados o robo de datos sensibles. Subraya los mismos obstáculos detectados por la investigación: demora de bancos y operadoras en entregar registros, peritajes limitados a simples capturas de pantalla y falta de laboratorios y peritos certificados.

Considera indispensable agilizar la cooperación internacional (respuestas en horas y no en meses) y acredita que los elementos más sólidos son trazas de IP, ruta bancaria del dinero y, de ser posible, videos o audios que muestren el retiro de fondos.

Entrevistado No. 6

Lcdo. Alex Cáceres Villacís, Esp.

Perfil del Entrevistado: Es Licenciado en Fisioterapia y actualmente fue victima de un delito informatico el cual ha quedado en la impugnidad.

Contenido de la entrevista:

Pregunta 1. ¿Cómo empezó todo?

El 24 de junio de 2025 dejé mi carro estacionado en el centro de Guayaquil; cuando regresé, lo habían forzado. Se llevaron la computadora del vehículo y mi billetera, donde estaba la tarjeta de crédito del Banco Internacional. Dos días después descubrí un consumo no autorizado por USD 304,43 a nombre de Neteller apropiacion fraudulenta por medios electronicos.

Pregunta 2. ¿El banco le alertó a tiempo de la transacción?

Solo me llegó un SMS anunciando el cobro; no recibí ningún correo pese a que esa es la práctica habitual del banco. Me pareció extraño, porque el protocolo 3-D Secure exige doble notificación apropiacion fraudulenta….

Pregunta 3. ¿Qué hizo inmediatamente después?

Bloqueé la tarjeta, pedí el reverso y presenté un reclamo ante la Defensoría del Cliente. El banco respondió que la compra se había hecho con todos mis datos personales y que, por tanto, la operación era válida. En otras palabras, me dejaron la responsabilidad a mí.

Pregunta 4. ¿Se inició alguna acción penal?

Sí. Con mi abogado presentamos una denuncia por apropiación fraudulenta por medios electrónicos (art. 190 COIP); solicitamos que el fiscal oficie al banco para

entregar los movimientos y que un perito certifique que nunca fui notificado por correo apropiacion fraudulenta.

Pregunta 5. ¿Qué obstáculos ha encontrado?

Primero, el banco tardó semanas en remitir los logs y, cuando lo hizo, mandó simples hojas de cálculo sin metadatos ni encabezados. Segundo, la Defensoría rechazó la audiencia de conciliación alegando que no había falla del banco, así que el dinero sigue perdido mientras el proceso penal avanza a ritmo lento.

Pregunta 6. ¿Cómo le ha afectado esta situación?

Además de la pérdida económica, siento desprotección: el banco se ampara en que usaron mi tarjeta con mis datos, y la investigación penal se enreda entre si es estafa, robo o apropiación electrónica. Uno termina revictimizándose al reclamar.

Pregunta 7. ¿Qué espera del sistema de justicia?

Que se determine cómo obtuvieron mis datos, se obligue al banco a reponer el monto y se sancione a los responsables. Sobre todo, que este caso sirva para que las instituciones financieras mejoren sus protocolos y la Fiscalía actúe con mayor celeridad cuando se trata de fraudes digitales.

CONCLUSIONES

La mala aplicación de los tipos penales en casos de engaños digitales sobre todo la confusión entre estafa tradicional (art. 186) y apropiación fraudulenta por medios electrónicos (art. 190), retrasa los procesos, provoca reformulaciones y termina elevando la impunidad, se logró fundamentar jurídicamente el problema con doctrina y derecho comparado, mostrando que el ordenamientos como el español ya cuentan con una figura específica de estafa informática, ausente en el COIP, también se caracterizaron las modalidades dominantes en 2020 hasta el 2025 las ventas falsas en Marketplace, suplantaciones por WhatsApp, ofertas laborales engañosas, criptoinversiones, evidenciando por qué encajan mal en el art. 186, finalmente se identificaron las fallas probatorias que debilitan la acusación peritajes sin estándares, pocos laboratorios acreditados y demoras prolongadas para obtener registros de plataformas.

Los hallazgos muestran efectos concretos en la realidad ecuatoriana: revictimización las personas no recuperan su dinero a tiempo, desconfianza en el sistema y subregistro de denuncias, el daño recae con mayor fuerza en adultos mayores y pequeños negocios, blancos frecuentes de suplantaciones y ventas inexistentes, a nivel institucional persiste una respuesta fragmentada entre bancos, defensoría del cliente y fiscalía, sumada a brechas territoriales, los recursos forenses se concentran en pocas ciudades, lo que aumenta archivos por falta de prueba técnica, en conjunto la calificación jurídica incorrecta y la debilidad de la evidencia erosionan la tutela judicial efectiva.

La propuesta es clara y aplicable es crear una figura penal de estafa digital que describa el fraude en redes y mensajería, con agravantes cuando se use IA y deepfakes o cuando la víctima sea vulnerable o se afecten servicios esenciales, el ordenar la evidencia electrónica con reglas de captura, preservación y presentación, además de exigir un peritaje mínimo desde la formulación de cargos por delitos informáticos.

El fortalecer la capacidad pericial acreditando más laboratorios y profesionalizando a peritos, fiscales y jueces, el acelerar la cooperación con

plataformas mediante un canal 24 horas los 7 días a la semana, plazos perentorios y representación local para la entrega de datos, se debería medir los resultados con un observatorio que publique indicadores semestrales sobre denuncias, sobreseimientos y sentencias.

En definitiva, los resultados confirman que la impunidad en los engaños digitales no es un destino, sino la consecuencia directa de una ley mal aplicada y de una prueba mal tratada, alinear tipificación, evidencia y coordinación institucional es viable y urgente si el sistema adopta las medidas propuestas, la respuesta penal será oportuna, las víctimas serán reparadas con mayor celeridad y la confianza ciudadana en la justicia digital empezará a recuperarse.

RECOMENDACIONES

Para cerrar esos vacíos y dar eficacia real a la persecución penal se proponen, en primer término, introducir un tipo penal autónomo de estafa digital que describa expresamente fraudes ejecutados por redes, deepfakes etc, y que prevea agravantes cuando la víctima sea adulto mayor o cuando el ataque afecte servicios esenciales.

En segundo lugar, es imprescindible un capítulo procesal sobre evidencia electrónica que adopte las normas ISO 27037-27042 y exija que toda acusación basada en los arts. 190, 231 o 232 se acompañe de un peritaje mínimo con certificado digitales certeros y legitimos; esta medida responde al objetivo de evaluar la aplicación de los tipos penales.

Tercero, deben acreditarse al menos tres laboratorios ISO 17025 adicionales y financiar la formación continua de peritos, pues sin informes técnicos válidos cualquier reforma legal queda inerte.

Cuarto, se recomienda obligar a las plataformas con más de 100 000 usuarios en el país a designar un representante legal local y a entregar registros en un máximo de diez días (o 48 horas en flagrancia) mediante el Punto de Contacto 24/7; ello agilizará la cooperación internacional.

Quinto, se propone capacitar de modo obligatorio a fiscales y jueces en distinciones entre estafa tradicional y electrónica, trazado de cripto-activos y valoración de deepfakes, para evitar errores de subsunción y garantizar la protección efectiva de las víctimas.

Finalmente, la creación de un observatorio nacional de ciberdelito que publique indicadores semestrales permitirá medir el impacto de estas reformas y ajustar las políticas públicas.

REFERENCIAS BIBLIOGRÁFICAS

Alicio. (6 de SEPTIEMBRE de 2021). *alicebiometrics*. Recuperado el 01 de 07 de 2025, de https://alicebiometrics.com/entendiendo-el-ciberfraude/?utm_source

Analytic exchange program . (Octubre de 2024). *Impact of artificial intelligence* . Obtenido de Criminal and illicit actiuties: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf

Arcotel. (2025). *Protocolo de seguridad para evitar la suplantación de identidad*. Recuperado el 01 de 07 de 2025, de Agencia de Regulación y Control de las Telecomunicaciones: https://www.arcotel.gob.ec/protocolo-de-seguridad-para-evitar-la-suplantacion-de-identidad/?utm_source

Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito, Ecuador: Asamblea Nacional. Recuperado el 01 de 07 de 2025

Asamblea Nacional del Ecuador. (2024). *Proyecto de Ley Orgánica de Seguridad Digital*. Recuperado el 21 de Julio de 2025, de https://asobanca.org.ec/wp-content/uploads/2021/10/Proyecto-de-Ley-Organica-de-Seguridad-Digital-Ciberseguridad-Ciberdefensa-y-Ciberinteligencia.pdf

Banco, S. d. (18 de enero de 2024). *Asobanca*. Obtenido de https://asobanca.org.ec/wp-content/uploads/2024/01/Circular-No.-SB-IG-2024-0003-C%E2%80%93-Comunicacion-al-ente-de-control-sobre-ventanas-de-mantenimiento-programadas-e-incidentes.pdf?

Boe. (s.f.). *Agencia estatal boletin oficial del estado de España*. Recuperado el 01 de 07 de 2025, de https://www.boe.es/

Bonilla. (2025). *Universidad Técnica del Norte*. Obtenido de Los delitos de estafa y apropiación fraudulenta por redes sociales ocurridos en la cuidad de cayabe año 2022- 2023: https://repositorio.utn.edu.ec/bitstream/123456789/17066/2/02%20DER%20169%20TRABAJO%20DE%20GRADO.pdf?

Cárdenas Verdesoto, E. (12 de Mayo de 2025). *Las estafas digitales crecen, pero sí es posible evitarlas*. Obtenido de https://ecuadorchequea.com/las-estafas-digitales-crecen-pero-si-es-posible-evitarlas/

Carrillo, P. (28 de Marzo de 2024). */revistagestion.primicias.ec*. Obtenido de https://revistagestion.primicias.ec/analisis-sociedad/la-violencia-sexual-en-internet-otra-deuda-de-la-justicia-ecuatoriana/

Cherry, K. (17 de 09 de 2024). *verywellmind*. Recuperado el 05 de 07 de 2025, de https://www.verywellmind.com/why-we-fall-for-scams-8705528?utm_source

CNT. (2025). *CNT*. Recuperado el 05 de 07 de 2025, de https://csirt-cnt.gob.ec/index.php/es/?utm_source

COIP. (17 de Febrero de 2014). *Codigo Organico Integral Penal*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

COIP. (17 de Febrero de 2021). *Codigo Organico Integral Penal*. Obtenido de Lexis Finder: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Comisión Especializada Permanente de Soberanía, I. y. (2023). *https://observatoriolegislativo.ec/wp-content/uploads/2024/06/INFORME-PARA-PRIMER-DEBATE.pdf?* Obtenido de https://https://observatoriolegislativo.ec/wp-content/uploads/2024/06/INFORME-PARA-PRIMER-DEBATE.pdf?/wp-content/uploads/2024/06/INFORME-PARA-PRIMER-DEBATE.pdf?

Connolly et al. (23 de enero de 2025). *discovery.ucl.ac.uk*. (discovery.ucl.ac.uk, Editor) Recuperado el 02 de 07 de 2025, de discovery.ucl.ac.uk: https://discovery.ucl.ac.uk/id/eprint/10207993/3/Borrion_connolly-et-al-2025-ransomware-crime-through-the-lens-of-neutralisation-theory.pdf?utm_source

Consejo de Europa. (12 de Diciembre de 2024). *Convenio sobre Delito Cibernético: Ecuador se convierte en la 77ª Parte y Perú firma el Segundo Protocolo sobre pruebas electrónicas*. Obtenido de Cibercrimen: https://www.coe.int/en/web/cybercrime/-/convention-on-cybercrime-ecuador-becomes-the-77th-party-and-peru-signs-the-second-protocol-on-electronic-evidence

Constitución de la república del Ecuador. (20 de Octubre de 2008). *Asamblea nacional republica del Ecuador* . Obtenido de Registro Oficial Suplemento 449: https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Corporación forense digital . (28 de Abril de 2025). *La Matanza Silenciosa: Desenmascarando la Estafa de Criptomonedas de la Carnicería de Cerdos*. Obtenido de Digitalforensics: https://www.digitalforensics.com/blog/extortion/pig-butchering-scam/?srsltid=AfmBOoquQ51xc4E-X631msB9xCWiqRr8FkfnsclIVSrOetMVMRZb1NAc&utm_source

Corte constitucional del Ecuador. (6 de julio de 2022). *Sentencia No. 200-20-EP/22* . Recuperado el 02 de 07 de 2025, de https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBl

dGE6J3RyYW1pdGUnLCB1dWlkOic2MzA1MjhiMS0xZjJlLTQ0MjAtOTEwNC0wYTk0NTA3ZjUwYWMucGRmJ30%3D

Corte nacional de justicia . (15 de Junio de 2025). *Desafios del proceso penal en la actualidad* . Obtenido de https://www.cortenacional.gob.ec/cnj/images/RevistasPenales/rpenal15.pdf?utm_source

Corte nacional de justicia del Ecuador. (2018). *Abuso de confianza*. Recuperado el 7 de Julio de 2025, de https://cortenacional.gob.ec/cnj/images/Diccionario/Vocabulario/A/Abuso-de-confianza.pdf?utm_source

Crespo, H. F. (30 de Junio de 2021). *Universidad central del Ecuador*. Obtenido de Derecho penal central : https://revistadigital.uce.edu.ec/index.php/derechopenal/article/download/3341/4121/17095?utm_source

Creswell, J. W. (2019). *https://academia.utp.edu.co/*. (https://academia.utp.edu.co/, Editor) Obtenido de https://academia.utp.edu.co/seminario-investigacion-II/files/2017/08/INVESTIGACION-CUALITATIVACreswell.pdf?

Departamento de seguridad nacional . (30 de Marzo de 2022). *Plan nacional de ciberseguridad*. Obtenido de https://www.dsn.gob.es/index.php/es/actualidad/sala-de-prensa/plan-nacional-ciberseguridad-0

Diario primicias Ecuador. (17 de Junio de 2021). *Fiscalía allanó sala de sorteos del consejo de la judicatura del Guayas*. Recuperado el 02 de 07 de 2025, de Primicias : https://www.primicias.ec/noticias/lo-ultimo/fiscalia-allano-casa-oficina-servidora-judicial-guayaquil/?utm_source

E-ciber . (5 de Febrero de 2020). *Estratégia nacional de seguranca cibernética* . Obtenido de https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf

Ecuador, C. C. (24 de 05 de 2023). *Corte Constitucional Ecuador*. Obtenido de https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOidiMGQ3MmM5Yy02M2I0LTQ1MDgtOGQwYi00M2Q0ZDI4Mzg2N2YucGRmJ30%3D

Ecuador, D. P. (27 de 07 de 2022). *revistagestion.primicias.ec*. Obtenido de https://revistagestion.primicias.ec/cifras/8-modelos-de-estafas-comunes-en-facebook-marketplace/?utm_source

Ecuador, P. N. (2024). *noticias.policia.gob.ec*. Recuperado el 02 de 07 de 2025, de https://noticias.policia.gob.ec/policia-desarticula-red-internacional-de-ciberdelincuentes-en-ecuador

El comercio. (25 de Julio de 2022). *3.183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. Obtenido de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020/

Estrategia nacional de ciberseguridad. (2017). Recuperado el 19 de Julio de 2025, de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

European Union. (2022). *Ciberseguridad de redes y sistemas de información*. Recuperado el 02 de 07 de 2025, de Acceso al Derecho de la Unión Europea: https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-network-and-information-systems.html?utm_source

Europeo, C. (12 de 12 de 2024). *://www.coe.int*. Recuperado el 05 de 07 de 2025, de https://www.coe.int/en/web/cybercrime/-/convention-on-cybercrime-ecuador-becomes-the-77th-party-and-peru-signs-the-second-protocol-on-electronic-evidence?

Europol. (2022). *Europol*. Obtenido de https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf?utm_source

Factor trabajo. (01 de Mayo de 2022). *Impacto del COVID-19 en el mercado laboral: ¿Qué ha pasado desde la crisis económica, y qué sigue?* Obtenido de https://blogs.iadb.org/trabajo/es/el-mercado-laboral-desde-el-covid-19/

FBI US. (13 de Junio de 2025). *Boston*. Obtenido de https://www.fbi.gov/contact-us/field-offices/boston/news/fbi-highlights-growing-number-of-reported-elder-fraud-cases-ahead-of-world-elder-abuse-awareness-day?utm_source

Fiscalía general del estado. (03 de Marzo de 2023). *Fiscalía obtiene sentencia por los delitos de acceso no consentido a un sistema informático, telemático o de telecomunicaciones y revelación ilegal de base de datos*. 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/

Forenses, s. n. (2023). *cienciasforenses.gob.ec*. Recuperado el 05 de 07 de 2025, de https://www.cienciasforenses.gob.ec/wp-content/uploads/2024/03/Informe-preliminar-de-Rendicio%CC%81n-de-Cuentas-2023-SNMLCF.pdf

Freitas, N. (2024). *biocatch*. Recuperado el 05 de 07 de 2025, de https://www.biocatch.com/es/blog/abordar-el-impacto-emocional-del-fraude-financiero

Galán, C. M., & Cordero, C. G. (6 de 7 de 2016). *Repositorio pucp*. Recuperado el 2025, de https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/download/18892/19110

Generando. (30 de Junio de 2023). *Delitos informáticos en Ecuador: Estafas en redes sociales* . Obtenido de Revista G-NER@NDO: https://revista.gnerando.org/revista/index.php/RCMG/article/view/82

Gobierno, M. d. (2019). *www.ministeriodegobierno.gob.ec*. Recuperado el 05 de 07 de 2025, de https://www.ministeriodegobierno.gob.ec/ecuador-y-espana-afianzan-acuerdos-de-cooperacion-en-seguridad/?

Harán, J. M. (14 de octubre de 2021). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Hernández et al. (2014). *https://www.esup.edu.pe/*. Obtenido de https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez%2C%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Hux, L. J. (2024). *scribd*. Obtenido de https://es.scribd.com/document/413290223/Tratamiento-de-La-Evidencia-Digital-Segun-ISO-27037?utm_source

Ian. (2002). *https://opus.lib.uts.edu.au*. Obtenido de https://opus.lib.uts.edu.au/rest/bitstreams/931e14b1-ffb9-4e75-a4d0-874f82ab364e/retrieve?

Ibm. (20 de enero de 2022). *¿Qué es la ciberresiliencia?* Recuperado el 01 de 07 de 2025, de https://www.ibm.com/think/topics/cyber-resilience?utm_source

Incibe. (5 de Agosto de 2020). *Instituto Nacional de Ciberseguridad* . Obtenido de https://www.incibe.es/aprendeciberseguridad/vishing?utm_source

Instituto nacional de estadistica y censos . (2024). *ecuadorencifras.gob.ec*. Obtenido de https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/?utm_source

International telecommunication Union. (2020). *Global cybersecurity Index*. Recuperado el 18 de Julio de 2025, de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Internet crime complaint. (2024). *Federal bureau of investigation internet crime report*. Recuperado el 05 de 07 de 2025, de https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf?utm_source

Interpol. (2025). *Interpol*. Recuperado el 05 de 07 de 2025, de https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres?utm_source

Interpol.int. (Agosto de 2020). *Cybercrime: Covid 19 Impact*. Recuperado el 02 de 07 de 2025, de https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf?utm_source

Justice, U. D. (2025). *.ic3.gov*. Obtenido de www.ic3.gov/: https://www.ic3.gov/Outreach/Brochures/elder_fraud_tri-fold.pdf?utm_source

Karuppannan, J. (Enero de 2008). *Teoría de la transición espacial de los delitos cibernéticos*. Recuperado el 02 de 07 de 2025, de researchgate.net : https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes?utm_source

kaspersky. (04 de 11 de 2024). *latam.kaspersky*. Recuperado el 02 de 07 de 2025, de https://latam.kaspersky.com/about/press-releases/america-latina-enfrenta-mas-de-31-millones-de-ataques-de-malware-por-dia-alerta-kaspersky?srsltid=AfmBOoqQ0etv_PwpGm-_RPskxqa2bZvnfs_42OUbWKfzgWH12tuUgRZb&utm_source

Katherine, C. C. (2022). *Análisis dogmático penal de los delitos de apropiación fraudulenta y estafa cuando son realizados por medios electrónicos en el COIP*. Recuperado el 10 de Julio de 2025, de dspace.uce.edu.ec: https://www.dspace.uce.edu.ec/server/api/core/bitstreams/a40ea4f7-91fa-4613-b270-62ef825c001c/content?utm_source

Kianpour et al. (3 de Diciembre de 2021). *Comprender sistemáticamente la economía de la ciberseguridad: una encuesta*. (Mdpi, Productor) Recuperado el 02 de 07 de 2025, de https://www.mdpi.com/2071-1050/13/24/13677

klepper. (1 de 06 de 2024). *apnews.com/*. Recuperado el 02 de 07 de 2025, de https://apnews.com/article/mexico-election-sheinbaum-facebook-lopez-obrador-79adddaf8300f30af51fddbbf3165216

knowbe4. (2024). *knowbe4*. Recuperado el 02 de 07 de 2025, de https://www.knowbe4.com/ceo-fraud?utm_source

León, M. T. (Noviembre de 2023). *Universidad de otavalo*. Recuperado el 02 de 07 de 2025, de

https://repositorio.uotavalo.edu.ec/server/api/core/bitstreams/70ec8a14-9a9b-45e3-89e2-a83780bb2ff8/content

Lexis noticias . (11 de Junio de 2025). *Registro Oficial del día: Ley Orgánica de Inteligencia*. Obtenido de https://www.lexis.com.ec/noticias/registro-oficial-del-dia-ley-organica-de-inteligencia

Lisa Institute. (2024). *Deepfakes: Qué es, tipos, riesgos y amenazas*. Recuperado el 10 de Julio de 2025, de https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas?srsltid=AfmBOopPFiyMT4_WYAisciJtpdyNN6VKkjGCReo9iJNDUFsOuVPDCVbM&utm_source

López et al. (30 de mayo de 2025). *www.nature.com*. Recuperado el 05 de 07 de 2025, de https://www.nature.com/articles/s41599-025-05100-7?utm_source

Mark, C. (24 de 4 de 2024). *levelblue*. Obtenido de https://levelblue.com/blogs/security-essentials/understanding-how-rationality-deterrence-theory-and-indeterminism-influence-cybercrime

Mera. (Junio de 2019). *dspace.uce.edu.ec*. Obtenido de https://www.dspace.uce.edu.ec/server/api/core/bitstreams/1eabcf84-3170-47b0-91be-5ec35de767dc/content

Mera. (03 de julio de 2025). *Ciberdelincuencia avanza en Ecuador y la justicia no logra alcanzarla: ¿Hay solución?* (D. Expreso, Editor) Recuperado el 06 de 07 de 2025, de https://www.expreso.ec/actualidad/ciberdelincuencia-avanza-ecuador-justicia-no-logra-alcanzarla-solucion-248549.html

Ministerio de telecomunicaciones y de la sociedad de la informacion. (2021). *Politica de ciberseguridad*. Recuperado el 18 de Julio de 2025, de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Morales et al. (13 de mayo de 2025). *investigarmqr*. Recuperado el 05 de 07 de 2025, de https://www.https://www.investigarmqr.com/2025/index.php/mqr/article/view/565?utm_source

Morales, P. A., & Ramírez, A. L. (13 de Marzo de 2025). *investigarmqr*. Recuperado el 05 de 07 de 2025, de https://www.investigarmqr.com/2025/index.php/mqr/article/view/565?utm_source

Naciones, O. a. (30 de 09 de 2024). *www.oas.org*. Obtenido de https://www.oas.org/ext/en/main/calendar/event/id/481

OCU. Organización de consumidores y usurios . (1 de Abril de 2025). *Phishing: cómo evitarlo y prevenirlo*. Obtenido de https://www.ocu.org/tecnologia/ciberseguridad/consejos/evitar-ataque-phishing

Olivares, K. A. (5 de Noviembre de 2024). *Revista de Investigacion en ciencias juridicas* . Obtenido de https://revistalex.org/index.php/revistalex/issue/view/27?

Ortega et al. (04 de Enero de 2025). *Delitos cibernéticos y su tratamiento en la jurisdicción ecuatoriana.* Obtenido de Revista Sociedad & Tecnología, 8(S1), 249–261.: https://institutojubones.edu.ec/ojs/index.php/societec/article/view/582

Pablos, S. P. (01 de Febrero de 2025). *huffingtonpost*. Recuperado el 01 de 07 de 2025, de https://www.huffingtonpost.es/sociedad/naciones-unidas-alerta-estafas-nombre-advierte-onu-nunca-pide-datos-personales.html?utm_source

Peralta, S. (20 de 06 de 2025). *genexusconsulting*. Obtenido de https://www.genexusconsulting.com/insights/ciberataques-america-latina/?utm_source

Practical guide for CSIRTs. (2023). *A sustainable business model*. (www.oas.org, Productor) Obtenido de https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20Digital%20ENG.pdf?utm_source

Primicias. (8 de Septiembre de 2024). *La crisis de seguridad no se ha ido y ya golpea a la economía*. Recuperado el 20 de Julio de 2025, de https://revistagestion.primicias.ec/analisis-economia-y-finanzas/la-crisis-de-seguridad-no-se-ha-ido-y-ya-golpea-la-economia/

Primicias diario Ecuador . (28 de Julio de 2024). *Registro Civil denuncia a cuentas digitales que ofrecen turnos falsos*. Obtenido de https://www.primicias.ec/noticias/sociedad/registro-civil-denuncia-paginas-digitales-turnos/?utm_source

Primicias, D. (11 de 07 de 2023). *primicias.ec*. Recuperado el 02 de 07 de 2025, de https://www.primicias.ec/noticias/sociedad/registro-civil-denuncia-paginas-digitales-turnos/?utm_source

Proaño, P. (30 de abril de 2025). *equinocciodigital*. Recuperado el 05 de 07 de 2025, de https://equinocciodigital.com/conectividad-rural-ecuador-brecha-digital-2025/?utm_source

Proofpoint. (s.f.). *¿Que es el phishing?* Recuperado el 27 de Julio de 2025, de https://www.proofpoint.com/es/threat-reference/phishing

Proofpoint. (2024). *Compromiso de correo electrónico empresarial (BEC)*. Recuperado el 02 de 07 de 2025, de https://www.proofpoint.com/us/threat-reference/business-email-compromise?utm_source

Proofpoint. (2025). *proofpoint*. (proofpoint, Editor) Recuperado el 01 de 07 de 2025, de https://www.proofpoint.com/es/threat-reference/phishing

Radnaeva, E., & Semenova, N. (JUNIO de 2025). *researchgate*. (R. r. criminología, Editor) Obtenido de https://www.researchgate.net/publication/393186577_Cognitive_Biases_Influencing_the_Behavior_of_Online_Fraud_Victims_and_Considering_Them_in_the_Development_of_Victimological_Prevention_Measures?utm_source

Raj, R., & Caeiro, D. (01 de 09 de 2024). *.jscholaronline*. Obtenido de https://www.jscholaronline.org/articles/JFRC/A-Review-on-the-Application-of-Lifestyle-Routine-Activity-Theory.pdf

Reglamento de la ley organica de proteccion de datos personales . (13 de Noviembre de 2023). *Lexis* . Obtenido de https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

Rendón et al. (s.f.). *DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR* . (E. S. Manabí, Editor) Recuperado el 7 de Julio de 2025, de www.espam.edu.ec: https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

Rodríguez. (2022). *Repositorio Universidad Estatal Peninsula de Santa Elena*. (R. U. Elena, Editor) Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/8820/1/UPSE-TDR-2022-0064.pdf

Rodríguez. (07 de 09 de 2024). *elpais.com*. Recuperado el 05 de 07 de 2025, de https://elpais.com/mexico/2024-09-08/la-sofisticacion-de-los-ciberataques-aumenta-el-secuestro-de-datos-y-redes-sociales-en-mexico.html?utm_source

Sabin, S., & Rubin, A. (25 de abril de 2025). *.axios.com*. Recuperado el 05 de 07 de 2025, de https://www.axios.com/2025/04/23/fbi-internet-crime-loss-record-high-2024?utm_source

Santos, C. (Junio de 2025). *Principales daños psiquicos en las victimas de estafadores amorosas en las redes sociales*. Obtenido de UNIVERSIDAD DE CIENCIAS EMPRESARIALES Y SOCIALES -UCES MAESTRÍA EN CIENCIAS- CRIMINOLÓGICO FORENSES:

https://dspace.uces.edu.ar/jspui/bitstream/123456789/7195/1/Principios_Santos-Soares.pdf?utm_source

Scielo . (26 de Junio de 2025). *Asociación Investigadores Venezolanos de la Comunicación*. Obtenido de https://ve.scielo.org/scielo.php?script=sci_serial&pid=2739-0063&lng=es

Smath. L. Sanon. (s.f.). *Las redes sociales y su impacto y evolución en la era digital*. Recuperado el 1 de Julio de 2025, de https://smathlsanon.com/las-redes-sociales-impacto-y-evolucion-en-la-era-digital/

Superintendencia de bancos . (21 de Octubre de 2021). *superbancos.gob.ec*. Obtenido de https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada/?utm_source

Tapia. (12 de 04 de 2025). *Primicias Ecuador*. Obtenido de https://www.primicias.ec/economia/estafa-robo-tarjeta-credito-compra-exterior-servicios-postales-93804/

Tapia, E. (15 de 06 de 2025). *Primicias Ecuador*. (P. Ecuador, Editor) Recuperado el 01 de 07 de 2025, de https://www.primicias.ec/economia/tarjetas-credito-delitos-informaticos-estafas-cuentas-bancos-98471/

Tecnologías de la información & la comunicación. (Abril de 2021). *ecuadorencifras.gob.ec*. Recuperado el 02 de 07 de 2025, de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf

Telecomunicaciones. (2024). *Ministerio de Ecuador*. Recuperado el 05 de 07 de 2025, de www.telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2024/04/Acuerdo-Nro.-MINTEL-MINTEL-2024-0003-Esquema-Gubernamental-Seguridad-de-la-Informacion-EGSI.pdf?

Telecomunicaciones, M. d. (2023). *observatorioecuadordigital*. Recuperado el 05 de 07 de 2025, de https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2024/09/CHEQUEO-DIGITAL.pdf

TrendTic. (21 de Noviembre de 2023). *Manipulación, extorsión y contenido sexual: el peligro alrededor del deepfake entre los jóvenes y cómo prevenirlos* . Obtenido de https://www.trendtic.cl/2023/11/manipulacion-extorsion-y-contenido-sexual-el-peligro-alrededor-del-deepfake-entre-los-jovenes-y-como-prevenirlos/?utm_source

United states secret service . (Enero de 2025). *Cryptocurrency scams - Pig butchering*. Obtenido de

https://www.secretservice.gov/sites/default/files/reports/2025-01/Public-Alerts-2025-Cryptocurrency-Scams-Pig-Butchering.pdf?utm_source

Universidad del internet . (15 de 2 de 2024). *Delitos Informáticos: Tipos, legislación y medidas de prevención*. Obtenido de Unir : https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

Universo, D. e. (03 de junio de 2025). *El Universo*. Obtenido de https://www.eluniverso.com/noticias/economia/estafa-entidades-financieras-no-autorizadas-superintendente-de-bancos-roberto-romero-von-buchwald-ecuador-2025-nota/

Wang et al. (ENERO de 2024). *sciencedirect*. Recuperado el 02 de 07 de 2025, de https://www.sciencedirect.com/science/article/abs/pii/S0190740923005480?utm_source

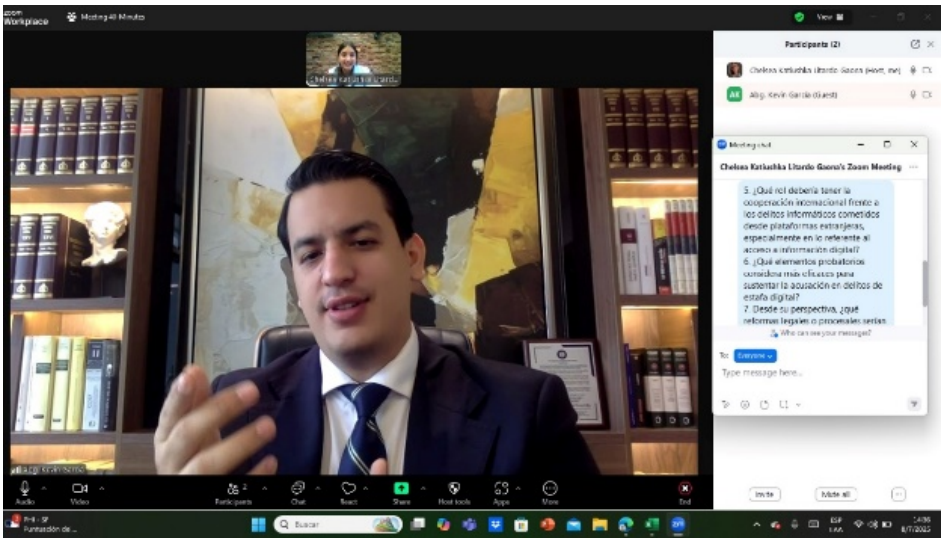
Wikipedia. (s.f.). *Wikipedia*. (Wikipedia, Editor) Recuperado el 01 de 07 de 2020, de https://en.wikipedia.org/wiki/Pig_butchering_scam?utm_source

World Bank Group . (31 de Enero de 2024). *Digital Economy for Latin America and the Caribbean*. Obtenido de Country Diagnostic: Ecuador: https://www.worldbank.org/en/programs/de4lac/publication/digital-economy-for-latin-america-and-the-caribbean-country-diagnostic-ecuador

ANEXOS

Anexo No. 1

Fotografía de entrevistado No. 1 Mgtr. Kevin David García Coronel, Esp.

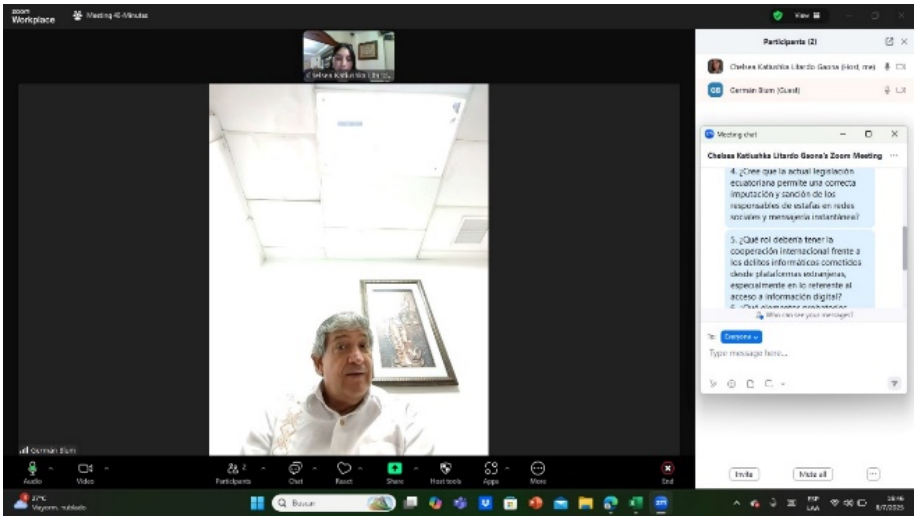


Anexo No. 2

Fotografía de entrevistado No. 2 Mgtr. Piedad Jacqueline Villacís Peña, Esp.

Anexo No. 3

Fotografía de entrevistado No. 3 Mgtr. German Alejandro Blum Espinoza, Esp.



Anexo No. 4

Fotografía de entrevistado No. 5 Mgtr. Francisco Cáceres Villacís, Esp

Anexo No. 5

Fotografía del entrevistado No. 6 Lcdo. Alex Cáceres

Anexo No. 6

4 de 215

Estimado Usuario/a,

Un saludo cordial de la Defensoría del Cliente, designada por la Superintendencia de Bancos, para Banco Internacional.

Su caso ha sido ingresado con número de **OFICIO No. DCBI-DABS-2025-121**, mismo que será atendido por la institución financiera mediante descargo de las pruebas solicitadas conforme lo estipula la norma legal correspondiente emitida por la SB que dice:

"Descargos. - Admitido a trámite el requerimiento se correrá traslado a la entidad financiera a fin de que, en el término de días hábiles, ocho (8) días, si es transacción nacional, y veinte (20) días, si es transacción internacional, presente sus descargos y a la vez se requerirá la información que considere necesaria, misma que deberá ser entregada en el mismo término. Excepcionalmente, a solicitud de la propia entidad financiera, podrá ampliarse dicho plazo por la mitad del periodo otorgado inicialmente".

Una vez que este defensor recepte los descargos procederá a realizar el análisis correspondiente y comunicar por esta vía, teniendo un término de hasta 30 días conforme la complejidad de cada caso para emitir dicho fallo según lo estipula la normativa legal vigente.

Atentamente,

Abg. Diego Barba Salazar MSc.
Defensor del Cliente
Banco Internacional
Av. Patria E4-41 y 9 de Octubre. Edf. Patria, Mezzanine
Teléfono: 025003600 Ext. 999005

DEFENSOR DEL CLIENTE

Activar Windows
Ve a Configuración para activar Windows.

Anexo No. 7

Estimado usuario/a,

Un saludo cordial de la Defensoría del Cliente, designada por la Superintendencia de Bancos, para Banco Internacional.

Con respecto a su requerimiento signado con oficio **No. DCBI-DABS-2025-121**, esta instancia de defensa del cliente se permite manifestar lo siguiente:

Conforme lo estipulado en la normativa correspondiente que en su art. 5 indica.

- Obligaciones del Defensor del Cliente. - Son obligaciones del Defensor/a del Cliente las siguientes:

a) Atender las consultas, quejas o reclamos que los clientes interpongan en contra de las entidades financieras en los plazos y términos señalados en la presente norma, para lo cual requerirá a la entidad financiera la información y documentación pertinente al caso;

Una vez que, recibido su caso el cual ha sido analizado por este defensor como primer filtro y se ha solicitado los respectivos descargos a la institución financiera, procedo a comunicar a usted en calidad de usuario financiero del banco, la respectiva resolución a su proceso por parte de esta **instancia de investigación y conciliación** que es la Defensoría del Cliente:

1. DESCARGOS:

En atención al caso presentado por el señor Francisco Alex Cáceres [redacted] portador de la cédula de ciudadanía Nro. [redacted] y titular de la tarjeta de crédito Nro. 439473******5058, me permito manifestar lo siguiente:

- La transacción registrada en el mes de junio de 2025 por el valor de $ 304.43 se realizó a través del establecimiento Neteller cuyo giro de comercio corresponde a INST.FINANCIERAS-MERCADERIAS Y SERVICIO, la misma que **se efectuó ingresando todos los datos personales del tarjetahabiente; así como, el número de la tarjeta y código de seguridad CVV elementos que deben permanecer bajo cuidado diligente y custodia de su titular**.

Se acompaña Log de transacciones en el que se puede evidenciar el tipo de captura 1 (Transacciones por internet o vía telefónica).

Adjunto detalle de **notificaciones enviadas durante el mes de junio de 2025 al número celular** [redacted] **al correo electrónico** [redacted]. Adicionalmente se remite notificaciones enviadas como protocolo de seguridad adicional es decir 3DS 2.0, correspondiente al mes de junio, el banco para garantizar que el cliente está haciendo uso de su medio de pago (tarjeta) remitió a su celular una clave temporal (OTP) la misma que al registrarla en el link autoriza y garantiza una compra segura.

El protocolo de seguridad 3DS posibilita la autenticación de las transacciones en línea al enviar la información únicamente a los teléfonos previamente registrados en la base de datos del Banco.

La tarjeta de crédito Nro. 439473******5058 fue bloqueada a través de Call Center el día 26 de junio de 2025 a las 15hrs56min.

Anexo No. 8

Señores
Defensoría del Cliente
Banco Internacional S.A.
Presente.-

Asunto: Apelación e inconformidad respecto al oficio No. DCBI-DABS-2025-121

De mi consideración:

Yo, **Francisco Alex Cáceres Villacís**, portador de la cédula de ciudadanía Nro. [redacted] titular de la tarjeta de crédito Nro. 439473******5058, me dirijo a ustedes en uso de mi derecho a presentar mi inconformidad con la resolución emitida mediante oficio No. DCBI-DABS-2025-121, en relación con el reclamo por la transacción no reconocida por un monto de USD 304.43 realizada en el mes de junio de 2025.

I. Fundamentación de mi inconformidad

1. **Falta de notificación efectiva**

Se indica en la resolución que fui notificado oportunamente de la transacción y del código OTP (3DS 2.0) tanto al número celular como al correo electrónico registrado ([redacted]. Sin embargo, niego categóricamente haber recibido notificación alguna en mi correo electrónico.
Cabe resaltar que el banco no ha presentado copia de los correos electrónicos enviados desde una dirección institucional oficial ni registros de los mensajes enviados (headers completos, contenido, y constancia de entrega), limitándose a adjuntar archivos en formato Excel que carecen de valor probatorio suficiente conforme al **Artículo 193 y 195 del Código Orgánico Administrativo**, los cuales exigen acreditar los hechos alegados mediante prueba idónea y suficiente.

2. **Ausencia de prueba documental fehaciente**

Los "logs" remitidos en formatos de hoja de cálculo no constituyen documentos verificables de notificación, ya que no se acompañan con los respaldos reales de los correos enviados (con su metadata técnica) ni capturas del envío de los mensajes SMS de forma íntegra.
Además, la simple referencia a un protocolo de seguridad (3DS 2.0) no prueba la efectiva autenticación por mi parte si no se acredita documentalmente la recepción y aceptación consciente de dichos códigos.

3. **Principio de responsabilidad objetiva y deber de seguridad**

De conformidad con la normativa vigente, las entidades financieras están obligadas a garantizar la seguridad de los medios de pago y verificar la autenticidad de las transacciones. En este caso, el uso indebido de mis datos personales evidencia una vulneración de la custodia y seguridad de la información, por lo que corresponde al banco demostrar plenamente la autorización expresa y consciente de la operación, lo cual no ha sido acreditado.

II. Solicitud

Por las razones expuestas, solicito que se convoque a **audiencia de conciliación** conforme al Art. 43 de la Ley de Arbitraje y Mediación, y en caso de no llegarse a un acuerdo, se remita el expediente completo a la Superintendencia de Bancos, a fin de que esta autoridad resuelva en última instancia conforme al Art. 17 de la normativa vigente.

Así mismo, requiero que el banco entregue copias certificadas y verificables de todos los correos electrónicos supuestamente enviados, así como registros completos (incluidos encabezados y metadatos) de los mensajes SMS, para que pueda ejercer adecuadamente mi derecho de contradicción y defensa.

Sin otro particular, agradezco su atención y quedo atento a la convocatoria respectiva.

Atentamente,