Pontificia Universidad Católica del Ecuador
Seréis mis testigos
ESMERALDAS

CARRERA DE DERECHO

TEMA: El delito de estafa a través de redes sociales y su incidencia en el comercio electrónico en el Ecuador.

Proyecto de investigación previo a la obtención del título de Abogado

Línea de investigación:

ESTADO, DERECHO Y SOCIEDAD

Autor:

José Jerohoan Sánchez Mora

Director:

Abg. Drouet Campo Nino Giovanny PhD.

Esmeraldas - Ecuador

Septiembre 2026

DEDICATORIA

Ante todo, a Dios, que ha sido mi guía en todo este camino y al cual le atribuyo su bendición en mi vida personal y académica, especialmente por los días que se tornaron difíciles, arduos y complicados, por darme su protección y sobre todo por brindarme la paciencia para persistir y cumplir este logro.

A mi familia, seres queridos y allegados, los cuales también formaron parte de este proceso y que confiaron en los resultados, por ofrecerme su apoyo, valorar mi esfuerzo, aconsejarme a buscar siempre la excelencia y motivarme en cada decisión importante. Les dedico estas palabras con mucho aprecio y estima.

Al final somos una mezcla de todas las personas que han sido parte de nuestro camino, me alegra saber que algunas de ellas son parte esencial de quien soy hoy.

AGRADECIMIENTO

A la Universidad Católica de Esmeraldas, mi Alma Mater, por permitirme ser parte de ella, ser el lugar donde conviví, aprendí y cultivé mis conocimientos, que contribuyeron en mi vida profesional y personal. A los docentes, que me orientaron en todo este camino y dejaron un aporte de valores y principios que representa la calidad de excelentes profesionales que influyeron en mi crecimiento académico. A todos ellos, les extiendo un especial agradecimiento por ser parte de este logro.

RESUMEN

El crecimiento del comercio electrónico y el uso masivo de las redes sociales en Ecuador han impulsado nuevas formas de intercambio comercial, pero también han favorecido el incremento de estafas digitales que afectan el patrimonio de los consumidores y generan desconfianza en las transacciones en línea. Esta investigación surge por la necesidad de analizar esta problemática desde una perspectiva jurídica, debido a su impacto en la seguridad del comercio electrónico y en la protección de los derechos de los usuarios.

El objetivo general consistió en analizar el delito de estafa a través de redes sociales y su incidencia en el comercio electrónico en el Ecuador. Para su desarrollo, se empleó un enfoque cualitativo, con un nivel de investigación descriptivo y explicativo. Asimismo, se utilizaron los métodos documental y comparativo, mediante la revisión y análisis de doctrina, normativa jurídica, jurisprudencia, artículos científicos e informes especializados relacionados con el delito de estafa, los delitos informáticos y el comercio electrónico.

Los resultados evidenciaron que las modalidades más frecuentes de estafa se realizan mediante la suplantación de identidad, perfiles falsos, phishing, ingeniería social y publicidad engañosa, principalmente en plataformas como Facebook, WhatsApp e Instagram. Estas conductas ocasionan pérdidas económicas, disminuyen la confianza de los consumidores y afectan el desarrollo del comercio electrónico en el país. Finalmente, se concluye que es necesario fortalecer la educación en ciberseguridad, promover mecanismos de verificación de identidad para vendedores en redes sociales e impulsar una mayor coordinación entre las instituciones públicas, el sector privado y las plataformas digitales para prevenir estas conductas y garantizar una mayor protección a los consumidores.

Palabras clave: delito de estafa, redes sociales, ciberdelitos, comercio electrónico, protección del consumidor.

ABSTRACT

The growth of e-commerce and the widespread use of social media in Ecuador have spurred new forms of commercial exchange, but they have also contributed to an increase in digital scams that affect consumers' financial well-being and generate mistrust in online transactions. This research arises from the need to analyze this issue from a legal perspective, given its impact on the security of e-commerce and the protection of users' rights.

The overall objective was to analyze the crime of fraud committed through social media and its impact on e-commerce in Ecuador. A qualitative approach was employed, with a descriptive and explanatory research focus. Additionally, documentary and comparative methods were employed through the review and analysis of legal doctrine, legislation, case law, scholarly articles, and specialized reports related to fraud, cybercrimes, and e-commerce.

The results showed that the most common forms of fraud involve identity theft, fake profiles, phishing, social engineering, and misleading advertising, primarily on platforms such as Facebook, WhatsApp, and Instagram. These practices cause financial losses, erode consumer trust, and hinder the development of e-commerce in the country. Finally, the study concludes that it is necessary to strengthen cybersecurity education, promote identity verification mechanisms for sellers on social media, and foster greater coordination among public institutions, the private sector, and digital platforms to prevent these behaviors and ensure greater consumer protection.

Keywords: fraud, social media, cybercrime, e-commerce, consumer protection.

INDICE GENERAL DE CONTENIDOS

DEDICATORIA 2
AGRADECIMIENTO 3
RESUMEN 4
ABSTRACT 5
INDICE GENERAL DE CONTENIDOS 6
INTRODUCCIÓN 8
MARCO TEORICO 11
1. El delito de estafa 11
1.1. Evolución del delito de estafa a través de redes sociales 13
1.2. Bien jurídico protegido 15
1.3. Distinción con el delito de apropiación fraudulenta por medios electrónicos 15
2. El delito de estafa a través de redes sociales 17
2.1. La ingeniería social 18
2.2. El phishing 20
2.3. La inteligencia artificial 21
2.4. Tratados internacionales 23
3. Modalidades del delito de estafa a través de redes sociales 24
3.1. Facebook, marketplace y falsos perfiles 26
3.2. Whatsapp, suplantación de identidad y phishing 27
3.3. Instagram, falsas tiendas y publicidad engañosa 27
4. Incidencia en el comercio electrónico ecuatoriano 28
4.1. Crecimiento del comercio electrónico en Ecuador 30
4.2. Marco normativo de comercio electrónico ecuatoriano 31

4.3. Sistemas de seguridad en el comercio electrónico.....32

4.3. Propuesta Normativa 34

CONCLUSIONES.....36

RECOMENDACIONES 37

REFERENCIAS BIBLIOGRÁFICAS.....38

INTRODUCCIÓN

Para iniciar, la transformación digital experimentada en los últimos años ha generado cambios importantes en las relaciones sociales, económicas y comerciales a escala mundial. En el caso del Ecuador, el incremento del acceso a internet, el uso generalizado de dispositivos móviles y el crecimiento de las redes sociales han impulsado nuevas formas de interacción entre las personas, favoreciendo al mismo tiempo la consolidación del comercio electrónico como una alternativa ágil y eficiente para la adquisición y comercialización de bienes y servicios. No obstante, este desarrollo tecnológico también ha sido aprovechado por organizaciones delictivas que utilizan plataformas como Facebook, WhatsApp e Instagram para llevar a cabo distintas modalidades de fraude, engaño y suplantación de identidad con el fin de obtener beneficios económicos de manera ilícita. Como resultado, estas prácticas han afectado la confianza de los usuarios y han comprometido la seguridad de las operaciones comerciales efectuadas en entornos digitales.

La presente investigación se circunscribe al análisis del delito de estafa perpetrado a través de redes sociales y su incidencia en el comercio electrónico ecuatoriano. En lo que respecta a su delimitación temática, el estudio se centra en las modalidades fraudulentas mediadas por dichas plataformas, su vinculación con técnicas de ingeniería social, phishing y otras formas de ciberdelincuencia, así como su repercusión en las actividades comerciales digitales. Desde una perspectiva espacial, la investigación se circunscribe al territorio ecuatoriano, tomando en consideración el marco normativo vigente y el contexto social inherente al uso de plataformas digitales. Respecto a la delimitación temporal, el periodo de análisis comprende los años 2020 a 2025, etapa caracterizada por un crecimiento exponencial del comercio electrónico, la digitalización de servicios y el correlativo incremento de los ilícitos informáticos asociados a las redes sociales.

La justificación del estudio reposa en su pertinencia jurídica, social y tecnológica, en tanto que las estafas instrumentadas a través de entornos digitales constituyen una problemática creciente que afecta de manera directa el patrimonio de los ciudadanos y la credibilidad del comercio electrónico. Su relevancia estriba en la necesidad de comprender las nuevas dinámicas criminales emergentes a partir del uso de herramientas tecnológicas y del desarrollo de innovaciones cada vez más complejas, como la inteligencia artificial aplicada a la ciberdelincuencia. Asimismo, el trabajo

presenta un elemento de novedad al explorar la correlación existente entre las estafas en redes sociales y su impacto específico en el comercio electrónico ecuatoriano durante el último lustro. La viabilidad del proyecto se sustenta en la disponibilidad de fuentes doctrinarias, normativas y jurisprudenciales relativas al delito de estafa, los delitos informáticos y el comercio digital. Los beneficiarios directos de esta investigación serán los operadores judiciales, las instituciones públicas encargadas de la prevención y persecución del delito, los comerciantes digitales, los consumidores en línea, los estudiantes de derecho y la ciudadanía en general, quienes dispondrán de elementos analíticos que coadyuven a la comprensión y mitigación de este fenómeno delictivo.

Con base en el problema identificado, el objetivo general de la investigación consiste en analizar el delito de estafa a través de redes sociales y su incidencia en el comercio electrónico en el Ecuador. Para cumplir con este propósito, se plantean como objetivos específicos identificar las principales modalidades de estafa cometidas mediante redes sociales y establecer una propuesta institucional frente a su incidencia en el comercio electrónico ecuatoriano. Estos objetivos permitirán examinar las estrategias empleadas por los ciberdelincuentes, determinar los efectos que producen en las actividades comerciales desarrolladas mediante plataformas digitales y plantear mecanismos orientados a fortalecer la prevención de este delito y la protección de los usuarios.

La investigación se desarrollará bajo un enfoque cualitativo, orientado a comprender e interpretar los aspectos jurídicos, doctrinarios y sociales relacionados con el delito de estafa cometido a través de redes sociales. El estudio será de tipo descriptivo y explicativo. Tendrá un carácter descriptivo porque permitirá identificar y caracterizar las distintas modalidades de estafa digital, sus elementos constitutivos y la incidencia que tienen en el comercio electrónico; mientras que será explicativo porque buscará establecer las causas, condiciones y consecuencias derivadas de estas conductas ilícitas dentro del contexto digital ecuatoriano. Para la recopilación y el análisis de la información se emplearán los métodos documental y comparativo. El método documental facilitará la revisión de libros, artículos científicos, normativa jurídica, informes institucionales y demás fuentes especializadas relacionadas con el objeto de estudio. Por su parte, el método comparativo permitirá confrontar criterios doctrinarios, disposiciones normativas y experiencias relacionadas con la regulación y prevención de las estafas digitales, contribuyendo a una comprensión más amplia e

integral del fenómeno investigado. Finalmente, la información obtenida será examinada mediante técnicas de revisión bibliográfica y análisis jurídico, garantizando la consistencia, validez y confiabilidad de los resultados alcanzados. Por último, esta investigación pretende contribuir al estudio jurídico del delito de estafa cometido a través de redes sociales, analizando su incidencia en el comercio electrónico ecuatoriano y proponiendo alternativas institucionales que fortalezcan la protección del patrimonio de los usuarios, la seguridad de las transacciones digitales y la confianza en el desarrollo del comercio electrónico en el Ecuador.

MARCO TEORICO

1. El delito de estafa

El artículo 186 del Código Orgánico Integral Penal, expresa; "La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario. 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años. La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años. La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días." (Asamblea, 2014). En otras palabras, se tipifica la estafa como una conducta basada en el engaño, la simulación de hechos falsos, la deformación de la verdad o el ocultamiento de información relevante, con el propósito de inducir a una persona a realizar un acto que cause perjuicio a su patrimonio. El elemento central de este delito es la generación de un error en la víctima, que la lleva a desprenderse voluntariamente de dinero, bienes o derechos en beneficio del autor o de un tercero.

De este modo, la estafa ocurre generalmente cuando alguien construye un engaño (con mentiras, simulaciones u ocultando información relevante) para que otra persona crea una realidad falsa, tome una decisión patrimonial y, como resultado, pierda dinero, bienes o derechos, mientras el autor del delito obtiene un beneficio económico para sí o para un tercero. Dicho de forma más simple, la estafa no es solo "mentir", sino hacer que la mentira funcione como una trampa, es decir, el engaño provoca un error en la víctima y ese error la lleva a entregar algo o a realizar un acto que termina afectando su patrimonio.

Por otra parte, doctrinariamente se constituye como un delito en el que se obtiene una ganancia mediante engaños, aprovechándose de la desinformación o del abuso de confianza de otra persona. Consiste en cualquier forma de defraudación que afecte a alguien en aquello que legítimamente le pertenece. Implica apropiarse de bienes ajenos con un consentimiento solo aparente del dueño, quien es inducido a actuar por su buena fe o por haber sido superado mediante astucia. Entre sus manifestaciones se incluyen conductas como solicitar algo con intención de no pagarlo, cobrar dos veces una misma obligación, negar un pago ya recibido, así como realizar una promesa falsa u ofrecer algo sabiendo que no se cumplirá. (Cabanellas, 1993). De esta manera, la estafa es una forma de defraudación en la que el autor del delito obtiene un lucro aprovechándose del engaño, de la ignorancia de la víctima o del abuso de confianza, logrando que esta actúe bajo una apariencia de consentimiento que en realidad está viciada por la mentira o la manipulación; lo central aquí no es solo "quitar" algo, sino provocar que la propia víctima realice un acto que termina perjudicándola patrimonialmente, porque confía en una promesa, en una versión distorsionada de los hechos o en información ocultada intencionalmente.

Por lo tanto, la estafa se conforma como un delito de resultado y no como un simple incumplimiento o conflicto civil, porque explica que su consumación depende de una cadena causal claramente identificable: primero existe una conducta engañosa (ardid), luego se produce el error en la víctima, después ocurre el acto de disposición o prestación motivado por ese error y, finalmente, se materializa el perjuicio patrimonial. Este enfoque es relevante porque delimita cuándo una conducta pasa del ámbito meramente prejurídico (por ejemplo, una mentira sin efectos) al terreno penal, exigiendo que el engaño sea funcional, es decir, que provoque efectivamente una disposición patrimonial perjudicial. Asimismo, el artículo 186 del COIP demuestra una notable

capacidad de adaptación a las nuevas formas de criminalidad económica, pues su redacción permite sancionar no solo las estafas tradicionales, sino también aquellas cometidas mediante herramientas tecnológicas y redes sociales. Aunque la norma no menciona expresamente plataformas digitales, los elementos de simulación, engaño e inducción a error son perfectamente aplicables a las modalidades modernas de fraude electrónico.

1.1. Evolución del delito de estafa a través de redes sociales

De acuerdo al contexto histórico, "este aumento en la popularidad también ha traído consigo un incremento significativo en el crimen virtual desde que estas plataformas se iniciaron hasta la actualidad. El crimen virtual en las redes sociales se manifiesta en diversas formas, donde los delincuentes aprovechan estas plataformas para cometer diversos tipos de crímenes." (Moncada & Miranda, 2025). De este modo, la evolución histórica de las estafas y delitos en redes sociales está directamente vinculada al crecimiento y consolidación de estas plataformas digitales en la sociedad. En el contexto ecuatoriano, este fenómeno refleja cómo el desarrollo tecnológico no solo ha transformado la comunicación y el comercio, sino que también ha generado nuevas oportunidades para la criminalidad.

Desde sus inicios, las redes sociales han pasado de ser simples herramientas de interacción a convertirse en escenarios complejos donde los delincuentes adaptan continuamente sus métodos para engañar a los usuarios, especialmente mediante estafas digitales. Esta evolución evidencia que las conductas delictivas no son estáticas, sino que se perfeccionan con el tiempo, aprovechando la confianza, el anonimato y la masividad de estos medios. En consecuencia, el crecimiento de las estafas en redes sociales en Ecuador no puede entenderse sin considerar su desarrollo histórico paralelo al avance tecnológico, lo que resalta la necesidad de fortalecer tanto el marco jurídico como la educación digital para enfrentar eficazmente este tipo de delitos contemporáneos.

El Código Penal ecuatoriano de 1938 constituye una de las primeras manifestaciones normativas orientadas a sancionar el delito de estafa dentro del ordenamiento jurídico nacional, posteriormente, esta codificación se unifico al Código Penal de 1971. Esta ley sancionaba una modalidad de defraudación patrimonial, tradicionalmente asociada al abuso de confianza. La conducta típica consistía en que una persona recibiera legítimamente bienes o documentos ajenos

bajo la obligación de devolverlos o destinarlos a una finalidad específica y posteriormente, actuara de manera fraudulenta apropiándose de ellos o dándoles un destino distinto al acordado.

Se establece expresamente en el artículo 560 que dice lo siguiente;

> El que fraudulentamente hubiere distraído o disipado en perjuicio de otro, efectos, dinero, mercancías, billetes, finiquitos, escritos de cualquier especie, que contengan obligación o descargo, y que le hubieren sido entregados con la condición de restituirlos, o hacer de ellos un uso o empleo determinado, será reprimido con prisión de uno a cinco años y multa de ocho a dieciséis dólares de los Estados Unidos de Norte América. (Asamblea N. , 1938).

Al comparar esta tipificación con el actual artículo 186 del Código Orgánico Integral Penal (COIP), se observa una evolución significativa en la técnica legislativa. El COIP establece que:

> "Comete estafa la persona que, buscando un beneficio patrimonial para sí o para un tercero, mediante la simulación de hechos falsos, la deformación u ocultamiento de hechos verdaderos, induzca a error a otra persona para que realice un acto que perjudique su patrimonio o el de un tercero" (2013, Art 186).

Esta definición es más amplia y menos ambigua, ya que no se limita a enumerar determinadas formas de engaño, sino que permite abarcar nuevas modalidades fraudulentas surgidas con el desarrollo tecnológico. Al comparar ambas normativas, puede afirmarse que el artículo 560 del Código Penal de 1971 protegía de forma específica las situaciones de confianza en las que una persona recibía bienes ajenos con una obligación determinada y posteriormente abusaba de esa confianza. Su fortaleza era la precisión descriptiva de la conducta. Sin embargo, su alcance resultaba limitado frente a nuevas modalidades de fraude. Por su parte, el artículo 186 del COIP adopta una concepción más moderna de la estafa, centrada en el engaño como mecanismo de obtención del beneficio patrimonial ilícito. Esta regulación ofrece mayor flexibilidad para sancionar conductas defraudatorias actuales, aunque al ser más amplia exige una interpretación cuidadosa para evitar confundir incumplimientos civiles o contractuales con verdaderos delitos de estafa. En síntesis, la actual redacción del artículo 186 favorece la persecución de nuevas modalidades delictivas porque ofrece una definición tecnológicamente neutral y adaptable. Esto permite que el Derecho penal responda a las transformaciones de la ciberdelincuencia, siempre

que se comprueben todos los elementos jurídicos de la estafa y se evite una interpretación excesivamente amplia que convierta cualquier conflicto comercial en un delito.

1.2. Bien jurídico protegido

En este sentido, "los ciberdelitos pueden abarcar conductas que pueden vulnerar varios bienes jurídicos como la intimidad, el patrimonio económico, el honor, etc., a través de sistemas informáticos. (Altamirano, 2025). Es decir, especialmente conforme al delito de estafa el bien jurídico protegido es el patrimonio o la propiedad de la persona afectada. Asimismo, las conductas fraudulentas ejecutadas mediante sistemas informáticos tienen la capacidad de afectar simultáneamente diversos intereses jurídicamente protegidos, lo que evidencia la complejidad de este tipo de delitos en los entornos digitales.

Del mismo modo, en el bien jurídico protegido de la estafa el ciberdelincuente busca obtener un beneficio económico indebido mediante la manipulación de datos, sistemas o procesos informáticos. Sin embargo, la conducta fraudulenta también puede comprometer la confidencialidad de la información, la confianza en los sistemas tecnológicos y la seguridad de las transacciones electrónicas. Por ello, estos delitos poseen un carácter pluriofensivo, pues pueden lesionar simultáneamente varios intereses jurídicamente protegidos.

1.3. Distinción con el delito de apropiación fraudulenta por medios electrónicos

Respecto a "Ecuador es uno de los países que incorporó en el Código Orgánico Integral Penal diversas figuras delictivas relacionado con el uso indebido de las tecnologías como la apropiación fraudulenta por medios electrónicos, interceptación ilegal de datos, ataque a la integridad de sistemas informáticos, entre otros, con el fin de proteger la seguridad de la información y los derechos de los ciudadanos en el entorno digital." (Portilla, Menza, & Portilla, 2025). El delito de apropiación fraudulenta por medios electrónicos forma parte de un conjunto de delitos informáticos que el legislador ecuatoriano incorporó al COIP para proteger la seguridad de la información, los sistemas tecnológicos y los derechos de los ciudadanos en entornos digitales. A diferencia del delito de estafa, previsto en el artículo 186 del COIP, cuya esencia radica en el engaño dirigido a una persona para inducirla a error y obtener de ella una disposición patrimonial voluntaria, la apropiación fraudulenta por medios electrónicos, regulada en el artículo 190, se

caracteriza por el uso ilícito de sistemas informáticos, redes electrónicas o telecomunicaciones para conseguir una transferencia o apropiación de bienes sin consentimiento del titular.

En este sentido, la diferencia principal radica en la acción empleada para obtener el beneficio económico. La estafa requiere necesariamente la existencia de un engaño que afecte la voluntad de la víctima, quien entrega dinero, bienes o realiza una acción perjudicial para su patrimonio debido a una falsa representación de la realidad. Por el contrario, en la apropiación fraudulenta por medios electrónicos el autor manipula sistemas tecnológicos, credenciales, plataformas digitales o mecanismos de seguridad informática para obtener el resultado ilícito, incluso sin mantener contacto directo con la víctima. En esta modalidad, el autor del delito no necesariamente busca convencer o engañar directamente a la víctima, sino que aprovecha vulnerabilidades tecnológicas o manipula sistemas informáticos para obtener el resultado económico. Sin embargo, en el primer numeral y segundo del artículo 186 del COIP existe una semejanza que puede generar confusión con la tipificación del delito de apropiación fraudulenta por medios electrónicos. En el primer numeral se aplica cuando una persona defrauda utilizando una tarjeta de crédito, débito o pago que fue alterada, clonada, duplicada, robada u obtenida sin la autorización de su titular. El segundo se refiere a la utilización de dispositivos electrónicos manipulados o instalados en cajeros automáticos para capturar y reproducir la información de las tarjetas, como ocurre con los aparatos usados para copiar datos bancarios. En ambos casos, la norma protege el patrimonio del titular y la confianza en los sistemas de pago, y dispone la aplicación de la pena máxima prevista para la estafa. Asimismo, esto no cambia la esencia del delito ya que se usa el engaño, error y persuasión para cometer la estafa, en contraparte, en el delito de apropiación fraudulenta por medios electrónicos solo es necesario que el ciberdelincuente tenga conocimientos informáticos para consumar el delito sin necesidad de contacto directo o comunicación con la víctima, es decir, no se emplea el engaño, error y persuasión.

Por otra parte, el COIP distingue entre diversas modalidades de delitos informáticos, incorporando figuras específicas como la apropiación fraudulenta por medios electrónicos dentro de los delitos que afectan la seguridad de los sistemas informáticos y las transacciones digitales, mientras que la estafa informática se relaciona con las conductas fraudulentas que buscan obtener un beneficio económico mediante el engaño, aprovechando herramientas tecnológicas para provocar un

perjuicio patrimonial a la víctima. Es decir, tanto la estafa como la apropiación fraudulenta por medios electrónicos tienen como finalidad la obtención de un beneficio patrimonial ilícito, ambas figuras jurídicas presentan diferencias importantes dentro del COIP. La estafa, regulada en el artículo 186, se configura cuando el autor emplea engaños, simulaciones o falsedades para inducir a error a la víctima y lograr que esta realice voluntariamente un acto de disposición patrimonial que le ocasione un perjuicio económico. Por tanto, el elemento esencial de este delito es el engaño dirigido a la voluntad de la persona afectada. (Saltos, Robalino, & Pazmiño, 2021).

La diferencia principal radica en que la estafa protege el patrimonio frente al engaño que afecta la voluntad de la víctima, mientras que la apropiación fraudulenta por medios electrónicos sanciona la utilización ilícita de herramientas tecnológicas para obtener bienes o recursos sin autorización. Así, si una persona realiza una transferencia porque fue engañada mediante una publicación falsa en redes sociales, se estaría frente a una estafa; en cambio, si un delincuente accede de forma fraudulenta a una cuenta digital y ejecuta transferencias no autorizadas, la conducta encajaría en la apropiación fraudulenta por medios electrónicos. Ambas figuras tutelan el patrimonio, pero difieren en su forma de ejecución y en el mecanismo empleado para causar el perjuicio económico.

2. El delito de estafa a través de redes sociales

Cabe destacar, "Ecuador no es ajeno a esta realidad, y cada vez son más frecuentes los casos de personas que son víctimas de estafadores que utilizan las redes sociales para llevar a cabo sus crímenes." (Morcillo, 2023). Las estafas en redes sociales se han convertido en una problemática creciente en Ecuador, asociada directamente al contexto de digitalización de la vida cotidiana: al trasladarse la comunicación y las transacciones a entornos virtuales, las redes sociales dejan de ser solo espacios de interacción y pasan a funcionar también como escenarios de riesgo, donde el delincuente aprovecha la confianza, la inmediatez y la facilidad de contacto para engañar y cometer el delito.

En el ámbito digital, puede entenderse que las redes sociales funcionan como un ecosistema de alto riesgo para la estafa porque operan como canales masivos de exposición, persuasión y contacto inmediato con potenciales víctimas: en ellas se difunden anuncios y publicaciones que aparentan ser ofertas legítimas a menudo con precios "demasiado buenos para ser ciertos" que redirigen o empujan a los usuarios hacia sitios web falsos que simulan tiendas reales, o bien capturan

directamente información personal y financiera a través de formularios, enlaces o mensajes; en ese sentido, la dinámica propia de las redes (inmediatez, viralidad, confianza social, facilidad de suplantación y creación de perfiles) facilita que el engaño se vuelva verosímil y se traduzca rápidamente en un acto de disposición patrimonial; (pago/transferencia), cuyo resultado típico es la pérdida económica y la consecuencia de engaño a la víctima, con un efecto más amplio: la erosión de la desconfianza en las transacciones digitales y en el comercio electrónico.

De acuerdo con datos oficiales de la Fiscalía General del Estado difundida por El Comercio, las estafas digitales en Ecuador registraron un crecimiento significativo entre 2020 y 2025, alcanzando su nivel más alto en 2021 con 5.237 denuncias. Posteriormente, aunque las cifras disminuyeron, continuaron siendo elevadas durante 2023 y 2024, con 3.449 y 3.698 denuncias respectivamente. Hasta mayo de 2025 ya se habían contabilizado 1.549 denuncias, evidenciando que este fenómeno continúa representando una amenaza importante para los usuarios de entornos digitales. Asimismo, Guayaquil y Quito concentran aproximadamente el 50 % de las denuncias registradas en el país. (Comercio, 2025).

El crecimiento de las estafas por redes sociales y medios electrónicos entre 2020 y 2025 guarda una estrecha relación con la expansión del comercio electrónico y la digitalización acelerada que experimentó Ecuador después de la pandemia de covid-19. A medida que más ciudadanos comenzaron a realizar compras, pagos y transferencias mediante internet, también aumentaron las oportunidades para que los delincuentes utilizaran plataformas como Facebook, Instagram, WhatsApp, TikTok y páginas web fraudulentas para engañar a los usuarios. Además, las estafas digitales perjudican la reputación del ecosistema de comercio electrónico, obligando a empresas y plataformas a invertir más recursos en mecanismos de seguridad, verificación de identidad y protección de datos. Como consecuencia, se incrementan los costos operativos y se dificulta la consolidación de una economía digital basada en la confianza y la seguridad jurídica.

2.1. La ingeniería social

Cabe mencionar, “estos ataques no solo capitalizan fallos tecnológicos, sino que explotan las debilidades humanas, convirtiendo a cualquier usuario en un potencial blanco. La ingeniería social, en este sentido, se aleja de los tradicionales ataques informáticos basados en software malicioso, centrándose en el ‘factor humano’ como el eslabón más débil en la cadena de seguridad.” (Ibarra,

Tapia, Tene, Toapanta, & Ormaza., 2024). La ingeniería social constituye uno de los mecanismos más relevantes en la ejecución de estafas a través de redes sociales, ya que su efectividad no radica únicamente en vulnerabilidades tecnológicas, sino principalmente en la manipulación psicológica de las personas. Este enfoque permite comprender que el delincuente digital no necesita necesariamente conocimientos técnicos avanzados, sino habilidades para generar confianza, engañar y persuadir a la víctima.

En el contexto del comercio electrónico en el Ecuador, esta situación adquiere mayor relevancia, debido a que los usuarios realizan transacciones en entornos donde predomina la confianza digital y la interacción directa con otros usuarios, lo que incrementa el riesgo de caer en engaños. En consecuencia, la ingeniería social se convierte en el elemento central que articula las estafas digitales, afectando no solo al patrimonio económico de las víctimas, sino también a la seguridad y credibilidad del comercio electrónico, lo que evidencia la necesidad de fortalecer tanto la educación digital como los mecanismos de prevención.

La técnica de ingeniería social más empleada en el ámbito digital es el phishing, mediante la cual los ciberdelincuentes obtienen de manera fraudulenta información confidencial. Entre los datos que buscan captar se encuentran, principalmente, credenciales de acceso, contraseñas y datos financieros, como números de tarjetas de crédito. Para lograrlo, el atacante conocido como phisher suele hacerse pasar por una entidad o persona de confianza, simulando comunicaciones oficiales a través de distintos medios, como correos electrónicos, servicios de mensajería instantánea, redes sociales, mensajes de texto o incluso llamadas telefónicas. (Astudillo, Díaz, & Gordon., 2020). El phishing constituye una de las estrategias más eficaces dentro de la ingeniería social, debido a su capacidad para simular entornos confiables y engañar a los usuarios mediante distintos canales de comunicación digital. Este tipo de ataque evidencia que la vulnerabilidad principal no se encuentra únicamente en los sistemas tecnológicos, sino en el comportamiento humano, puesto que las personas suelen confiar en mensajes que aparentan ser oficiales o provienen de entidades reconocidas.

Al respecto, esta situación resulta especialmente preocupante, ya que la obtención de datos como contraseñas o información financiera puede derivar en delitos de estafa, afectando directamente el patrimonio de las víctimas. Además, la diversidad de medios utilizados por los atacantes como

correo electrónico, mensajería instantánea o llamadas telefónicas demuestra la adaptabilidad de estas técnicas y su constante evolución frente a los mecanismos de seguridad, lo que resalta la importancia de fortalecer la educación digital y la conciencia preventiva en los usuarios para reducir los riesgos asociados a este tipo de ciberdelincuencia.

2.2. El phishing

Para comenzar, "el significado de phishing viene del inglés "fishing" que significa "pesca", haciendo referencia al acto de "pescar" usuarios mediante señuelos que no son detectados por la víctima." (UNIR, 2025). Esta práctica se ha convertido en una de las formas más frecuentes de ciberdelincuencia, ya que los delincuentes aprovechan la confianza que los usuarios depositan en plataformas como Facebook, Instagram, WhatsApp o TikTok para obtener información personal, credenciales de acceso o datos financieros. El "anzuelo" puede presentarse bajo la apariencia de promociones, concursos, premios, mensajes de entidades reconocidas o solicitudes de personas aparentemente conocidas, lo que incrementa la probabilidad de que la víctima interactúe con enlaces fraudulentos o proporcione información sensible.

Por otra parte, el phishing constituye una modalidad de engaño que busca inducir al error a la víctima mediante la simulación de situaciones reales y legítimas, afectando bienes jurídicos como el patrimonio económico, la privacidad y la seguridad de la información. Su peligrosidad radica en que no requiere vulnerar directamente sistemas tecnológicos complejos, sino que explota el factor humano, aprovechándose de la curiosidad, confianza o desconocimiento de los usuarios. En las redes sociales, donde la comunicación es inmediata y masiva, los ciberdelincuentes pueden alcanzar a un gran número de personas en poco tiempo, facilitando la comisión de estafas, suplantaciones de identidad y accesos no autorizados a cuentas personales.

De acuerdo con Emiliano Piscitelli, especialista en ciberseguridad, las modalidades de fraude denominadas phishing, vishing y smishing tienen en común la suplantación de identidad como mecanismo para engañar a las víctimas. La diferencia entre ellas radica en el canal utilizado para cometer el ataque: el phishing se realiza mediante correos electrónicos o sitios web falsificados, el vishing a través de llamadas telefónicas y el smishing mediante mensajes de texto o códigos QR. Asimismo, señala que estos ataques resultan especialmente efectivos porque explotan las vulnerabilidades humanas más que las fallas tecnológicas. Los delitos informáticos modernos no

dependen únicamente del uso de herramientas tecnológicas avanzadas, sino principalmente de la capacidad de los delincuentes para manipular el comportamiento de las personas. En este sentido, el phishing y sus variantes constituyen formas de ingeniería social que buscan generar confianza, urgencia o temor en la víctima para inducirla a revelar información confidencial, realizar transferencias de dinero o proporcionar credenciales de acceso. (Paredes, 2025).

El aspecto más preocupante de estas modalidades es que el objetivo principal no es vulnerar directamente los sistemas informáticos, sino aprovechar errores humanos derivados del desconocimiento, la confianza excesiva o la falta de atención. Asimismo, estas prácticas representan una amenaza constante para la seguridad de los usuarios, ya que los delincuentes adaptan sus estrategias a los medios de comunicación más utilizados por la población. Por esta razón, la prevención de estos delitos no solo requiere mecanismos tecnológicos de protección, sino también educación digital y concienciación ciudadana. En consecuencia, la afirmación de que el ser humano constituye el eslabón más débil de la cadena de seguridad evidencia la necesidad de fortalecer las capacidades de los usuarios para identificar intentos de fraude y evitar convertirse en víctimas de este tipo de ciberdelitos.

2.3. La inteligencia artificial

Ante todo, "la ciberdelincuencia emplea IA para recolectar información sobre posibles víctimas, identificando perfiles específicos en redes sociales. Esto se logra mediante la correlación de imágenes y datos de los usuarios en distintas plataformas, con el objetivo de facilitar engaños más efectivos a través de la IA." (Dirección de Ciberdelitos, 2024). La inteligencia artificial ha transformado las modalidades tradicionales de estafa en redes sociales, permitiendo a los delincuentes recopilar y analizar grandes cantidades de información pública de los usuarios para diseñar engaños altamente personalizados. A diferencia de las estafas convencionales, que suelen dirigirse a un público amplio con mensajes genéricos, la IA facilita la identificación de hábitos, relaciones personales, gustos e intereses de las víctimas, incrementando significativamente la credibilidad de los fraudes y, por consiguiente, las probabilidades de éxito de los delincuentes.

Asimismo, el uso de tecnologías como los deepfakes y la clonación de voz, herramientas que permiten crear contenidos falsos capaces de simular con gran realismo a familiares, amigos, directivos empresariales o figuras públicas. Esta capacidad tecnológica representa un riesgo

considerable para la seguridad digital, puesto que las víctimas pueden confiar en mensajes, llamadas o videos aparentemente auténticos y terminar entregando información confidencial, realizando transferencias de dinero o facilitando accesos a sistemas informáticos. Además, las redes sociales se convierten en una fuente valiosa de datos para los ciberdelincuentes, quienes aprovechan la sobreexposición de información personal para perfeccionar sus estrategias de ingeniería social.

Del mismo modo, la inteligencia artificial ha fortalecido las modalidades de estafa digital al permitir la creación de mecanismos de engaño más sofisticados, como la suplantación de identidad, los contenidos falsos hiperrealistas (deepfakes) y los sistemas automatizados de interacción. Estas herramientas facilitan que los delincuentes generen escenarios aparentemente auténticos en redes sociales y plataformas digitales, dificultando que las víctimas distingan entre información real y fraudulenta, lo que incrementa las probabilidades de éxito del engaño y del perjuicio patrimonial. Es decir, ha transformado significativamente las estafas realizadas a través de redes sociales, dotando a los ciberdelincuentes de herramientas capaces de simular identidades, conversaciones, imágenes y contenidos con un nivel de realismo sin precedentes. En plataformas como Facebook, Instagram, TikTok o WhatsApp, estas tecnologías facilitan la creación de perfiles falsos, videos manipulados y mensajes personalizados que generan confianza en los usuarios y los inducen a compartir información personal o realizar transferencias económicas. (Yong & Medina, 2026).

Por otro lado, el uso de inteligencia artificial no modifica la esencia del delito de estafa, ya que continúa existiendo un engaño destinado a inducir a error a la víctima para obtener un beneficio económico indebido. Sin embargo, sí incrementa la capacidad de persuasión del fraude y dificulta tanto la detección por parte de los usuarios como la investigación de los responsables. Esto supone nuevos desafíos para el derecho penal, especialmente en materia de prueba, identificación de autores y protección de las víctimas frente a modalidades de fraude cada vez más complejas. La inteligencia artificial permite analizar dichos datos para diseñar engaños adaptados a cada víctima, aumentando la credibilidad de las estafas. Por ello, la prevención debe combinar medidas tecnológicas, educación digital y actualización normativa, con el fin de proteger eficazmente a los usuarios frente a los riesgos derivados del uso fraudulento de la inteligencia artificial en entornos digitales.

2.4. Tratados internacionales

En este sentido, “el Convenio de Budapest sobre delitos cibernéticos, es el principal tratado internacional para la lucha contra la delincuencia informática. Fue adoptado en 2001 por el Consejo de Europa, y cuenta, a la fecha, con la participación de 75 países, incluyendo algunos de fuera de Europa, como Estados Unidos, Canadá, Japón o Australia y varios latinoamericanos como Ecuador.” (Naranjo, 2024). La adhesión de Ecuador al Convenio de Budapest representa un avance significativo en el fortalecimiento de su marco jurídico para enfrentar los delitos informáticos, entre ellos la estafa a través de redes sociales. Este tipo de delito ha adquirido una mayor incidencia debido al crecimiento del comercio electrónico y al uso masivo de plataformas digitales para la compra y venta de bienes y servicios. Además, el Convenio proporciona herramientas de cooperación internacional que facilitan la investigación, obtención de evidencia digital y persecución de los responsables, especialmente cuando las conductas delictivas trascienden las fronteras nacionales. Es decir, la participación de Ecuador en este instrumento internacional contribuye a mejorar la capacidad del Estado para combatir las estafas realizadas mediante redes sociales, fortalecer la protección de los usuarios del comercio electrónico y generar mayor confianza en las transacciones digitales.

El Convenio de Budapest sobre los Delitos Cibernéticos constituye un instrumento internacional de gran relevancia para enfrentar los desafíos que plantea la criminalidad en el entorno digital. Su relación con el delito de estafa a través de redes sociales es evidente, ya que esta modalidad delictiva se vale de plataformas digitales para engañar a los usuarios mediante perfiles falsos, anuncios fraudulentos y ofertas inexistentes, afectando principalmente las transacciones realizadas en el comercio electrónico. En el caso de Ecuador, la adhesión al Convenio en el año 2024 representó un avance importante, pues fortalece la cooperación internacional para la investigación de estos delitos, facilita la obtención de evidencia electrónica y promueve la armonización de la legislación nacional con estándares internacionales. En consecuencia, este instrumento no solo contribuye a una respuesta más eficaz frente a las estafas cometidas a través de redes sociales, sino que también favorece el desarrollo de un comercio electrónico más seguro, fortaleciendo la confianza de consumidores y comerciantes en las plataformas digitales y reduciendo los riesgos asociados a las transacciones en línea.

De acuerdo con las Naciones Unidas, la Convención contra la Ciberdelincuencia constituye el primer instrumento jurídico de alcance universal destinado a fortalecer la cooperación internacional para la investigación y sanción de los delitos cometidos mediante las tecnologías de la información y la comunicación. Este tratado establece un marco legal vinculante para enfrentar diversas modalidades de ciberdelitos, entre ellas el fraude financiero, garantizando que todos los Estados cuenten con mecanismos de colaboración que les permitan responder de manera más efectiva frente a estas amenazas digitales. Asimismo, representa un avance significativo en la consolidación de un sistema internacional orientado a prevenir, investigar y sancionar los delitos que se cometen mediante el uso de las tecnologías de la información y la comunicación. Su importancia radica en que reconoce que la ciberdelincuencia constituye un fenómeno de carácter transnacional que no puede ser enfrentado únicamente mediante la legislación interna de cada Estado, sino que requiere mecanismos permanentes de cooperación internacional para el intercambio de información, la obtención de pruebas electrónicas y la asistencia jurídica entre países. (ONU, 2025).

Esta realidad guarda una estrecha relación con el delito de estafa a través de redes sociales, ya que esta modalidad delictiva suele ejecutarse mediante plataformas como Facebook, Instagram, WhatsApp, TikTok o Telegram, donde los delincuentes crean perfiles falsos, publican ofertas inexistentes, suplantan la identidad de empresas o personas y utilizan técnicas de ingeniería social para inducir a las víctimas a realizar pagos o proporcionar información confidencial. En la mayoría de los casos, estas conductas no se limitan al territorio de un solo Estado, sino que involucran servidores, plataformas digitales, cuentas bancarias o responsables ubicados en diferentes países, lo que dificulta considerablemente su investigación y sanción.

3. Modalidades del delito de estafa a través de redes sociales

Es preciso señalar, “es importante saber que el tema del comercio electrónico deja todavía ciertos vacíos legales en nuestro país. Evidentemente, eso hace un poco más complejo el procedimiento de control y atención, y sobre todo de protección a los derechos de las personas usuarias y consumidoras que adquieren bienes y servicios a través de plataformas digitales”. (Bermeo, 2026). Asimismo, el comercio electrónico crece rápidamente, el marco institucional y normativo no siempre avanza al mismo ritmo, lo que genera “vacíos legales” y, en la práctica, dificulta tres

frentes clave: control, atención y protección efectiva del consumidor. En términos concretos, esos vacíos se reflejan en que muchas transacciones ocurren en plataformas digitales (redes sociales, tiendas virtuales, "marketplaces", mensajería) donde la identidad del oferente puede ser opaca, la trazabilidad del pago y del producto depende de intermediarios (bancos, pasarelas, couriers) y la evidencia suele ser digital (capturas, chats, comprobantes), lo que vuelve más compleja la reacción estatal frente al fraude.

El uso intensivo de redes sociales como Facebook, WhatsApp, Instagram, entre otras, ha creado un entorno especialmente fértil para la mutación de la estafa hacia formas digitales, porque estas plataformas combinan alcance masivo, rapidez de interacción, baja fricción para transaccionar (mensajes, catálogos, enlaces, transferencias) y, sobre todo, facilidad para simular legitimidad mediante identidades digitales; por eso, modalidades como perfiles falsos y la venta de productos inexistentes se vuelven recurrentes: basta con construir una cuenta que aparente ser "tienda", exhibir productos atractivos y cobrar por adelantado para luego desaparecer, fenómeno descrito en casos locales donde perfiles en Instagram ofrecen mercancía, reciben pagos y no entregan ni devuelven el dinero, evidenciando además el impacto del engaño en múltiples provincias.

Del mismo modo, las estafas han aumentado y se han adaptado al uso de plataformas digitales y redes sociales, donde los delincuentes emplean engaños para inducir al error y lograr que la víctima realice un acto de disposición patrimonial; además, la falta de información y prevención hace que muchas personas sean especialmente vulnerables a estas modalidades en línea. (Vergara & Zurita, 2025). Es decir, se evidencia que la expansión de las compras y transacciones en línea ha creado un "territorio de oportunidad" para la estafa, porque el ciclo típico del comercio electrónico; publicidad, contacto, pago y entrega, puede ser intervenido por el delincuente en sus fases más sensibles: la confianza y el pago. Asimismo, en plataformas digitales y redes sociales, el estafador puede simular ser un proveedor legítimo (perfiles falsos o "tiendas" aparentes), ofrecer productos atractivos y solicitar pagos por adelantado, logrando que la víctima realice el acto de disposición patrimonial sin contar con verificaciones robustas sobre identidad, reputación o respaldo del vendedor; así, el perjuicio se materializa cuando no existe entrega o devolución, lo que afecta directamente la seguridad del consumidor y erosiona la confianza en el comercio electrónico.

Además, el señalamiento sobre la falta de información y prevención se conecta con una debilidad estructural del comercio electrónico: muchos usuarios transaccionan fuera de canales formales (sin garantías claras, sin trazabilidad completa o sin mecanismos eficaces de reclamo), situación que incrementa la vulnerabilidad y vuelve más complejos los procesos de control, atención y tutela de derechos, especialmente cuando existen "vacíos" en la protección del consumidor en entornos digitales. En otras palabras, el fenómeno descrito no solo supone pérdidas individuales, sino un impacto sistémico: cuanto más frecuentes son las estafas en compras en línea, mayor es la desconfianza hacia el comercio digital, lo que puede frenar su desarrollo y obligar a consumidores y negocios a asumir costos adicionales (verificaciones, intermediarios, pagos contra entrega), reforzando la necesidad de combinar educación preventiva, verificación de proveedores y fortalecimiento institucional para sostener un ecosistema de comercio electrónico más seguro.

3.1. Facebook, marketplace y falsos perfiles

En el Ecuador, "las estafas cibernéticas a menudo se llevan a cabo en plataformas como Marketplace de Facebook, donde los estafadores venden productos falsos o inexistentes. Estos fraudes se caracterizan por la simulación de hechos falsos y la venta de productos a precios significativamente inflados." (Coronel, 2024). Es decir, la cita señala que Facebook Marketplace se ha convertido en un espacio utilizado para cometer estafas, debido a la facilidad con la que una persona puede crear un perfil y publicar productos sin demostrar necesariamente su identidad o la existencia real de lo ofrecido. Los estafadores aprovechan esta situación para presentar anuncios engañosos, utilizar fotografías falsas, ofrecer productos inexistentes o entregar artículos diferentes a los anunciados. Generalmente, buscan atraer a las víctimas mediante ofertas llamativas y luego solicitan pagos anticipados. Desde el punto de vista jurídico, esta conducta puede constituir una estafa cuando existe una simulación de hechos falsos que provoca que el comprador entregue dinero y sufra una pérdida económica. Además del perjuicio patrimonial, estas prácticas generan inseguridad y disminuyen la confianza de los consumidores en las compras realizadas mediante redes sociales.

Además, pone de manifiesto un problema recurrente en Ecuador: la dificultad para identificar a los responsables debido al anonimato que brindan las plataformas digitales y a las limitaciones técnicas para rastrear a los infractores. Por consiguiente, las estafas realizadas mediante Facebook

no solo afectan el patrimonio de los usuarios, sino que también generan desconfianza en el comercio electrónico y en las transacciones efectuadas a través de redes sociales. Esta realidad evidencia la necesidad de fortalecer los mecanismos de control, investigación y prevención, así como de promover una cultura de seguridad digital que permita a los consumidores verificar la autenticidad de vendedores y ofertas antes de realizar cualquier pago o transacción.

3.2. Whatsapp, suplantación de identidad y phishing

Según una publicación del diario; "El Telégrafo", se ha identificado una nueva modalidad de estafa en WhatsApp en la que los delincuentes buscan apoderarse de la cuenta de la víctima mediante el engaño y la obtención de códigos de verificación. Una vez que logran acceder a la cuenta, utilizan la identidad de la persona afectada para comunicarse con sus contactos y solicitar dinero o realizar otros fraudes aprovechándose de la confianza existente entre las partes. La información expuesta refleja cómo las estafas mediante WhatsApp han evolucionado desde mecanismos tradicionales de engaño hacia formas más sofisticadas basadas en la ingeniería social y la suplantación de identidad. Este tipo de fraude resulta especialmente peligroso porque el delincuente no solo busca obtener un beneficio económico directo de la víctima inicial, sino que también utiliza su cuenta para extender el engaño a familiares, amigos y conocidos, quienes tienden a confiar en los mensajes recibidos por provenir aparentemente de una persona cercana. (Telégrafo, 2022).

Estas conductas constituyen una manifestación moderna de la estafa, pues el autor del delito induce a error a las víctimas mediante maniobras fraudulentas destinadas a obtener provecho económico indebido. Asimismo, esta modalidad evidencia los desafíos que enfrentan las autoridades para investigar delitos cometidos en entornos digitales, donde el anonimato y la rapidez de las comunicaciones dificultan la identificación de los responsables. Por ello, resulta fundamental fortalecer la educación en ciberseguridad, promover el uso de mecanismos de autenticación en dos pasos y concienciar a los usuarios sobre la importancia de no compartir códigos de verificación ni información confidencial a través de aplicaciones de mensajería instantánea.

3.3. Instagram, falsas tiendas y publicidad engañosa

Desde esta perspectiva, "por ejemplo, en la red social Instagram es común ver concursos en los que, para participar, debes comentar un post y mencionar hasta a tres amigos tuyos. Esta es ahora

la forma de estafa que busca, entre otras cosas, acceder a sus datos personales para sustraerlos. Para que las víctimas caigan el perfil, que no tiene seguidores, le llegará una notificación y un mensaje que dirá: '¿Has sido etiquetado en la foto? ¡Felicidades! ¡Has ganado la tarjeta de regalo! ¡Sigue la historia y obtén tu premio!'". (Telégrafo D. e., 2023). Una de las modalidades de estafa más frecuentes en Instagram, basada en la manipulación psicológica de los usuarios mediante la promesa de premios o beneficios inexistentes. Los delincuentes aprovechan la dinámica de los concursos que habitualmente circulan en esta red social para generar confianza y aparentar legitimidad, induciendo a las víctimas a proporcionar información personal a través de enlaces fraudulentos. Desde una perspectiva jurídica, esta conducta constituye una forma de engaño orientada a obtener un beneficio ilícito mediante la captación de datos personales, los cuales posteriormente pueden ser utilizados para suplantación de identidad, acceso indebido a cuentas o fraudes económicos.

Asimismo, se observa la utilización de técnicas de ingeniería social que explotan la curiosidad, la emoción y la expectativa de obtener recompensas, elementos que disminuyen la capacidad crítica de los usuarios al momento de verificar la autenticidad de los mensajes recibidos. En este contexto, las estafas por Instagram representan un riesgo creciente para la seguridad digital de las personas y demuestran cómo las redes sociales han evolucionado de simples espacios de interacción social a escenarios utilizados por la delincuencia informática. Por ello, resulta fundamental fomentar la educación digital y la verificación de la autenticidad de perfiles, concursos y enlaces antes de compartir cualquier dato personal o acceder a sitios externos.

4. Incidencia en el comercio electrónico ecuatoriano

Es relevante señalar, "el comportamiento del delito post-pandemia muestra un claro aumento en los casos de estafas y apropiación fraudulenta a través de medios electrónicos, directamente relacionado con el auge de las transacciones digitales y el comercio electrónico durante y después de la pandemia." (Campos, Moreno, & Jimenez, 2025). El comercio electrónico contemporáneo sugiere que el crecimiento acelerado de las transacciones digitales en Ecuador no solo amplió las oportunidades de compra y venta, sino que también expandió la "superficie de ataque" para fraudes y estafas: a medida que más personas migran a pagos en línea, marketplaces y acuerdos comerciales gestionados por redes sociales o mensajería, los ciberdelincuentes encuentran un

entorno propicio para explotar la confianza del consumidor mediante técnicas de ingeniería social (phishing, suplantación de identidad, falsos soportes y anuncios engañosos), lo que se traduce en un aumento de denuncias y en una afectación directa a la seguridad económica de usuarios y organizaciones.

En ese sentido, el comercio electrónico aparece como un espacio donde el factor crítico es la confianza: cuando ésta se deteriora por estafas repetidas, el impacto no se limita a pérdidas individuales, sino que puede frenar la adopción del comercio electrónico, elevar costos de verificación (más controles, intermediarios, pagos contra entrega) y reforzar la percepción de riesgo en la economía digital; por ello, se enfatiza la necesidad de fortalecer educación y concienciación en seguridad digital, así como mecanismos normativos y de denuncia que permitan proteger la información personal y financiera, justamente para sostener un ecosistema de comercio electrónico más seguro y confiable.

Durante la emergencia sanitaria en Ecuador se evidenciaron estafas masivas a través de Internet relacionadas con el comercio electrónico: se difundían supuestas ofertas de productos que, en algunos casos, no correspondían a lo prometido y, en los escenarios más graves, la mercancía nunca era entregada pese a que la víctima ya había realizado el pago. (Enriquez, Muñoz, Guerron, & Santander, 2024). Asimismo, mientras las compras en línea se expanden por su facilidad y alcance, ese mismo entorno abre la puerta a estafas masivas basadas en ofertas engañosas, incumplimientos de entrega y cobros previos, especialmente visibles durante la emergencia sanitaria.

En términos prácticos, el fenómeno descrito revela cómo el comercio electrónico puede convertirse en un escenario de riesgo cuando la transacción se sostiene en confianza digital (publicaciones, anuncios y promesas) sin garantías suficientes de verificación y cumplimiento, de modo que el pago se concreta, pero el producto no llega o no corresponde a lo ofrecido, produciendo un perjuicio patrimonial directo a la víctima. En consecuencia, la observación del delito de estafa sugiere que estas dinámicas afectan más allá del daño individual: erosionan la confianza del consumidor en las compras por Internet y presionan al sistema penal y regulatorio para que actualice su respuesta frente a modalidades que se adaptan rápidamente a los canales digitales,

donde la masividad y la distancia dificultan la identificación del responsable y la reparación efectiva.

4.1. Crecimiento del comercio electrónico en Ecuador

En efecto, "En Ecuador, el crecimiento del comercio electrónico durante el período 2020–2025 evidencia un escenario favorable para los negocios digitales, no obstante, el paso de vender en línea a operar en mercados internacionales exige capacidades más complejas, entre ellas destacan la selección de proveedores, el cumplimiento de requisitos aduaneros, la administración de pagos, la trazabilidad logística, la gestión de devoluciones y la construcción de confianza en consumidores ubicados fuera del país." (Cuñes, Jacome, & Farez, 2026). La cita demuestra que el comercio electrónico en Ecuador experimentó una expansión continua entre 2020 a 2025, convirtiéndose en una herramienta estratégica para el crecimiento empresarial y la apertura de nuevos mercados. Este fenómeno estuvo estrechamente relacionado con la transformación digital, la mayor utilización de plataformas tecnológicas y la adopción de pagos electrónicos, factores que permitieron al país a acceder a oportunidades comerciales que antes estaban reservadas para empresas con mayores recursos.

Sin embargo, especialmente como consecuencia de la digitalización impulsada por la pandemia de covid-19. El incremento del 300 % en la adopción de pagos digitales demuestra una mayor confianza de los consumidores en las transacciones electrónicas y una progresiva incorporación de herramientas tecnológicas en las actividades comerciales. Asimismo, la reducción de los tiempos de entrega en un 40 % refleja una mejora sustancial en los procesos logísticos, aspecto fundamental para la competitividad de los negocios digitales. Es decir, este crecimiento ha permitido que más empresas, especialmente las pequeñas y medianas, accedan a nuevos mercados y amplíen su cartera de clientes. No obstante, el desarrollo del comercio electrónico también ha generado nuevos desafíos relacionados con la seguridad digital y la protección de los consumidores. En este contexto, los delitos de estafa cometidos mediante redes sociales, páginas web falsas o medios electrónicos pueden afectar la confianza del usuario y constituirse en una barrera para la consolidación del comercio electrónico.

4.2. Marco normativo de comercio electrónico ecuatoriano

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos Ecuatoriana establece que "Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información." (Congreso, 2002). Del mismo modo, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce la importancia del comercio electrónico como una herramienta fundamental para el desarrollo económico del país, pero al mismo tiempo advierte la necesidad de proteger este entorno frente a actividades ilícitas. El legislador ecuatoriano considera que las transacciones realizadas mediante redes electrónicas deben desarrollarse dentro de un marco de seguridad jurídica que impida que las plataformas digitales sean utilizadas para fines delictivos.

Esta ley busca fortalecer la confianza de los usuarios mediante mecanismos como la contratación electrónica, las firmas electrónicas, la protección de los consumidores y el reconocimiento jurídico de los mensajes de datos. Asimismo, otorga seguridad a las transacciones digitales y sirven como medios de prueba cuando se producen controversias o conductas fraudulentas, además, representa un instrumento jurídico complementario enfocado en la prevención y para la protección de los usuarios que participan en actividades comerciales realizadas a través de medios electrónicos. Los artículos más importantes son el artículo 8, que permite conservar mensajes, comprobantes y datos de la transacción como evidencia; el artículo 10, que ayuda a comprobar la identidad y procedencia de los mensajes; el artículo 36, que establece la obligación estatal de proteger el comercio electrónico frente a actividades ilícitas; el artículo 50, que exige al vendedor proporcionar información clara, completa y verdadera sobre los productos o servicios; y los artículos 52, 54 y 55, que reconocen y regulan los documentos, mensajes y registros electrónicos como medios de prueba. En conjunto, estas disposiciones permiten prevenir engaños, proteger al consumidor y facilitar la investigación cuando la estafa ya se ha producido, aunque deben complementarse con el artículo 186 del COIP para aplicar la correspondiente sanción penal.

Por otro lado, de acuerdo con la Ley Orgánica de Protección de Datos Personales, toda persona tiene derecho a controlar el uso de su información personal, conocer cómo se recopilan y tratan sus datos, acceder a ellos, rectificarlos, eliminarlos u oponerse a su tratamiento cuando corresponda. Además, la normativa obliga a las entidades públicas y privadas a implementar

medidas técnicas, organizativas y jurídicas que garanticen la seguridad, confidencialidad e integridad de los datos personales, así como a prevenir accesos no autorizados, divulgaciones indebidas o usos ilícitos de la información. (Asamblea N. , 2021).

Por otra parte, las conductas delictivas se apoyan en la obtención, uso indebido o divulgación de información personal de los usuarios. Los estafadores suelen recopilar datos como nombres, números telefónicos, fotografías, direcciones de correo electrónico, información financiera e incluso detalles familiares obtenidos de perfiles públicos en redes sociales para construir engaños más creíbles y personalizados. La ley busca reducir estos riesgos al reconocer el derecho de los ciudadanos a decidir sobre el tratamiento de sus datos personales y exigir que cualquier recopilación o uso de dicha información cuente con una base legal o con el consentimiento del titular. Asimismo, entre los artículos más relevantes para prevenir las estafas digitales son el artículo 7, que exige una base legítima para utilizar datos personales; el artículo 8, que establece que el consentimiento debe ser libre, informado y específico; el artículo 10, que obliga a aplicar principios de confidencialidad, seguridad y responsabilidad; y el artículo 23, que reconoce el derecho a la educación digital. También destacan los artículos 37, 39, 40 y 41, que exigen medidas de seguridad, protección desde el diseño y análisis permanente de riesgos; los artículos 43 y 46, que obligan a notificar las vulneraciones de seguridad; y el artículo 47, que establece las responsabilidades de quienes tratan datos personales. En conjunto, estas disposiciones ayudan a evitar que nombres, fotografías, contraseñas o información financiera sean obtenidos y utilizados para crear perfiles falsos, suplantar identidades o realizar engaños. Además, los artículos 65, 68, 71 y 72 permiten aplicar medidas correctivas y sanciones administrativas cuando las entidades incumplen sus obligaciones de protección, aunque la sanción penal por estafa debe analizarse junto con el artículo 186 del COIP.

4.3. Sistemas de seguridad en el comercio electrónico

Sin embargo, “si bien la Ley Orgánica de Protección de Datos Personales de 2021 establece principios fundamentales para la seguridad digital, su débil articulación con el COIP deja a las víctimas de delitos informáticos sin un marco integral de reparación y justicia. La ausencia de mecanismos sancionadores específicos para el uso indebido de datos personales en casos de fraude o suplantación de identidad incrementa la sensación de impunidad y vulnerabilidad ante los

ciberdelincuentes." (Espinosa & Paredes, 2025). La protección de los datos personales constituye uno de los principales mecanismos de defensa frente al delito de estafa en el entorno digital ecuatoriano. El estudio destaca que los ciberdelitos más frecuentes en Ecuador comprenden el acceso no autorizado a sistemas informáticos, la suplantación de identidad y las estafas digitales, conductas que afectan directamente la privacidad, seguridad y patrimonio de los ciudadanos. Los autores sostienen que la vulneración de datos personales se ha convertido en una de las principales herramientas utilizadas por los delincuentes para obtener beneficios económicos ilícitos mediante engaños y fraudes electrónicos.

En el ámbito del comercio electrónico, los consumidores proporcionan constantemente información personal y financiera, como nombres, números de identificación, direcciones, correos electrónicos, cuentas bancarias y datos de tarjetas de crédito. Cuando esta información es obtenida ilegalmente o utilizada sin autorización, los delincuentes pueden emplearla para realizar fraudes, crear identidades falsas o inducir a error a las víctimas con el propósito de obtener dinero o acceder a bienes y servicios de manera ilícita. Además, se señala que, aunque Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales y con disposiciones penales en el Código Orgánico Integral Penal para sancionar la estafa y otros delitos informáticos, todavía existen vacíos normativos y dificultades operativas que limitan una protección efectiva de los ciudadanos. Esta situación genera escenarios de vulnerabilidad para los consumidores digitales y dificulta la persecución de quienes utilizan datos personales para cometer estafas mediante redes sociales, plataformas digitales o sistemas electrónicos.

Resulta importante señalar, que la seguridad en el comercio electrónico depende de la implementación de mecanismos tecnológicos capaces de proteger la confidencialidad, integridad y autenticidad de las transacciones. Entre los sistemas más utilizados se encuentran los protocolos SSL/TLS para la transmisión segura de datos, el protocolo SET para operaciones con tarjetas electrónicas, así como herramientas de protección empresarial como firewalls, antivirus, sistemas de prevención de intrusiones y redes privadas virtuales (VPN), las cuales permiten resguardar la información intercambiada a través de internet. Asimismo, la seguridad constituye uno de los pilares fundamentales para el desarrollo del comercio electrónico en Ecuador. A medida que crecen las compras y transacciones digitales, también aumentan los riesgos asociados con el robo

de información, la suplantación de identidad, el fraude informático y otras formas de ciberdelincuencia. (Chiriguayo, 2015).

Por esta razón, la implementación de protocolos de seguridad y sistemas de protección tecnológica no solo representa una necesidad técnica, sino también una condición indispensable para generar confianza en los consumidores y garantizar la continuidad de las actividades comerciales en línea. Del mismo modo, las amenazas pueden provenir tanto de agentes externos como internos, lo que obliga a las empresas a adoptar políticas integrales de ciberseguridad. En este contexto, herramientas como las VPN, los firewalls y los sistemas de autenticación contribuyen a minimizar vulnerabilidades y a proteger los datos financieros de usuarios y organizaciones. Desde una perspectiva jurídica, estos mecanismos adquieren especial relevancia porque ayudan a prevenir conductas que podrían derivar en delitos informáticos, estafas electrónicas o accesos no autorizados a sistemas de información.

4.3. Propuesta Normativa

Política pública nacional para la prevención de estafas y protección del consumidor en redes sociales

Nombre de la política pública: “Ecuador Compra Seguro”

Se propone implementar la política pública denominada “Ecuador Compra Seguro”, liderada por el Estado ecuatoriano y desarrollada en coordinación con las plataformas privadas de redes sociales, las entidades financieras y los organismos encargados de la administración de justicia. Su objetivo principal sería prevenir las estafas cometidas durante la compra y venta de productos o servicios mediante redes sociales, proteger el patrimonio de los consumidores y fortalecer la confianza en el comercio electrónico nacional. Esta política incluiría campañas permanentes de educación digital para enseñar a la ciudadanía a reconocer perfiles falsos, suplantaciones de identidad, phishing, publicidad engañosa, ofertas inexistentes y otras modalidades de fraude. También establecería un sistema obligatorio de verificación de identidad para quienes comercialicen productos o servicios de manera habitual en redes sociales, permitiendo que los consumidores puedan distinguir claramente entre una cuenta verificada y un perfil cuya identidad no ha sido comprobada. Asimismo, promovería mecanismos de pago protegido, mediante los

cuales el dinero permanezca temporalmente retenido hasta que el comprador confirme la recepción del producto en las condiciones acordadas. La política también contemplaría la creación de un canal público único, gratuito y de fácil acceso para presentar alertas, reclamos y denuncias, permitiendo adjuntar capturas de pantalla, conversaciones, comprobantes de pago, enlaces y demás evidencia digital. Por su parte, las plataformas privadas tendrían la responsabilidad de revisar las cuentas denunciadas, detectar comportamientos sospechosos, suspender perfiles fraudulentos, conservar temporalmente la información relacionada con posibles delitos y colaborar con las autoridades mediante procedimientos legales. Las entidades financieras participarían en la identificación de operaciones sospechosas y en la atención rápida de reportes relacionados con transferencias fraudulentas, mientras que la Policía, la Fiscalía y los organismos de justicia fortalecerían la investigación y sanción de estas conductas.

CONCLUSIONES

- El análisis realizado permitió identificar que el delito de estafa a través de redes sociales constituye una de las modalidades de ciberdelincuencia con mayor crecimiento en el Ecuador, favorecida por el uso masivo de plataformas digitales para la comercialización de bienes y servicios. Se determinó que los delincuentes emplean técnicas como la suplantación de identidad, perfiles falsos, publicidad engañosa, phishing e ingeniería social para inducir al error a las víctimas y obtener un beneficio económico ilícito. Asimismo, se evidenció que estas conductas afectan directamente la confianza de los consumidores, generan pérdidas patrimoniales y debilitan la seguridad del comercio electrónico, lo que demuestra la necesidad de fortalecer tanto los mecanismos de prevención como la aplicación efectiva del marco jurídico vigente frente a esta problemática.
- En relación con la propuesta institucional, se concluye que falta una respuesta institucional coordinada y específica frente a las estafas realizadas mediante redes sociales. No existen suficientes mecanismos de cooperación entre el Estado, las plataformas digitales, las entidades financieras y los organismos de justicia para detectar perfiles fraudulentos, conservar evidencia digital, atender denuncias y facilitar la investigación de estos delitos. Asimismo, la protección del comprador en redes sociales continúa siendo limitada, por lo que resulta necesario fortalecer la regulación, los canales de reclamo y la responsabilidad de las plataformas privadas.

RECOMENDACIONES

- Se recomienda establecer campañas permanentes de educación y prevención digital para que los usuarios puedan identificar las principales modalidades de estafa cometidas mediante redes sociales, como perfiles falsos, suplantación de identidad, phishing, ingeniería social y publicidad engañosa. Estas campañas deben enseñar a verificar la identidad y reputación de los vendedores, desconfiar de ofertas demasiado atractivas, evitar pagos anticipados sin garantías, no compartir contraseñas ni códigos de verificación y utilizar medios de pago seguros. Además, las plataformas digitales deberían mostrar alertas preventivas y facilitar el reporte inmediato de publicaciones, enlaces y cuentas sospechosas.
- Se recomienda implementar la política pública "Ecuador Compra Seguro", liderada por el Estado y ejecutada en coordinación con las plataformas de redes sociales, las entidades financieras y los organismos de justicia. Esta política tendría como finalidad prevenir las estafas y proteger a los consumidores mediante campañas de educación digital, verificación de la identidad de los vendedores, identificación visible de cuentas comerciales confiables, medios de pago protegidos y un canal único para presentar alertas, reclamos y denuncias. Además, las plataformas deberán detectar y suspender perfiles fraudulentos, conservar la evidencia digital y colaborar con las autoridades. De esta manera, la política actuaría antes, durante y después de la transacción, reduciendo las pérdidas económicas y fortaleciendo la seguridad y la confianza en el comercio electrónico ecuatoriano.

REFERENCIAS BIBLIOGRÁFICAS

Altamirano, A. (2025). *La Apropiación Fraudulenta por Medios Electrónicos y el Bien Jurídico Protegido.* Ambato: Ciencia Latina Revista Cientifica Multidisciplinar.

Asamblea. (10 de Febrero de 2014). *Lexis Ecuador.* Obtenido de Lexis Ecuador: https://www.lexis.com.ec/biblioteca/coip

Asamblea, N. (1938). *Codigo Penal.* Quito, Ecuador: Ediciones Legales – Fiel Web.

Asamblea, N. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito, Ecuador: Registro Oficial Suplemento No. 459.

Astudillo, E. B., Díaz, W. F., & Gordon., S. S. (2020). *Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social.* Milagro, Ecuador: Revista Ciencia UNEMI, Universidad Estatal de Milagro.

Bermeo, A. (15 de Enero de 2026). *Ecuavisa*. Obtenido de Ecuavisa: https://www.ecuavisa.com/economia/alerta-estafa-ecuador-tiendas-virtuales-20260115-0085.html

Cabanellas, G. (1993). *Diccionario juridico elemental.* Buenos aires, Argentina: Heliasta S.R.L.

Campos, M., Moreno, R., & Jimenez, B. (2025). *Detección de fraudes y estafas basadas en ingeniería social en Ecuador.* Maracaibo: Revista InveCom (Revista INVECOM "Estudios transdisciplinarios en comunicación y sociedad").

Chiriguayo, S. (2015). *Comercio Electrónico: Importancia de la Seguridad en las Transacciones Electrónicas, Amenazas y Soluciones a Implementar.* Guayaquil, Ecuador: Revista Empresarial, ICE-FEE-UCSG.

Comercio. (16 de junio de 2025). *Más del 50% de las estafas digitales en Ecuador se concentra en dos ciudades*. Obtenido de El Comercio:

https://www.elcomercio.com/actualidad/seguridad/mayoria-denuncias-estafas-digitales-concentra-dos-ciudades-ecuador/

Congreso, N. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.* Quito, Ecuador: Registro Oficial Suplemento No. 557 de la República del Ecuador.

Coronel, I. (2024). *Recomendaciones para evitar ser víctima de estafas por Internet.* Machala: Diario Correo (Ecuador).

Cuñes, J., Jacome, A., & Farez, M. (2026). *Dropshipping internacional y transformación digital empresarial en Ecuador: oportunidades y desafíos para la internacionalización de las MIPYMES durante el período 2020–2025.* Machala: Universidad Técnica de Machala.

Dirección de Ciberdelitos, M. d. (2024). *La nueva era de la ciberdelincuencia, el lado oscuro de la Inteligencia Artificial.* Quito, Ecuador: Ministerio del Interior del Ecuador, Subsecretaría de Combate al Delito, Dirección de Ciberdelitos.

Enriquez, B., Muñoz, D., Guerron, M., & Santander, S. (2024). *La estafa electrónica en el Sistema Penal Ecuatoriano.* Santa Ana de Coro, Venezuela.: Fundación Koinonia (F.K.) / Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas.

Espinosa, G., & Paredes, F. (2025). *Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano.* Ambato: Universidad Tecnológica Indoamérica.

Gaston, P. (1996). *Metodología de la investigación educacional.* Cuba: Editorial Pueblo y Educación.

Ibarra, C. S., Tapia, C. A., Tene, A. M., Toapanta, R. J., & Ormaza., G. S. (2024). *Análisis de los ataques de ingeniería social en Ecuador.* Ecuador: Ciencia Latina Revista Científica Multidisciplinar.

Jiménez, A. R., & Jacinto, A. O. (2017). *Métodos científicos de indagación y de construcción del conocimiento.* Bogotá : Revista EAN (Escuela de Administración de Negocios).

Moncada, J., & Miranda, A. (2025). *La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la Legislación en Ecuador.* Ambato: RICEd: Revista de Investigación en Ciencias de la Educación, Fundación Internacional para Educación la Ciencia y la Tecnología (FIECYT).

Morcillo, L. (2023). Delitos informáticos en Ecuador: Análisis de la intervención penal en casos de estafas mediante redes sociales. *Revista Científica Multidisciplinar G-ner@ndo*, 558–573.

Naranjo, L. (25 de julio de 2024). *Convenio de Budapest sobre delitos cibernéticos*. Obtenido de Universidad de Las Américas (UDLA): https://sitios.udla.edu.ec/2024/07/convenio-de-budapest-sobre-delitos-ciberneticos/

Newman, G. D. (2006). *El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales.* Caracas, Venezuela: Revista Laurus – Universidad Pedagógica Experimental Libertador.

ONU, N. (25 de Octubre de 2025). *Sesenta y cinco países firman el primer tratado contra la ciberdelincuencia, un hito para la cooperación digital*. Obtenido de Noticias ONU: https://news.un.org/es/story/2025/10/1540631

Paredes, E. (28 de Junio de 2025). *Ciberseguridad: cómo detectar estafas digitales y protegerte del phishing.* Obtenido de Revista Gestión – PRIMICIAS: https://www.primicias.ec/revistagestion/tu-dinero/ciberseguridad-estafas-digitales-phishing-99506/

Portilla, R., Menza, E., & Portilla, M. (2025). *Delitos informáticos en el Código Orgánico Integral Penal: una revisión sobre acceso no autorizado, fraude digital y ciberseguridad en Ecuador.* Ecuador: Pro Sciences: Revista de Producción, Ciencias e Investigación.

Ramírez, A. B. (2007). *El carácter científico de la dogmática jurídica.* Santiago de Chile: Revista de Derecho, Universidad Austral de Chile.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). *Análisis conceptual del delito informático en Ecuador.* Cuba: Revista Conrado, Universidad de Cienfuegos.

Telégrafo. (2022). *Reportan nuevo tipo de estafa en WhatsApp.* Quito, Ecuador: Diario el Telégrafo.

Telégrafo, D. e. (2023). *Alerta de estafa en la red social Instagram.* Quito: Diario El Telégrafo.

UNIR, E. (7 de Marzo de 2025). *Phishing: qué es y cómo evitarlo en las empresas.* Obtenido de UNIR Ecuador: https://ecuador.unir.net/actualidad-unir/phising-que-es/

Vergara, J., & Zurita, L. (2025). *La Problemática del Delito de Estafa en Ecuador: Evolución Jurídica, Impacto Tecnológico, Tutela y Protección del Patrimonio.* Pilar, Paraguay: Vitalia Revista Científica y Académica.

Yong, M., & Medina, V. (2026). *El Delito de Estafa en la era de la Inteligencia Artificial: Desafíos Jurídicos ante el Uso Fraudulento de Tecnología.* Ambato, Ecuador: Polo del Conocimiento.