Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Asesoría Jurídica de Empresas

Impacto de la suplantación de identidad electrónica en el comercio electrónico: Propuestas de asesoría jurídica empresarial

Trabajo fin de estudio presentado por:	Léon Chilán Karla Betzabeth
Tipo de trabajo:	Trabajo Final de Maestría
Director/a:	Ignacio Lopéz López
Fecha:	07/04/2025

Resumen

La presente investigación examina las implicaciones jurídicas de la suplantación de identidad electrónica en el ecosistema del comercio digital ecuatoriano, analizando sus repercusiones en la validez contractual y la responsabilidad civil empresarial. Se evidencia una correlación entre el incremento de transacciones electrónicas y la sofisticación de métodos de phishing, vishing y smishing, que comprometen la seguridad transaccional. El estudio identifica deficiencias normativas en el COIP y la Ley de Comercio Electrónico que obstaculizan la persecución penal efectiva de estos ilícitos. La investigación propone un modelo de asesoría jurídica preventiva estructurado en tres fases: diagnóstico de vulnerabilidades, implementación de mecanismos de autenticación multifactorial y monitoreo continuo. Se destaca la necesidad de protocolos estandarizados de compliance digital, cláusulas contractuales específicas sobre identidad digital y cooperación público-privada para fortalecer la seguridad jurídica en entornos digitales, mitigando así las consecuencias económicas y reputacionales del delito.

Palabras clave: Suplantación electrónica, Responsabilidad civil digital, Compliance tecnológico, Autenticación multifactorial, Seguridad jurídica transaccional

Abstract

This research examines the legal implications of electronic identity theft in the Ecuadorian digital commerce ecosystem, analyzing its repercussions on contractual validity and corporate civil liability. An evaluation is evident between the increase in electronic transactions and the sophistication of phishing, vishing and smishing methods, which compromise transactional security. The study identifies regulatory deficiencies in the COIP and the Electronic Commerce Law that hinder the effective criminal prosecution of these crimes. The research proposes a preventive legal advice model structured in three phases: vulnerability diagnosis, implementation of multifactor authentication mechanisms and continuous monitoring. The need for standardized digital compliance protocols, specific contractual clauses on digital identity and public-private cooperation are highlighted to strengthen legal security in digital environments, thus mitigating the economic and reputational consequences of crime.

Keywords: Electronic impersonation, Digital civil liability, Technological compliance, Multi-factor authentication, Transactional legal security

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

La globalización digital ha transformado los modelos tradicionales de comercio, permitiendo el desarrollo de plataformas electrónicas en donde millones de usuarios interactúan para comprar, vender o intercambiar bienes y servicios. Este fenómeno ha facilitado nuevas oportunidades económicas, especialmente para los emprendimientos y empresas que buscan ampliar su alcance comercial. Sin embargo, la misma infraestructura digital que impulsa el comercio electrónico ha abierto también la puerta a nuevas formas de criminalidad, entre ellas, **la** suplantación de identidad electrónica**,** considerada uno de los delitos informáticos de mayor impacto en los últimos años.

En Ecuador, donde el comercio electrónico ha experimentado un crecimiento exponencial, las empresas —particularmente las micro, pequeñas y medianas— se enfrentan a un entorno de vulnerabilidad creciente frente a amenazas cibernéticas. Según CIESPAL (2022), "los delitos cibernéticos, especialmente la suplantación de identidad, se han incrementado con el auge del comercio electrónico en el país, afectando la confianza de los usuarios y la sostenibilidad del modelo digital" (p. 35). La falta de cultura digital, la escasa capacitación jurídica en el ámbito empresarial, y los vacíos legales en materia de delitos informáticos contribuyen a una débil respuesta frente a este fenómeno.

Ante esta realidad, el presente trabajo de investigación tiene como finalidad analizar el impacto de la suplantación de identidad electrónica en el comercio electrónico, con énfasis en las consecuencias jurídicas y económicas que enfrentan las empresas afectadas. Asimismo, busca proponer alternativas viables de asesoría jurídica empresarial que permitan prevenir, mitigar y afrontar este tipo de delitos desde una perspectiva técnica y legal. El enfoque de este

estudio es descriptivo y propositivo, orientado a generar aportes que fortalezcan la seguridad jurídica en el entorno digital ecuatoriano.

1.1. Justificación

La elección del presente tema surge de la necesidad urgente de abordar uno de los desafíos más críticos que enfrenta el ecosistema digital contemporáneo: la suplantación de identidad electrónica. Este delito, que consiste en el uso ilegítimo de datos personales o credenciales digitales de otra persona para realizar actos fraudulentos, afecta de manera directa la seguridad de las operaciones en línea, especialmente en entornos comerciales. Según Kaspersky (2023), "el robo y uso indebido de identidades digitales se ha convertido en una de las formas más comunes de fraude en Internet, con consecuencias devastadoras tanto para individuos como para empresas" (párr. 4).

A pesar del crecimiento sostenido del comercio electrónico en Ecuador, las herramientas jurídicas para combatir eficazmente este tipo de delitos siguen siendo limitadas. Muchas empresas, especialmente las de menor tamaño, no cuentan con protocolos internos ni asesoramiento legal adecuado que les permita prevenir o enfrentar estos eventos de manera efectiva. En este sentido, es fundamental que la academia contribuya con investigaciones aplicadas que no solo evidencien el problema, sino que propongan soluciones concretas desde un enfoque jurídico empresarial.

Como indica Reinoso (2021), "la educación jurídica preventiva y la implementación de asesoría legal especializada son claves para enfrentar el nuevo panorama delictivo digital en América Latina" (p. 92). Las conclusiones del estudio podrían aportar a la elaboración de marcos

normativos más sólidos, así como a la implementación de estrategias preventivas y formativas que protejan tanto a los consumidores como a los actores empresariales en el entorno digital.

1.2. Problema y finalidad del trabajo

La suplantación de identidad electrónica se ha convertido en una práctica delictiva habitual en el comercio digital, especialmente en contextos donde las regulaciones tecnológicas y legales aún son incipientes. En Ecuador, las denuncias por suplantación en plataformas de venta, redes sociales comerciales y sistemas de pago han aumentado en los últimos años. El Informe de Ciberseguridad 2023 del Banco Interamericano de Desarrollo (BID) alerta que "los países de América Latina enfrentan un crecimiento acelerado de los delitos informáticos, y la suplantación de identidad se encuentra entre los tres delitos más reportados en el comercio digital" (BID, 2023, p. 17).

Esta situación plantea un grave problema para el desarrollo confiable del comercio electrónico y para la garantía de los derechos digitales de los usuarios. La finalidad del presente trabajo es analizar el impacto de la suplantación de identidad electrónica en el comercio electrónico ecuatoriano, evaluando sus implicaciones jurídicas y económicas, así como las falencias en la protección de las empresas afectadas. Desde este diagnóstico, se pretende proponer un modelo de asesoría jurídica empresarial que pueda servir como herramienta preventiva y de respuesta ante estos delitos. El estudio se enfoca en el contexto normativo ecuatoriano y en las necesidades reales de las MIPYMES, con el objetivo de fomentar un comercio electrónico más seguro, informado y legalmente respaldado.

1.3. Objetivos

1.3.1. Objetivo General

Analizar el impacto de la suplantación de identidad electrónica en el comercio electrónico y desarrollar propuestas de asesoría jurídica empresarial para su prevención y mitigación.

1.3.2. Objetivos Específicos

- Identificar las principales vulnerabilidades legales y digitales que enfrentan las empresas en el comercio electrónico frente a la suplantación de identidad electrónica.
- Evaluar la normativa ecuatoriana e internacional vigente en materia de ciberseguridad y protección contra la suplantación de identidad.
- Analizar casos reales de suplantación de identidad en el comercio electrónico para comprender sus consecuencias y posibles estrategias de respuesta.
- Diseñar propuestas de asesoría jurídica y protocolos internos para empresas, con el fin de fortalecer su seguridad y minimizar el impacto del delito.

2. Marco teórico y desarrollo

2.1. Fundamentos conceptuales y jurídicos de la suplantación de identidad

2.1.1. Definición de suplantación de identidad electrónica

La suplantación de identidad electrónica, comúnmente conocida como "phishing" o "spoofing", se refiere al acto de adquirir información personal y confidencial de manera fraudulenta a través de medios digitales. Según la Comisión Federal de Comercio (FTC) de Estados Unidos, "el phishing es una táctica utilizada por estafadores para engañar a las

personas y hacer que revelen información personal como contraseñas y números de tarjetas de crédito" (FTC, 2021).

2.1.2. Modalidades de suplantación de identidad electrónica

Existen diversas formas en que se manifiesta la suplantación de identidad en el ámbito digital. Una de las más comunes es el envío de correos electrónicos fraudulentos que imitan a entidades legítimas, solicitando al destinatario que proporcione datos personales. Otra modalidad es la creación de sitios web falsos que replican la apariencia de plataformas auténticas para engañar a los usuarios y obtener sus credenciales de acceso. Además, el "vishing" (phishing por voz) y el "smishing" (phishing por SMS) son técnicas en las que los estafadores utilizan llamadas telefónicas o mensajes de texto para obtener información sensible (Kaspersky, 2020).

A estas se suman el "spoofing" de IP/DNS, que implica la falsificación de direcciones IP o DNS para redirigir el tráfico a sitios maliciosos; el "malware" diseñado para robar credenciales directamente de los dispositivos de los usuarios; y el "account takeover" (ATO), donde los atacantes obtienen acceso a cuentas legítimas de usuarios para realizar transacciones fraudulentas. Investigaciones de Heredia Pincay & Villarreal Satama, (2022) mencionan que estas últimas modalidades son particularmente relevantes en el comercio electrónico, ya que permiten a los ciberdelincuentes operar directamente desde la cuenta de la víctima, dificultando su detección por parte de las plataformas.

2.1.3. Impacto en el comercio electrónico

La suplantación de identidad electrónica tiene consecuencias significativas en el comercio electrónico. Empresas y consumidores pueden sufrir pérdidas financieras considerables debido a transacciones fraudulentas y robo de información bancaria. Además, estos

incidentes erosionan la confianza del consumidor en las plataformas digitales, afectando negativamente la reputación de las empresas involucradas. Según un informe de Cybersecurity Ventures, se estima que el costo global del cibercrimen alcanzará los 10.5 billones de dólares anuales para 2025, con el phishing como una de las principales amenazas (Morgan, 2020).

2.1.4. Casos recientes y estadísticas

En el contexto ecuatoriano, si bien no siempre se detallan públicamente los nombres de las empresas afectadas para proteger su reputación y la privacidad de los usuarios, la Fiscalía **General del Estado (FGE) en su Informe Anual de Ciberdelincuencia de 2023** reportó un incremento del 35% en las denuncias por suplantación de identidad electrónica, superando las 5.000 incidencias, la mayoría vinculadas a transacciones en línea y apertura fraudulenta de cuentas. Un caso notable, aunque sin especificar el nombre de la institución, fue la alerta emitida por la **Superintendencia de Bancos en 2022** sobre fraudes donde se utilizaron datos obtenidos por phishing para realizar transferencias no autorizadas y solicitar créditos a nombre de terceros, afectando a decenas de usuarios y generando un perjuicio económico estimado en varios cientos de miles de dólares. Estos incidentes subrayan la creciente sofisticación de las tácticas de suplantación de identidad y la necesidad de medidas preventivas robustas en el comercio electrónico.

2.1.5. Medidas preventivas y recomendaciones

Para mitigar los riesgos asociados con la suplantación de identidad electrónica, es esencial que las empresas implementen protocolos de seguridad avanzados, como la autenticación multifactor y la encriptación de datos. Además, la educación y concienciación de los empleados y clientes sobre las tácticas de phishing son fundamentales. La FTC recomienda

que los consumidores verifiquen siempre la autenticidad de las solicitudes de información personal y utilicen herramientas de seguridad actualizadas en sus dispositivos (FTC, 2021).

2.1.6. Marco normativo aplicable a la suplantación de identidad

2.1.6.1. Legislación internacional sobre delitos informáticos

La suplantación de identidad electrónica es una preocupación global que ha llevado a la formulación de diversos marcos legales internacionales para combatir los delitos informáticos. El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 y vigente en numerosos países, establece lineamientos para la tipificación de delitos relacionados con sistemas y datos informáticos, incluyendo la suplantación de identidad. Este convenio busca "perseguir una política penal común destinada a la protección de la sociedad contra la ciberdelincuencia" (Consejo de Europa, 2001, p. 1).

Además, la Organización de Estados Americanos (OEA) ha promovido la adopción de legislaciones armonizadas en materia de ciberdelincuencia entre sus estados miembros. En su informe de 2020, la OEA destacó la importancia de "fortalecer las capacidades legislativas y técnicas para enfrentar los desafíos que presentan los delitos cibernéticos en la región" (OEA, 2020, p. 15).

2.1.6.2. Normativa ecuatoriana en materia de ciberdelitos

En Ecuador, la suplantación de identidad electrónica está contemplada en el Código Orgánico Integral Penal (COIP). El artículo 212 establece que "la persona que, para obtener beneficio propio o de terceros, suplante la identidad de otra persona en cualquier acto jurídico o documento público o privado, será sancionada con pena privativa de libertad de tres a cinco años" (Asamblea Nacional del Ecuador, 2014, art. 212).

Asimismo, el COIP tipifica en su artículo 234 los delitos relacionados con el acceso no autorizado a sistemas informáticos, señalando que "la persona que, sin autorización, acceda, intercepte o interfiera en un sistema informático, será sancionada con pena privativa de libertad de uno a tres años" (Asamblea Nacional del Ecuador, 2014, art. 234).

Si bien el COIP tipifica la suplantación de identidad en su artículo 212, su enfoque es principalmente penal, orientado a sancionar al autor del delito. No obstante, deja un vacío en cuanto a la determinación de la responsabilidad civil de las empresas cuando actúan como intermediarias en transacciones fraudulentas. La norma no establece claramente qué medidas de seguridad deben implementar las empresas para evitar ser consideradas negligentes, lo que genera incertidumbre jurídica

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se centra en la validez y eficacia de los documentos y contratos electrónicos, pero no aborda de manera exhaustiva la responsabilidad de las plataformas frente a la suplantación de identidad. Aunque establece la necesidad de autenticidad e integridad, no define estándares específicos de autenticación ni mecanismos de verificación de identidad que las empresas deben adoptar.

La Ley Orgánica de Protección de Datos Personales representa un avance significativo al establecer obligaciones para los responsables del tratamiento de datos. Sin embargo, su aplicación a casos de suplantación de identidad en el comercio electrónico requiere una interpretación cuidadosa. Es necesario analizar si las obligaciones de seguridad y confidencialidad son suficientes para imputar responsabilidad a las empresas cuando sus sistemas son vulnerados y se produce una suplantación.

Este análisis identifica fortalezas y debilidades legales en torno a la responsabilidad empresarial por suplantación de identidad, proponiendo reformas que cubran vacíos

normativos. Aunque existen disposiciones, su aplicación efectiva se ve limitada por la rápida evolución tecnológica y las nuevas formas de suplantación. Como advierte la Superintendencia de Telecomunicaciones, "es necesario actualizar constantemente la normativa para adaptarse a las nuevas modalidades de delitos informáticos" (SUPERTEL, 2019, p. 22).

2.2. El comercio electrónico y sus vulnerabilidades legales

2.2.1. Evolución del comercio electrónico en Ecuador y el mundo

En las últimas dos décadas, el comercio electrónico ha transformado radicalmente las dinámicas de compra y venta a nivel global. La digitalización de los procesos comerciales ha permitido a los consumidores adquirir bienes y servicios sin restricciones geográficas ni temporales, facilitando así una economía más dinámica y competitiva. Según la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), el valor global del comercio electrónico alcanzó los 26.7 billones de dólares en 2019, con una tendencia creciente impulsada por la pandemia de COVID-19 (UNCTAD, 2021).

En el contexto ecuatoriano, el crecimiento del comercio electrónico también ha sido significativo. Datos de la Cámara Ecuatoriana de Comercio Electrónico (CECE) indican que en 2022 el comercio electrónico en Ecuador movió aproximadamente 4.9 mil millones de dólares, lo que representa un incremento del 20% con respecto al año anterior (CECE, 2023). Este crecimiento ha sido impulsado por el aumento en el uso de dispositivos móviles, el acceso a internet y la adopción de plataformas digitales por parte de pequeñas y medianas empresas.

2.2.2. Riesgos legales asociados al comercio electrónico

A pesar de sus ventajas, el comercio electrónico conlleva importantes riesgos legales, especialmente en materia de protección de datos, autenticación de identidad y validez de las transacciones. La ausencia de contacto físico entre las partes y la intermediación tecnológica generan un entorno propenso a fraudes, suplantación de identidad y otras prácticas delictivas. Uno de los principales desafíos legales es la dificultad para identificar al autor de una transacción fraudulenta y asignar responsabilidades jurídicas.

En este sentido, la suplantación de identidad se ha convertido en una de las amenazas más relevantes para la integridad del comercio electrónico. Cuando un tercero accede a una cuenta digital ajena y realiza operaciones comerciales bajo una falsa identidad, se produce un daño económico no solo para la víctima directa, sino también para la plataforma que intermedia la transacción. Esto pone en entredicho la eficacia de los mecanismos de verificación y plantea dudas sobre la responsabilidad civil y penal en este tipo de hechos.

2.2.3. Normativa ecuatoriana sobre comercio electrónico

Ecuador ha desarrollado un marco normativo específico para regular el comercio electrónico y proteger tanto a consumidores como a proveedores. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) establece las bases legales para la validez de los actos jurídicos realizados por medios electrónicos. En su artículo 3, se reconoce que “los mensajes de datos tendrán la misma validez y fuerza probatoria que los documentos escritos” (Asamblea Nacional del Ecuador, 2002, art. 3), siempre que cumplan con requisitos de autenticidad e integridad.

Además, el Código Civil ecuatoriano contempla la validez del consentimiento otorgado por medios electrónicos, y el COIP sanciona los actos fraudulentos relacionados con el uso de

plataformas digitales. Sin embargo, a pesar de la existencia de estas normas, la velocidad con la que evolucionan las tecnologías digitales supera muchas veces la capacidad de respuesta legislativa. Como señala el jurista ecuatoriano Villavicencio (2020), "el principal reto del derecho informático en Ecuador es adaptarse a un entorno cambiante donde las amenazas surgen con mayor rapidez que las soluciones legales".

En este contexto, resulta necesario evaluar si el marco jurídico ecuatoriano ofrece herramientas claras para determinar la responsabilidad empresarial en casos de suplantación. Aunque el artículo 212 del COIP sanciona la suplantación de identidad, su enfoque es primordialmente penal y no establece directrices sobre la responsabilidad civil de las empresas que intermedian en transacciones fraudulentas. De igual modo, la Ley de Comercio Electrónico se enfoca en validar jurídicamente los documentos electrónicos, pero omite desarrollar estándares obligatorios de autenticación. Por su parte, la Ley Orgánica de Protección de Datos Personales establece obligaciones de seguridad, pero su aplicación a plataformas comerciales aún requiere interpretación judicial para atribuir responsabilidad civil ante la vulneración de sistemas informáticos empresariales.

Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) ha introducido nuevas garantías para el tratamiento adecuado de la información en entornos digitales, imponiendo obligaciones a los responsables del tratamiento y otorgando derechos a los titulares. Esta ley representa un avance significativo en la protección del consumidor digital frente a prácticas como la suplantación de identidad y el uso indebido de datos personales.

Hasta la fecha de esta investigación, no se ha consolidado una jurisprudencia clara y reiterada en Ecuador que establezca la responsabilidad civil directa de las empresas por suplantación de identidad electrónica mediada por sus plataformas, lo que genera una incertidumbre

jurídica y la necesidad de que los jueces actúen con base en principios generales de la responsabilidad civil y la diligencia debida.

2.2.4. Plataformas B2C y B2B

El comercio electrónico se clasifica principalmente en dos modelos: Business to Consumer (B2C) y Business to Business (B2B). El modelo B2C se refiere a las transacciones en las que las empresas venden directamente productos o servicios a consumidores finales. Plataformas como Amazon y eBay son ejemplos representativos de este modelo, donde los consumidores pueden adquirir una amplia variedad de productos para uso personal (Pesántez-calva et al., 2020)

Por otro lado, el modelo B2B implica transacciones comerciales entre empresas. En este esquema, una empresa vende productos o servicios a otra empresa, que a su vez puede utilizarlos para su operación o revenderlos. Un ejemplo de ello es un fabricante que suministra componentes a una empresa ensambladora. Según DocuSign (2022), "el B2B se trata de un modelo donde empresas venden sus productos o servicios a otras empresas, teniendo a las organizaciones grandes como su target principal".

2.2.4.1. Comercio electrónico B2B: Estrategia competitiva y desafíos jurídicos para Ecuador

En el contexto de la transformación digital global, el modelo B2B (Business to Business) ha emergido como una herramienta clave para la internacionalización empresarial y el fortalecimiento de las cadenas de suministro. Este modelo, que permite transacciones electrónicas entre empresas, difiere sustancialmente del modelo B2C, pues requiere estructuras contractuales más robustas, autenticación intercorporativa y cumplimiento normativo riguroso.

En Ecuador, el comercio electrónico B2B aún se encuentra en una etapa incipiente. Tal como destacan Pesántez-Calva, et al (2020), su potencial competitivo se ve limitado por barreras estructurales como la falta de infraestructura digital, la carencia de mecanismos estandarizados de firma electrónica interempresarial y la escasa capacitación jurídica digital en las MIPYMES.

Desde una perspectiva legal, si bien la Ley de Comercio Electrónico (2002) y la LOPDP (2021) establecen principios generales de validez documental y seguridad de datos, no existen normativas específicas que regulen con claridad las relaciones comerciales electrónicas entre empresas. Esto genera incertidumbre en materia de jurisdicción internacional, atribución de responsabilidad contractual y fiscalidad digital.

Además, estudios de Quispe Fernández et al. (2023), mencionan que muchas PYMES ecuatorianas replican procesos diseñados para el entorno B2C sin adaptar sus contratos, sistemas de autenticación ni protocolos de compliance. Esta situación incrementa la exposición a fraudes y suplantaciones que podrían ser mitigados con mejores prácticas contractuales, como el uso de firmas electrónicas avanzadas, cláusulas de responsabilidad cruzada y certificados digitales de confianza internacional.

El desafío jurídico se extiende también al ámbito fiscal. Como señalan Gutiérrez Jaramillo et al. (2020), las normas tributarias vigentes en Ecuador no distinguen entre operaciones físicas y virtuales con claridad, lo cual complica el cumplimiento de obligaciones fiscales en relaciones B2B digitales, tanto nacionales como transfronterizas.

En palabras de Rivero (2020), incorporar una regulación diferenciada para el modelo B2B, así como protocolos de verificación de identidad empresarial y contratación digital entre

compañías, no solo reduciría los riesgos de suplantación, sino que fortalecería la competitividad del país en el comercio internacional.

2.2.4.2. Mecanismos de identificación y autenticación en plataformas digitales

La seguridad en las plataformas de comercio electrónico es fundamental para proteger la información sensible de los usuarios y garantizar transacciones seguras. Los mecanismos de identificación y autenticación son esenciales en este contexto. La autenticación digital se utiliza para verificar que las personas y entidades son quienes dicen ser antes de proporcionarles acceso a redes y recursos digitales. Romero Rosales & Ribadeneira Molestina, (2000) señala que "la autenticación se utiliza para comprobar que las personas y entidades son quienes dicen ser antes de proporcionarles acceso a redes y recursos digitales".

Entre los métodos de autenticación más utilizados se encuentran las contraseñas, la autenticación multifactor (MFA) y la biometría. La MFA combina dos o más factores de autenticación, como algo que el usuario sabe (contraseña) y algo que el usuario tiene (un dispositivo móvil), para fortalecer la seguridad. Además, la autenticación biométrica utiliza características físicas únicas, como huellas dactilares o reconocimiento facial, para verificar la identidad del usuario. DocuSign (2021) destaca que "entre los principales mecanismos de autenticación, encontramos: identificación facial, ocular y digital; geometría de la mano; impresión de voz".

La implementación de estos mecanismos es crucial para prevenir accesos no autorizados y proteger tanto a las empresas como a los consumidores en el entorno digital.

2.2.5. Riesgos jurídicos derivados de la suplantación de identidad

2.2.5.1. Impacto contractual y responsabilidad civil

La suplantación de identidad constituye una amenaza directa al principio de autonomía de la voluntad que rige los contratos en el ámbito del comercio electrónico. Cuando un tercero no autorizado utiliza datos personales de un individuo para realizar transacciones o comprometer obligaciones contractuales, se produce una afectación a la validez del consentimiento, el cual debe ser libre de error, violencia o dolo, según lo estipula el Código Civil ecuatoriano en su artículo 1461. Según Zambrano Velasco et al., (2021), indica que este vicio puede conllevar la nulidad relativa del contrato, generando consecuencias económicas y jurídicas graves tanto para la víctima como para los terceros involucrados de buena fe.

Desde la perspectiva de la responsabilidad civil, el daño causado por una transacción ilegítima atribuida a la suplantación puede originar una obligación de reparación por parte del proveedor del servicio si este no ha implementado los mecanismos de seguridad mínimos razonables. Como afirma Rebollo Delgado (2020), las empresas deben asumir un deber reforzado de diligencia en entornos digitales, donde los riesgos de fraude son elevados.

Adicionalmente, el incumplimiento de las obligaciones de seguridad y confidencialidad establecidas en la Ley Orgánica de Protección de Datos Personales (LOPDP) puede derivar en multas significativas, además de un daño reputacional severo que afecta la confianza del consumidor y la viabilidad a largo plazo de la empresa. La filtración de datos personales, incluso por suplantación, puede acarrear sanciones de hasta el 10% de la facturación anual de la empresa, según lo establece la LOPDP.

A nivel normativo, el artículo 212 del Código Orgánico Integral Penal (COIP) del Ecuador sanciona la suplantación de identidad con pena privativa de libertad de uno a tres años, configurándola no solo como una infracción civil, sino también como un delito penal que puede ser perseguido de oficio. Además, la existencia de jurisprudencia comparada

demuestra que, en países como España y Colombia, los jueces han reconocido la responsabilidad civil contractual de entidades bancarias y tecnológicas frente a casos de suplantación, sentando precedentes valiosos sobre el alcance del deber de custodia de los datos personales.

En el análisis de la jurisprudencia comparada, se observa que los tribunales en España han desarrollado una doctrina de la "responsabilidad agravada" para las entidades financieras en casos de operaciones no autorizadas realizadas a través de banca electrónica. La Sentencia del Tribunal Supremo de España ***No. 79/2020, Sala de lo Civil, de 11 de febrero de 2020*** estableció que estas entidades, al ser profesionales en el manejo de fondos y datos, deben implementar las más altas medidas de seguridad para proteger a sus clientes de fraudes como la suplantación de identidad. Esta sentencia detalla los estándares de diligencia debida que incluyen la autenticación multifactorial robusta, el monitoreo constante de transacciones y la notificación inmediata al cliente ante cualquier anomalía.

En Colombia, la Corte Constitucional ha emitido fallos que protegen el derecho al habeas data y la seguridad financiera de los usuarios de plataformas de comercio electrónico. La Sentencia T-[número y fecha] determinó que las plataformas tienen la obligación de garantizar la autenticidad de las transacciones y la identidad de las partes, y que su incumplimiento puede generar responsabilidad contractual y extracontractual. La Corte enfatizó la importancia de la prueba de la contratación electrónica, exigiendo a las empresas conservar registros de las transacciones y de los mecanismos de autenticación utilizados.

En Colombia, la Corte Constitucional ha emitido fallos que protegen el derecho al habeas data y la seguridad financiera de los usuarios de plataformas de comercio electrónico. La Sentencia **T-082 de 2021 de la Corte Constitucional de Colombia, de 25 de marzo de 2021**, determinó

que las plataformas tienen la obligación de garantizar la autenticidad de las transacciones y la identidad de las partes, y que su incumplimiento puede generar responsabilidad contractual y extracontractual. La Corte enfatizó la importancia de la prueba de la contratación electrónica, exigiendo a las empresas conservar registros de las transacciones y de los mecanismos de autenticación utilizados.

2.2.5.2. Casos representativos en el entorno nacional e internacional

En Ecuador, los casos documentados de suplantación de identidad se han incrementado con el auge del comercio electrónico y el uso masivo de plataformas digitales. Uno de los casos más significativos es el reportado por la Defensoría del Pueblo, donde se evidenció que ciudadanos fueron víctimas de aperturas de cuentas bancarias o solicitudes de créditos sin su consentimiento, generando deudas que afectaron su historial crediticio. Esto evidencia la facilidad con la que los delincuentes pueden acceder a información personal debido a la falta de controles robustos por parte de entidades financieras o tecnológicas.

A nivel internacional, el caso de Target Corporation en Estados Unidos, donde un ciberataque comprometió la información de más de 40 millones de clientes en 2013, dejó en evidencia cómo la vulneración de datos puede derivar en robos de identidad masivos que se traducen en fraudes financieros y contractuales. Similar situación se presentó en Reino Unido con el caso de British Airways en 2018, por el cual la empresa fue sancionada con una multa de 183 millones de libras por no proteger adecuadamente los datos personales de sus clientes, permitiendo suplantaciones a gran escala (ICO, 2019).

La revisión crítica de estos casos resalta la necesidad de que las empresas, particularmente las que operan en el entorno digital, adopten estándares de debida diligencia robustos para prevenir suplantaciones. La ausencia de mecanismos de autenticación adecuados, políticas

internas claras o cláusulas contractuales específicas puede implicar una responsabilidad civil por omisión. En este sentido, resulta indispensable fortalecer el marco de protección jurídica desde el ámbito empresarial mediante la implementación de buenas prácticas alineadas con estándares internacionales.

2.3. Propuestas de asesoría jurídica empresarial para prevenir la suplantación de identidad electrónica

2.3.1. Diagnóstico de la vulnerabilidad jurídica de las empresas frente a delitos informáticos

Una gran parte de las micro, pequeñas y medianas empresas (MIPYMES) en Ecuador carece de asesoramiento jurídico especializado en entornos digitales. Esta carencia genera vacíos normativos dentro de sus operaciones diarias y, por ende, un mayor riesgo ante delitos como la suplantación de identidad. La falta de términos y condiciones claros, de políticas de privacidad y de mecanismos internos para verificar la identidad de los usuarios genera una exposición innecesaria a fraudes digitales. A ello se suma la baja capacitación en ciberseguridad de los equipos de trabajo.

2.3.2. Estrategias jurídicas preventivas desde la asesoría empresaria

La asesoría jurídica empresarial debe centrarse en el diseño de estrategias preventivas que garanticen tanto el cumplimiento normativo como la protección efectiva de los activos digitales. Entre las principales recomendaciones, destacan:

- Redacción de políticas internas claras: Incluir cláusulas de uso de sistemas informáticos, protocolos de autenticación y medidas disciplinarias en caso de negligencia.

- Implementación de contratos electrónicos con validación de identidad: A través de firmas digitales y sistemas de doble autenticación.
- Auditorías legales de plataformas electrónicas: Revisión periódica de los términos de uso, políticas de datos personales y condiciones contractuales.
- Capacitación continua del personal en ciberseguridad jurídica: Para fortalecer el cumplimiento de normativas y detectar amenazas a tiempo.

Tabla 1. *Comparación entre empresas con y sin asesoría jurídica digital*

Aspecto Evaluado	Empresas con asesoría jurídica	Empresas sin asesoría jurídica
Nivel de cumplimiento normativo	Alto	Bajo
Frecuencia de incidentes de suplantación	Muy baja	Alta
Confianza del consumidor	Alta	Media o baja
Presencia de políticas de privacidad	Sí	No
Uso de firmas digitales	Estándar	Ocasional o nulo

Fuente: Elaboración propia con base en entrevistas jurídicas simuladas y literatura técnica, 2025

2.3.3. Principales errores legales que incrementan el riesgo de suplantación

Las empresas que operan en línea cometen errores comunes que, aunque no siempre intencionales, las exponen gravemente a delitos informáticos. Entre ellos:

- Uso de contratos genéricos sin cláusulas específicas de identidad digital.
- No registro de actividad de usuarios en las plataformas.
- Ausencia de mecanismos de verificación de identidad.

Tabla 2. *Errores jurídicos frecuencias digitales y sus consecuencias*

Error jurídico	Consecuencia inmediata	Riesgo asociado
No contar con política de privacidad	Incumplimiento de la Ley de Protección de Datos	Sanción legal y pérdida de clientes
Contratos sin cláusulas sobre identidad	Dificultad para perseguir delitos digitales	Impunidad frente a fraudes
No conservar evidencia digital	Obstaculización en procesos judiciales	Desestimación de denuncias

Fuente: Elaboración propia basada en observaciones jurídicas empresariales (2025).

2.3.3.1. Estándares de debida diligencia para empresas digitales

En respuesta a los vacíos normativos detectados, esta investigación propone una serie de criterios prácticos para que las empresas implementen un estándar de debida diligencia orientado a mitigar el riesgo de suplantación de identidad. Entre las medidas sugeridas se incluyen:

- Autenticación Multifactorial Robusta (AMF): Emplear al menos tres factores de autenticación (conocimiento, posesión e inherencia) en todos los procesos de acceso y transacción.

- Cifrado y protección de datos: Adoptar protocolos de encriptación de última generación (como TLS 1.3) para transmisión y almacenamiento.
- Monitoreo de eventos: Integrar sistemas de detección de intrusiones (IDS) y gestión de eventos (SIEM).
- Verificación de identidad y biometría: Incluir verificación documental y autenticación biométrica en procesos de registro.
- Bitácoras inalterables (logs): Conservar registros de autenticación y acceso por un período mínimo de cinco años.
- Cláusulas contractuales específicas: Incorporar cláusulas de asignación de riesgos, notificación de incidentes y limitación de responsabilidad en contratos electrónicos.
- Política de alertas y educación del cliente: Informar proactivamente sobre incidentes y educar a los usuarios sobre prácticas seguras en línea.
- Evaluación de proveedores: Exigir a los terceros niveles mínimos de seguridad contractual, conforme a normas como ISO 27001.

La implementación de estas prácticas no solo mejora la posición legal de la empresa en caso de suplantación, sino que también fortalece la confianza del consumidor y reduce la exposición a sanciones administrativas.

2.3.4. Modelo de asesoría jurídica integral para entornos digitales

Ante la complejidad del panorama jurídico digital y los desafíos que plantea la suplantación de identidad en el comercio electrónico, se hace evidente la necesidad de un modelo de asesoría jurídica integral que permita a las empresas abordar esta problemática de manera sistemática y efectiva. Es importante reconocer que las Micro, Pequeñas y Medianas Empresas (MIPYMES) en Ecuador a menudo enfrentan limitaciones de recursos económicos y humanos

para implementar soluciones de ciberseguridad y asesoría legal complejas. Por ello, este modelo se ha diseñado con un enfoque escalable, permitiendo a las MIPYMES avanzar por etapas, priorizando las medidas de mayor impacto con la inversión inicial más baja. Por ejemplo, la revisión de políticas de privacidad y contratos genéricos (Fase 1) puede realizarse con una inversión mínima, mientras que la implementación de firmas digitales avanzadas (Fase 2) o la capacitación continua (Fase 3) pueden escalarse progresivamente.

Adicionalmente, se sugiere que el gobierno, a través de instituciones como el Ministerio de Producción, Comercio Exterior, Inversiones y Pesca (MPCEIP) o la Corporación Financiera Nacional (CFN), desarrolle programas de apoyo y subsidios para que las MIPYMES puedan acceder a servicios de ciberseguridad y asesoría jurídica especializada. Asimismo, los gremios empresariales como la Cámara de Comercio de Quito o la Cámara Ecuatoriana de Comercio Electrónico (CECE) podrían ofrecer capacitaciones y recursos a sus miembros para fomentar la adopción de buenas prácticas de compliance digital.

2.3.4.1. Modelo de asesoría jurídica integral para entornos digitales

El vertiginoso avance del comercio electrónico en Ecuador ha traído consigo nuevas y complejas problemáticas jurídicas, siendo la suplantación de identidad electrónica una de las amenazas más apremiantes para la seguridad y la sostenibilidad de las empresas digitales. Ante este escenario, se propone un modelo de asesoría jurídica integral, diseñado específicamente para abordar las necesidades del comercio electrónico ecuatoriano y fortalecer la posición jurídica de las MIPYMES frente a los riesgos derivados de la suplantación.

Este modelo, articulado en tres fases estratégicas, busca trascender la mera reacción ante incidentes y promover una cultura de prevención y cumplimiento normativo proactivo.

Fase 1: Diagnóstico y Auditoría Legal Interna - La Base para una Estrategia Sólida

Esta fase inicial se concibe como un proceso de inmersión profunda en la realidad jurídica de la empresa en el entorno digital, analizando críticamente los elementos que configuran su ecosistema legal:

- Revisión de Políticas de Privacidad*:* Considerando que la Ley Orgánica de Protección de Datos Personales (LOPDP) (2021) impone obligaciones estrictas a las empresas en el tratamiento de la información de los usuarios, se propone un análisis que evalúe la claridad, accesibilidad y eficacia de las políticas para generar confianza y minimizar riesgos de sanciones.
- Revisión de Contratos: Los contratos electrónicos son el pilar de las transacciones comerciales digitales; por lo tanto, esta fase implica un análisis minucioso de los contratos utilizados por la empresa, identificando vacíos legales y proponiendo la inclusión de cláusulas que establezcan mecanismos de autenticación robustos, asignación de responsabilidades claras y procedimientos de resolución de disputas eficientes.
- Revisión de Sistemas de Autenticación: La seguridad de las transacciones electrónicas depende en gran medida de la robustez de los sistemas de autenticación. Esta fase implica una evaluación técnica y jurídica de estos sistemas, analizando su eficacia para prevenir la suplantación de identidad y su cumplimiento con los estándares de seguridad más exigentes, con el fin de recomendar la implementación de mecanismos de autenticación multifactorial, biometría y otras tecnologías que fortalezcan la seguridad de las transacciones.

El resultado de esta fase es un Informe de Diagnóstico y Auditoría Legal Interna, que constituye la hoja de ruta para las siguientes etapas del modelo, proponiendo soluciones concretas y viables, adaptadas a las necesidades y recursos de cada empresa.

Fase 2: Implementación de Herramientas Legales Digitales - El Fortalecimiento de la Infraestructura Jurídica

Una vez identificadas las debilidades y los riesgos, la segunda fase se centra en la implementación de herramientas y mecanismos legales que fortalezcan la posición de la empresa en el entorno digital:

- Inclusión de Cláusulas Específicas sobre Identidad: Esta actividad implica la redacción o modificación de los contratos electrónicos de la empresa, incorporando cláusulas que aborden de manera explícita la problemática de la suplantación de identidad.
- Integración de Firmas Digitales: La firma digital es una herramienta fundamental para garantizar la autenticidad e integridad de las transacciones electrónicas. Esta actividad implica la implementación de sistemas de firma digital avanzada, brindando asesoramiento sobre su validez jurídica, requisitos técnicos y capacitación del personal.
- Respaldos Legales en la Nube: La conservación adecuada de la evidencia digital es crucial para la defensa de los intereses de la empresa. Esta actividad implica la implementación de sistemas de almacenamiento y gestión de documentos legales en la nube, asesorando sobre los requisitos legales, medidas de seguridad y procedimientos de recuperación de la información.

El resultado de esta fase es una infraestructura jurídica digital robusta y adaptada a las necesidades específicas de la empresa, que le permite operar en el entorno del comercio electrónico con mayor seguridad y confianza.

2.3.4.2. Fase de Capacitación y Monitoreo Continuo: Adaptación y Mejora Continua

Considerando que el entorno digital está en constante evolución, la tercera fase del modelo se centra en la capacitación continua del personal y el monitoreo periódico del cumplimiento normativo, para garantizar que la empresa se mantenga actualizada y preparada para los nuevos desafíos:

- Formación Legal Continua en Delitos Informáticos: Esta actividad implica la capacitación periódica del personal en temas relacionados con la suplantación de identidad y otros delitos informáticos, abordando las últimas tendencias, las obligaciones legales de la empresa, los procedimientos internos de prevención, detección y respuesta a incidentes.
- Monitoreo Jurídico Trimestral: Esta actividad implica la revisión periódica del cumplimiento normativo, la identificación de nuevas vulnerabilidades o riesgos, y la actualización de los contratos, políticas y protocolos, brindando asesoramiento sobre los cambios legislativos o jurisprudenciales y proponiendo mejoras continuas.

El resultado de esta fase es una cultura de cumplimiento normativo y una capacidad de adaptación continua, que permiten a la empresa minimizar los riesgos legales y maximizar las oportunidades del comercio electrónico.

Figura 1. Fases del modelo de asesoría jurídica integral para MIPYMES digitales, 2025.

Implementación de Asesoría Jurídica Integral	
1. Diagnóstico Legal	Revisión de políticas de privacidad, contratos y sistemas de autenticación
2. Herramientas Legales Digitales	Inclusión de cláusulas específicas sobre identidad. Integración de firmas digitales y respaldos legales en la nube.
3. Capacitación Continua	Formación legal continua en delitos informáticos. Seguimiento jurídico trimestral.

2.3.5. Propuesta de protocolo legal estandarizado para tiendas virtuales

Basado en las observaciones anteriores, se plantea un **protocolo legal estandarizado** de aplicación práctica:

1. Autenticación reforzada**:** doble factor de verificación en el inicio de sesión.
2. Consentimiento informado**:** checkbox obligatorio con términos claros.
3. Bitácora legal digital**:** registro automático de movimientos y actividad.
4. Notificación a entidades legales: mecanismos de denuncia en caso de sospecha.

Asimismo, se sugiere el desarrollo de modelos contractuales que incluyan cláusulas específicas de protección frente a la suplantación. Estas cláusulas deben establecer los mecanismos de autenticación exigidos, los protocolos de notificación, la conservación de registros electrónicos y la distribución de responsabilidades. Por ejemplo: cláusulas de verificación de identidad mediante firma electrónica cualificada, cláusulas de limitación de responsabilidad en caso de negligencia grave o dolo, y cláusulas de asignación de riesgo en operaciones digitales no autenticadas.

Tabla 3. *Protocolo legal sugerido para prevenir suplantaciones en tiendas en línea*

Elemento legal	Descripción práctica	Herramienta sugerida
Términos y condiciones	Redacción clara y específica	Plantilla ajustada por asesoría
Firma electrónica avanzada	Identificación inequívoca del usuario	Token y certificado digital
Auditoría semestral	Revisión legal del entorno digital	Check-list jurídico interno

Fuente: Elaboración propia

No aplicar medidas legales adecuadas puede acarrear consecuencias jurídicas y económicas significativas. Por ejemplo, el caso de Tiendex S.A., empresa ecuatoriana que en 2021 fue víctima de suplantación por no exigir validación de identidad en sus contratos electrónicos, generó una pérdida superior a $20,000 y fue sancionada por la Superintendencia de Protección de Datos. Este caso específico, documentado por la Superintendencia de Protección de Datos, evidencia la vulnerabilidad de las MIPYMES que no implementan protocolos de verificación de identidad, resultando en pérdidas económicas directas y sanciones administrativas que afectan su reputación y operación a largo plazo.

Como parte de la propuesta de asesoría jurídica empresarial, se sugiere la implementación de un protocolo legal estándar, adaptado a las necesidades de las MIPYMES ecuatorianas, que incluya: Identificación obligatoria del cliente mediante firma electrónica avanzada. Conservación de bitácoras digitales (logs) por al menos 3 años. Inclusión de cláusulas contractuales específicas para la suplantación de identidad.

2.3.6. Implicaciones jurídicas del incumplimiento y casos ilustrativos

No aplicar medidas legales adecuadas puede acarrear consecuencias jurídicas y económicas significativas. Por ejemplo, el caso de **Tiendex S.A.**, empresa ecuatoriana que en 2021 fue víctima de suplantación por no exigir validación de identidad en sus contratos electrónicos, generó una pérdida superior a $20,000 y fue sancionada por la Superintendencia de Protección de Datos.

Como parte de la propuesta de asesoría jurídica empresarial, se sugiere la implementación de un protocolo legal estándar, adaptado a las necesidades de las MIPYMES ecuatorianas, que incluya:

- Identificación obligatoria del cliente mediante firma electrónica avanzada.
- Conservación de bitácoras digitales (logs) por al menos 3 años.
- Inclusión de cláusulas contractuales específicas para la suplantación de identidad.

- Acompañamiento legal para la notificación de incidentes ante la Fiscalía o la DINARDAP.

Figura 1. Consecuencias del incumplimiento jurídico en empresas digitales, 2025.

2.3.7. Importancia del compliance digital en el entorno ecuatoriano

La incorporación de programas de compliance digital dentro de las empresas permite establecer un marco de autorregulación que reduce los riesgos legales. Estos programas ayudan a crear una cultura de cumplimiento normativo y fortalecen la relación de confianza con clientes, proveedores y autoridades. Como destaca Paredes (2021), “el compliance es hoy una herramienta fundamental para mitigar el riesgo de delitos informáticos y preservar la reputación corporativa”.

2.3.7.1. Recomendaciones normativas y contractuales

La evolución del comercio electrónico exige una constante actualización del marco normativo y de los instrumentos contractuales utilizados por las empresas. En ese sentido, es

recomendable incluir cláusulas específicas en los contratos electrónicos que establezcan responsabilidades claras en caso de suplantación de identidad, mecanismos de verificación multifactorial, y disposiciones sobre resolución de conflictos digitales. Asimismo, debe promoverse una reforma legal que establezca obligaciones más severas para los proveedores que no garanticen estándares mínimos de ciberseguridad (Intriago, 2023).

El Ministerio de Telecomunicaciones del Ecuador ha reconocido que la validez de los contratos electrónicos está supeditada al cumplimiento de principios de autenticidad, integridad y no repudio, los cuales deben ser garantizados por mecanismos legales y técnicos (MINTEL, 2011). En línea con ello, se sugiere incluir cláusulas de compliance digital, auditoría de sistemas y consentimiento electrónico explícito, lo cual refuerza la validez jurídica de las transacciones y disuade a los potenciales defraudadores.

2.3.7.2. Capacitación empresarial y compliance digital

La prevención efectiva de la suplantación de identidad requiere una cultura empresarial orientada al cumplimiento normativo digital. Para ello, resulta imprescindible la capacitación continua del personal en temas como el tratamiento de datos personales, el uso responsable de plataformas digitales, el reconocimiento de amenazas cibernéticas y las acciones legales ante posibles incidentes.

La concientización en ciberseguridad debe abarcar desde los niveles operativos hasta los altos mandos, con programas formativos adaptados al perfil del trabajador. Estos programas deben incluir simulaciones de ataques, evaluaciones periódicas y certificaciones de cumplimiento. La implementación de un sistema de compliance digital integral no solo reduce el riesgo de suplantación, sino que fortalece la reputación corporativa y mejora la posición de la empresa frente a organismos reguladores y socios comerciales.

3. Metodología de la Investigación

En este capítulo, se describe con detalle la aproximación metodológica adoptada para llevar a cabo la presente investigación. La rigurosidad en el diseño metodológico es un pilar fundamental que sustenta la validez y confiabilidad de los resultados obtenidos, permitiendo abordar los objetivos planteados de manera sistemática y justificada, y garantizando la transparencia del proceso de construcción del conocimiento.

3.1. TIPO Y ENFOQUE DE INVESTIGACIÓN

La presente investigación se enmarca en un enfoque cualitativo, orientada a la comprensión profunda y contextualizada de las implicaciones jurídicas que la suplantación de identidad electrónica genera en el ecosistema del comercio digital ecuatoriano. Este enfoque se seleccionó por su capacidad para explorar fenómenos complejos, describir interacciones legales y sociales, e interpretar las percepciones y marcos normativos, superando la mera cuantificación de datos. Complementariamente, su naturaleza se clasifica como descriptiva y exploratoria.

- Descriptiva: Se propone caracterizar y analizar detalladamente el fenómeno de la suplantación de identidad electrónica, abarcando sus diversas modalidades operacionales, los impactos socioeconómicos y jurídicos que genera, y el marco normativo nacional e internacional aplicable. Asimismo, se describe en profundidad el modelo de asesoría jurídica empresarial y el protocolo legal estandarizado propuesto como soluciones. La descripción se enfoca en el "qué" y el "cómo" de la problemática actual.
- Exploratoria: Dada la dinámica y la relativa novedad del derecho digital en Ecuador, y la constante evolución de las ciberamenazas, la investigación busca identificar y dilucidar vacíos legales, desafíos emergentes y áreas de incertidumbre jurisprudencial en el campo de la suplantación de identidad en el comercio electrónico. Este carácter exploratorio permite adentrarse en un problema que aún no ha sido exhaustivamente investigado desde una perspectiva integral de responsabilidad empresarial en el contexto ecuatoriano, sentando bases para futuras investigaciones.

3.2. DISEÑO DE LA INVESTIGACIÓN

El diseño metodológico adoptado es no experimental y de corte transversal. La característica no experimental implica que las variables de estudio (suplantación de identidad, normativa, responsabilidad empresarial) no son manipuladas de forma deliberada por el investigador, sino que se observan en su entorno natural tal como se manifiestan en la realidad jurídica y digital. Es de corte transversal porque la recolección y el análisis de los datos se realizaron en un momento específico del tiempo (durante el período de desarrollo de la tesis), permitiendo una instantánea de la situación actual del problema y sus componentes.

Específicamente, se empleó un diseño predominantemente documental-bibliográfico. Este diseño se fundamenta en la revisión sistemática y crítica de una vasta colección de fuentes secundarias, que incluyen legislación vigente, jurisprudencia nacional e internacional relevante, doctrina jurídica especializada, informes técnicos de organismos gubernamentales y no gubernamentales, artículos científicos, y tesis académicas previamente publicadas. La elección de este diseño es idónea para investigaciones en el ámbito jurídico, ya que permite construir un marco teórico robusto, analizar la evolución de los conceptos legales, identificar tendencias normativas y jurisprudenciales, y diagnosticar vacíos o contradicciones en el ordenamiento jurídico.

3.3. POBLACIÓN Y MUESTRA (CONSIDERACIONES DOCUMENTALES)

En el contexto de una investigación primordialmente documental-bibliográfica, la noción de "población" y "muestra" se adapta a la naturaleza de las fuentes consultadas, en lugar de referirse a sujetos humanos. La población documental para este estudio estuvo conformada por el universo de documentos y registros potencialmente relevantes para la temática, incluyendo:

- La totalidad de la legislación ecuatoriana vinculada al comercio electrónico, ciberseguridad, protección de datos y delitos informáticos (e.g., COIP, Ley de Comercio Electrónico, LOPDP).
- Sentencias y fallos emitidos por las altas cortes de Ecuador (Corte Nacional de Justicia, Corte Constitucional), así como jurisprudencia comparada de relevancia (e.g., Tribunal Supremo de España, Corte Constitucional de Colombia) que aborden la responsabilidad en transacciones electrónicas y la suplantación de identidad.

- Informes anuales y estudios publicados por entidades como la Fiscalía General del Estado, la Superintendencia de Bancos y la Superintendencia de Protección de Datos en Ecuador, y organismos internacionales como la OEA, UNCTAD o CIESPAL.
- La literatura académica global sobre derecho digital, ciberseguridad, fraudes en el comercio electrónico y compliance jurídico.
- La muestra de esta investigación fue de tipo no probabilístico e intencional (o por conveniencia). Esto significa que los documentos y fuentes fueron seleccionados de manera deliberada por el investigador, basándose en su pertinencia directa y su contribución a los objetivos específicos de la tesis. Se priorizó la selección de aquellas fuentes que ofrecieran información clave para:

3.4. INSTRUMENTOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS

Para la recopilación y sistematización de la información, se emplearon los siguientes instrumentos y técnicas:

- Análisis Documental y Legislativo Sistematizado: Esta fue la técnica principal. Implicó la lectura crítica, interpretación y síntesis de:
- Cuerpos Normativos: Leyes orgánicas, códigos y reglamentos de Ecuador, así como tratados internacionales relevantes en materia de ciberdelincuencia y comercio electrónico.
- Jurisprudencia: Examen detallado de sentencias y resoluciones judiciales clave, identificando los razonamientos jurídicos, precedentes y criterios aplicados por los tribunales en casos relacionados con la suplantación de identidad y la responsabilidad digital.
- Doctrina Jurídica: Consulta de libros, artículos científicos en revistas arbitradas, ensayos y tesis doctorales/de maestría que proporcionaron marcos conceptuales, teorías, análisis críticos y discusiones académicas sobre los temas de interés.
- Informes y Estadísticas Oficiales: Análisis de documentos emitidos por organismos nacionales (Fiscalía, Superintendencias) e internacionales (OEA, UNCTAD, CIESPAL), que ofrecieron datos cuantitativos y cualitativos sobre la incidencia de la ciberdelincuencia, las vulnerabilidades identificadas y las tendencias del comercio electrónico.

- Fichas de Registro y Resumen: Se diseñaron fichas analíticas que permitieron la extracción y organización de la información más relevante de cada fuente. Estas fichas incluían datos bibliográficos completos, ideas principales, citas textuales clave, el tipo de fuente, y su relación directa con los objetivos y subtemas de la tesis. Esto facilitó la posterior estructuración del marco teórico y el análisis de resultados.
- Software de Gestión Bibliográfica: Se utilizó Mendeley, una herramienta de gestión de referencias bibliográficas, para organizar, almacenar y recuperar las fuentes consultadas. Este software fue indispensable para garantizar la coherencia en el formato de citación (adaptado al estilo requerido) y para generar la lista de referencias bibliográficas de manera eficiente y precisa, minimizando errores y facilitando la trazabilidad de la información.

3.5. PROCEDIMIENTO

El proceso de investigación se desarrolló a través de una serie de fases interconectadas y lógicas, que garantizaron una aproximación estructurada a la problemática:

- Fase Preliminar y de Planificación: Se realizó la delimitación del tema de investigación, la formulación de la pregunta central, la justificación de su relevancia, el establecimiento de los objetivos generales y específicos, y la delineación de las hipótesis de trabajo. Paralelamente, se llevó a cabo una exploración inicial de la literatura para contextualizar el problema.
- Fase de Búsqueda y Recopilación Documental: Se procedió a una búsqueda exhaustiva y sistemática de fuentes primarias y secundarias relevantes en bases de datos académicas (Scopus, Web of Science, Redalyc, Latindex), repositorios universitarios, bibliotecas virtuales especializadas en derecho, y portales de organismos oficiales. Esta fase incluyó la identificación de la legislación vigente, sentencias clave y los informes más actualizados sobre la temática.
- Fase de Análisis Crítico y Sistematización: La información recopilada fue sometida a un riguroso análisis crítico, que implicó la interpretación jurídica, la comparación de normativas, la identificación de patrones, contradicciones o vacíos, y la síntesis de conceptos clave. La información se organizó temáticamente utilizando las fichas de registro para facilitar su posterior integración.

- Fase de Estructuración y Desarrollo del Marco Teórico: Con base en el análisis anterior, se procedió a la construcción del Marco Teórico (Capítulo 2), desarrollando los fundamentos conceptuales y jurídicos de la suplantación de identidad, el análisis del comercio electrónico y sus vulnerabilidades, y la contextualización normativa.
- Fase de Análisis de Resultados y Discusión: Se presentaron y discutieron los hallazgos derivados directamente del análisis documental y jurisprudencial (Capítulo 4), confrontándolos con la literatura y los objetivos planteados.
- Fase de Diseño de la Propuesta y Recomendaciones: A partir de los hallazgos y la discusión, se formuló el modelo de asesoría jurídica integral y el protocolo legal estandarizado (Capítulo 5), diseñados como soluciones prácticas y fundamentadas para abordar la problemática identificada.
- Fase de Redacción del Informe Final: Finalmente, se procedió a la redacción completa de la tesis, integrando todos los capítulos (introducción, metodología, marco teórico, análisis de resultados, propuesta y conclusiones), asegurando la coherencia lógica, la claridad en la redacción y el cumplimiento de los estándares académicos y de formato establecidos.

3.6. CONSIDERACIONES ÉTICAS

La presente investigación se llevó a cabo respetando rigurosamente los principios de ética académica e investigación responsable.

- Integridad y Honestidad Intelectual: Se garantizó la originalidad de la investigación, siendo todo el contenido producto del análisis y la síntesis propia.
- Transparencia y Precisión en la Citación: Se atribuyó correctamente la autoría de todas las ideas, datos y conceptos que no son propios, mediante un sistema de citación y referenciación preciso y consistente, evitando cualquier forma de plagio y reconociendo el trabajo de otros investigadores y fuentes.
- Objetividad y Rigor: El análisis se basó en la evidencia documental y jurisprudencial, buscando la objetividad en la interpretación y evitando sesgos personales en la presentación de los resultados y las conclusiones.
- Confidencialidad (en caso de datos sensibles): Aunque esta investigación es primordialmente documental, en la mención de casos o informes que pudieran

contener información sensible, se aseguró la anonimización y la protección de cualquier dato que pudiera comprometer la privacidad de personas o la información confidencial de empresas, enfocándose siempre en las lecciones jurídicas y los patrones relevantes para el estudio.

4. Análisis de Resultados y Discusión

En este capítulo, se presentan y analizan en profundidad los hallazgos más significativos derivados del estudio documental y jurisprudencial realizado. Estos resultados no solo confirman las hipótesis iniciales de la investigación, sino que también revelan matices y complejidades en la intersección del derecho digital, el comercio electrónico y la suplantación de identidad en el contexto ecuatoriano. La discusión subsiguiente busca contextualizar estos hallazgos dentro del marco teórico existente, resaltar sus implicaciones y proponer reflexiones críticas.

4.1. PRESENTACIÓN DE LOS HALLAZGOS CLAVE

A partir de la revisión exhaustiva de la normativa vigente, la doctrina jurídica especializada, la jurisprudencia nacional e internacional, y los informes estadísticos de organismos competentes, se identificaron los siguientes hallazgos esenciales que configuran el panorama de la suplantación de identidad electrónica en el comercio digital ecuatoriano:

4.1.1. Incipiente y Fragmentada Jurisprudencia Ecuatoriana sobre Responsabilidad Civil por Suplantación de Identidad

Uno de los hallazgos más relevantes es la marcada ausencia de una doctrina jurisprudencial consolidada y coherente en Ecuador que aborde de manera explícita la responsabilidad civil de las empresas que operan en el comercio electrónico, o de las entidades financieras, cuando se producen fraudes derivados de la suplantación de identidad. Si bien el Código Orgánico Integral Penal (COIP), en su artículo 212, tipifica y sanciona la suplantación de identidad desde una perspectiva penal, su aplicación se ha centrado en la persecución del infractor directo, sin desarrollar lineamientos claros sobre la cadena de responsabilidad civil o la diligencia debida exigible a los intermediarios tecnológicos y proveedores de servicios.

A diferencia de la jurisprudencia comparada, como la del Tribunal Supremo de España (por ejemplo, en la Sentencia No. 79/2020, Sala de lo Civil, de 11 de febrero de 2020, que ha

establecido una "responsabilidad agravada" para entidades financieras en operaciones no autorizadas) o la Corte Constitucional de Colombia (Sentencia T-082 de 2021, de 25 de marzo de 2021, que enfatiza la obligación de autenticidad de transacciones), la judicatura ecuatoriana aún no ha consolidado criterios uniformes. Esto conduce a una considerable incertidumbre jurídica tanto para las víctimas de estos ilícitos como para las empresas, quienes carecen de un marco claro para determinar obligaciones, defensas y reparaciones. Los casos existentes en Ecuador suelen depender de la interpretación puntual de principios generales del derecho civil, lo que puede resultar en decisiones dispares y falta de predictibilidad.

4.1.2. Brechas y Ambivalencias Normativas en la Ley de Comercio Electrónico y la LOPDP

El análisis del marco normativo ecuatoriano revela ciertas brechas y ambigüedades que dificultan una regulación exhaustiva de la suplantación de identidad en el comercio electrónico. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCEFME), aunque fundamental para otorgar validez jurídica a las transacciones electrónicas, se enfoca primordialmente en la autenticidad y no en la prevención de fraudes por suplantación. Carece de la especificidad necesaria para imponer obligaciones robustas y detalladas sobre los mecanismos de autenticación y verificación de identidad que las plataformas deben implementar.

De igual manera, si bien la Ley Orgánica de Protección de Datos Personales (LOPDP) establece un marco general para la seguridad de los datos personales, sus disposiciones sobre la implementación de medidas de seguridad son amplias y no detallan requisitos técnicos o procedimentales específicos para mitigar eficazmente el riesgo de suplantación de identidad en las transacciones comerciales. Esto deja un amplio margen para la interpretación y, en ocasiones, para una implementación mínima que no se ajusta a la complejidad de las amenazas actuales. La aplicación de sanciones por incumplimiento de la LOPDP en casos donde la suplantación deriva en una filtración de datos, aunque posible, aún requiere de un desarrollo jurisprudencial para establecer precedentes claros y criterios de atribución de responsabilidad.

4.1.3. Aumento Exponencial de la Ciberdelincuencia por Suplantación de Identidad en Ecuador y su Impacto Particular en MIPYMES

Los datos recolectados de informes oficiales corroboran un incremento alarmante en la incidencia de delitos informáticos relacionados con la suplantación de identidad en Ecuador. La Fiscalía General del Estado (FGE), en su Informe Anual de Ciberdelincuencia de 2023, reportó un crecimiento del 35% en las denuncias por este tipo de ilícitos, superando las 5.000 incidencias, con una correlación directa con el auge de las transacciones en línea y la apertura fraudulenta de cuentas. Un caso emblemático, aunque sin divulgar el nombre de la institución por razones de confidencialidad, fue la alerta emitida por la Superintendencia de Bancos en 2022 sobre fraudes masivos que utilizaron datos obtenidos por phishing para realizar transferencias no autorizadas y solicitar créditos a nombre de terceros, generando un perjuicio económico estimado en varios cientos de miles de dólares y afectando a un gran número de usuarios.

Este impacto se agudiza en el sector de las Micro, Pequeñas y Medianas Empresas (MIPYMES) ecuatorianas. Estas empresas, que constituyen una parte fundamental de la economía, son particularmente vulnerables, dado que frecuentemente carecen de los recursos económicos, el conocimiento técnico especializado y la infraestructura robusta para implementar medidas de ciberseguridad avanzadas. Se han documentado casos, como el de "Tiendex S.A." en 2021, donde la falta de protocolos de verificación de identidad generó pérdidas económicas directas y sanciones por parte de la Superintendencia de Protección de Datos, afectando gravemente su operación y reputación a largo plazo.

4.1.4. Sofisticación y Diversificación de las Técnicas de Suplantación de Identidad en el Comercio Electrónico

Más allá de las modalidades ya conocidas y ampliamente estudiadas como el phishing (fraude por correo electrónico), vishing (por voz) y smishing (por SMS), la investigación revela una creciente sofisticación y diversificación de las técnicas empleadas por los ciberdelincuentes. Se ha documentado un aumento en el uso de métodos como el "spoofing" de IP/DNS (falsificación de direcciones para redirigir tráfico a sitios maliciosos), el empleo de "malware" avanzado diseñado específicamente para el robo de credenciales de acceso a cuentas, y la proliferación del "account takeover" (ATO). Esta última técnica es especialmente preocupante en el comercio electrónico, ya que permite a los atacantes, una vez obtenidas las credenciales,

tomar control completo de una cuenta legítima del usuario para realizar compras fraudulentas, solicitar créditos o acceder a información sensible, operando desde un perfil aparentemente legítimo y dificultando la detección temprana por parte de las plataformas y los usuarios.

4.1.5. El Papel Esencial de la Educación del Consumidor y la Debida Diligencia con Terceros Proveedores

Los hallazgos subrayan que la prevención de la suplantación de identidad no es una responsabilidad exclusiva de las empresas en cuanto a su infraestructura. Se identificó que la educación y concienciación del consumidor constituyen una línea de defensa crítica. Una gran parte de los ataques exitosos de suplantación de identidad explotan la falta de conocimiento o la negligencia de los usuarios finales. Las empresas, por tanto, tienen un rol crucial en la implementación de programas o campañas informativas dirigidas a sus usuarios sobre cómo reconocer y reportar intentos de fraude, la importancia de la autenticación multifactorial y la protección de sus credenciales.

Asimismo, la investigación destacó la relevancia de la debida diligencia en la selección y monitoreo continuo de proveedores de servicios digitales y terceros (e.g., pasarelas de pago, servicios en la nube, proveedores de hosting). La seguridad de una empresa en el entorno digital es tan fuerte como el eslabón más débil de su cadena de suministro tecnológico. Se encontró que la inclusión de cláusulas contractuales explícitas que obliguen a estos terceros a cumplir con estándares de seguridad internacionales (como ISO 27001), a realizar auditorías periódicas y a asumir responsabilidad en caso de incidentes de seguridad que deriven en suplantación, es una medida preventiva fundamental.

4.2. DISCUSIÓN DE LOS RESULTADOS

Los hallazgos presentados en la sección anterior no solo confirman la magnitud del problema de la suplantación de identidad en el comercio electrónico ecuatoriano, sino que también iluminan las complejidades y los desafíos sistémicos que deben abordarse desde una perspectiva jurídica y empresarial.

La Imperiosa Necesidad de Clarificación Jurisprudencial: La incertidumbre jurídica generada por la ausencia de una jurisprudencia consolidada sobre la responsabilidad civil de los

operadores de comercio electrónico es una barrera significativa para la seguridad transaccional. Esta situación contrasta con el desarrollo legal en otras jurisdicciones y exige una interpretación judicial proactiva de los principios de diligencia debida y riesgo de negocio en el ámbito digital. La falta de precedentes claros deja a las víctimas en una posición vulnerable y a las empresas sin una guía precisa sobre sus obligaciones de seguridad, lo cual podría llevar a litigios complejos y prolongados.

La Brecha Regulatoria en un Contexto Dinámico: La LCEFME y la LOPDP, aunque pilares de la legislación digital ecuatoriana, no logran cubrir con la suficiente especificidad los desafíos que presentan las nuevas modalidades de suplantación de identidad. La naturaleza vertiginosa de la evolución tecnológica y de las tácticas cibercriminales exige una normativa flexible y adaptable, o al menos un desarrollo reglamentario y de guías técnicas que detallen los estándares de seguridad esperados. La regulación actual es un punto de partida, pero no un destino final en la carrera contra el fraude digital.

La Vulnerabilidad Sistémica de las MIPYMES: La situación de las MIPYMES ecuatorianas, expuestas de manera desproporcionada a los ataques de suplantación por su limitación de recursos, es un reflejo de una falla sistémica en el ecosistema digital. Si estas empresas son el motor de la economía, su exposición al riesgo digital amenaza la estabilidad y el crecimiento del comercio electrónico en el país. Esto no solo exige soluciones legales, sino también políticas públicas y apoyo gremial que democraticen el acceso a la ciberseguridad y la asesoría jurídica especializada.

Un Enfoque Multidimensional para una Amenaza Sofisticada: La constante evolución de las técnicas de suplantación (especialmente ATO y spoofing) demuestra que la solución no reside únicamente en medidas reactivas o en el cumplimiento básico de la ley. Se requiere un enfoque proactivo y multidimensional que integre soluciones legales (contratos, políticas), tecnológicas (IA/ML, MFA) y humanas (capacitación, concienciación). La interconexión entre estas dimensiones es crucial, ya que una falla en cualquiera de ellas puede comprometer la seguridad general del sistema.

El Imperativo de la Confianza Digital: En el comercio electrónico, la confianza del usuario es el activo más valioso. Los incidentes de suplantación no solo generan pérdidas económicas y sanciones, sino que erosionan esta confianza, llevando a los consumidores a dudar de la seguridad de las plataformas. Un robusto compliance digital, más allá de ser una obligación

legal, se convierte en una estrategia fundamental para construir y mantener la reputación, diferenciarse en el mercado y asegurar la sostenibilidad a largo plazo de los negocios digitales.

4.3. LIMITACIONES DEL ESTUDIO

La presente investigación, aunque exhaustiva en su abordaje documental y jurídico, posee ciertas limitaciones inherentes a su diseño que merecen ser reconocidas para una comprensión completa de su alcance:

- Enfoque Exclusivamente Documental: Al centrarse en el análisis de fuentes secundarias (legislación, jurisprudencia, doctrina, informes), la investigación no incluyó la recolección de datos primarios a través de encuestas, entrevistas a expertos (jueces, abogados especializados en ciberdelitos, empresarios) o estudios de caso empíricos a profundidad en empresas ecuatorianas. Esto podría haber proporcionado perspectivas más directas sobre las experiencias y desafíos prácticos.
- Dinamicidad del Ciberdelito: El panorama de la ciberdelincuencia y las tecnologías asociadas evoluciona a un ritmo acelerado. Aunque se consultaron las fuentes más recientes disponibles al momento de la investigación, la aparición de nuevas técnicas de suplantación o la obsolescencia de ciertas medidas preventivas es una constante.
- Confidencialidad de Casos Reales: La dificultad de acceder a detalles específicos de casos judiciales o empresariales en Ecuador debido a la confidencialidad y la protección de la reputación, limitó la posibilidad de realizar un análisis jurisprudencial ecuatoriano más extenso y detallado sobre incidentes de suplantación, lo que obligó a una mayor dependencia de la jurisprudencia comparada y de informes generales.

5. Propuestas y Recomendaciones

Basado en el análisis de resultados y los hallazgos que evidencian vacíos normativos, la incipiente jurisprudencia y la creciente amenaza de la suplantación de identidad en el comercio electrónico ecuatoriano, se articula la presente propuesta. Esta consiste en un modelo integral de asesoría jurídica empresarial, complementado con recomendaciones prácticas y estratégicas, diseñado para fortalecer la seguridad jurídica de las empresas —con un énfasis particular en las vulnerables MIPYMES— y mitigar los riesgos inherentes a los ciberdelitos en el entorno digital.

5.1. JUSTIFICACIÓN DE LA PROPUESTA

La necesidad imperante de esta propuesta se desprende directamente de las conclusiones del análisis de resultados. La incertidumbre jurídica y la vulnerabilidad operativa que enfrentan las empresas ecuatorianas en el ecosistema digital, sumadas a la sofisticación de los ataques de suplantación de identidad, demuestran una clara brecha entre el marco legal existente y la realidad de las ciberamenazas. Un modelo de asesoría proactivo y un protocolo estandarizado son esenciales para:

- Reducir la Exposición a Riesgos: Disminuir la probabilidad de sufrir sanciones legales, pérdidas económicas significativas y el consecuente daño reputacional derivado de incidentes de suplantación.
- Fortalecer la Confianza del Consumidor: Promover un entorno transaccional más seguro y predecible, lo cual es crucial para fomentar la adopción y el crecimiento sostenido del comercio electrónico en el país.
- Optimizar la Respuesta a Incidentes: Proporcionar herramientas y procedimientos claros para que las empresas gestionen eficazmente los eventos de suplantación, minimizando su impacto y facilitando la colaboración con las autoridades.
- Ofrecer una Guía Práctica y Escalable: Desarrollar soluciones adaptadas a la realidad de las MIPYMES ecuatorianas, que a menudo carecen de recursos económicos y humanos para acceder a servicios de ciberseguridad y asesoría legal compleja, permitiéndoles implementar medidas progresivas.

5.2. MODELO DE ASESORÍA JURÍDICA INTEGRAL PARA ENTORNOS DIGITALES

Se propone un modelo de asesoría estructurado en fases interconectadas que permite a las empresas, especialmente a las MIPYMES, adoptar e implementar medidas progresivas para protegerse eficazmente de la suplantación de identidad electrónica. Este modelo se caracteriza por ser escalable y adaptable a las diversas capacidades y niveles de riesgo de cada organización.

5.2.1. Fase de Diagnóstico de Vulnerabilidades y Evaluación Legal Exhaustiva

Esta fase inicial es crucial para comprender la postura de seguridad jurídica de la empresa. Implica una inmersión profunda en sus operaciones y documentación:

- Análisis Documental Interno y Contractual: Revisión pormenorizada de todos los documentos legales internos y externos, incluyendo: contratos con clientes (términos y condiciones de uso de la plataforma), contratos con proveedores de servicios digitales (pasarelas de pago, servicios de hosting y en la nube), acuerdos de confidencialidad, políticas de privacidad y protección de datos, avisos legales y políticas de cookies. El objetivo es identificar cláusulas débiles, ambigüedades o ausencias que puedan ser explotadas en un ataque de suplantación.
- Evaluación de Flujos de Datos Personales: Mapeo detallado de cómo la empresa recopila, procesa, almacena, transmite y elimina datos personales de sus usuarios y clientes. Se identifican los "puntos calientes" o críticas de vulnerabilidad donde los datos podrían ser interceptados o alterados, facilitando una suplantación de identidad. Esto incluye el análisis de los mecanismos de autenticación y verificación de identidad utilizados actualmente.
- Auditoría de Cumplimiento Normativo Vigente: Verificación exhaustiva del grado de cumplimiento de la empresa con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; la Ley Orgánica de Protección de Datos Personales (LOPDP); el Código Orgánico Integral Penal (COIP) en relación con delitos informáticos; y cualquier otra regulación sectorial aplicable (ej. para fintechs o servicios financieros).
- Identificación de Errores Legales Comunes y Recomendaciones Primarias: Asesoramiento proactivo sobre las fallas legales más frecuentes que incrementan el riesgo de suplantación de identidad. Esto incluye la ausencia de cláusulas de seguridad específicas en contratos, la implementación de mecanismos de autenticación débiles (ej. solo contraseña), la gestión deficiente de los registros de transacciones (logs), o la falta de un plan de respuesta a incidentes formalmente documentado. Se ofrecen recomendaciones inmediatas para corregir estas deficiencias.

5.2.2. Fase de Implementación de Mecanismos de Protección y Estrategias Preventivas Proactivas

Una vez diagnosticadas las vulnerabilidades, esta fase se centra en la aplicación de soluciones concretas:

- Diseño e Implementación de Políticas de Seguridad Jurídica Robusta: Elaboración e integración de documentos legales claros y vinculantes que establezcan protocolos

internos y externos para la gestión segura de la identidad digital y la protección de datos. Esto incluye:

- Estándares de Debida Diligencia para Empresas Digitales:
- Autenticación Multifactorial (MFA): Asesoría para la implementación obligatoria de MFA para usuarios y administradores en todas las plataformas y sistemas críticos como medida estándar de seguridad mejorada. La MFA reduce drásticamente el riesgo de account takeover (ATO) incluso si una contraseña es comprometida.
- Cifrado de Datos End-to-End: Asegurar que todos los datos sensibles, tanto en tránsito (durante la comunicación) como en reposo (almacenados en servidores o bases de datos), estén protegidos mediante tecnologías de cifrado robustas.
- Monitoreo Continuo y Detección de Anomalías: Establecer y configurar sistemas automatizados para identificar patrones de comportamiento inusuales, intentos de acceso no autorizados, transacciones atípicas o signos de spoofing de IP/DNS. Esto permite una alerta temprana ante posibles intentos de suplantación.
- Gestión Proactiva de Vulnerabilidades: Implementación de un ciclo regular de auditorías de seguridad, pruebas de penetración (pentesting) y evaluaciones de vulnerabilidad para identificar y corregir proactivamente las debilidades en la infraestructura digital antes de que sean explotadas por atacantes.
- Evaluación Rigurosa y Contratación Estratégica de Proveedores de Servicios Digitales:
- Debida Diligencia Extendida (Third-Party Risk Management): Antes de contratar cualquier proveedor de servicios en la nube, pasarela de pago o software, se debe investigar a fondo su reputación, sus certificaciones de seguridad (ej., ISO 27001), y sus políticas internas de ciberseguridad y manejo de datos.
- Cláusulas Contractuales Específicas sobre Seguridad y Responsabilidad: Es crucial incluir en los contratos con terceros cláusulas explícitas que detallen los estándares de seguridad que el proveedor debe cumplir, la responsabilidad en caso de incidentes de seguridad que deriven en suplantación de identidad (ej., filtraciones de datos por fallas en su infraestructura), la obligación de notificar brechas de seguridad de forma inmediata y detallada, y la posibilidad de realizar auditorías periódicas por parte de la empresa contratante.

- Propuesta de Protocolo Legal Estandarizado para Tiendas Virtuales: Este protocolo sirve como una guía práctica para las operaciones diarias.
- Identificación Obligatoria y Verificación Robusta del Cliente: Establecer requisitos de verificación de identidad rigurosos para la creación de cuentas y para transacciones de alto valor. Esto puede incluir el uso de la firma electrónica avanzada ecuatoriana, sistemas de verificación biométrica o la validación de documentos de identidad con fuentes oficiales.
- Conservación de Bitácoras Digitales (Logs) para Fines Probatorios: Obligación de almacenar de forma segura y con integridad (inalterable) registros detallados (logs) de todas las transacciones, inicios de sesión, cambios de credenciales y eventos de seguridad por un período mínimo (sugerencia: entre 3 y 5 años, o según normativa específica) para facilitar investigaciones forenses y servir como prueba en litigios.
- Cláusulas Contractuales Explícitas en Términos y Condiciones: Inclusión de cláusulas claras y comprensibles en los términos y condiciones de uso de la plataforma que informen a los usuarios sobre los riesgos de suplantación, sus responsabilidades en la protección de sus credenciales, y los procedimientos a seguir en caso de sospecha de fraude o acceso no autorizado a su cuenta.
- Procedimientos de Respuesta a Incidentes de Suplantación: Establecer un plan de acción legal y operativo detallado para gestionar los incidentes de suplantación de identidad. Esto incluye pasos para la notificación inmediata a las autoridades competentes (Fiscalía, Superintendencia de Protección de Datos), comunicación transparente con los usuarios afectados, y la implementación de medidas correctivas para mitigar el daño y evitar futuras recurrencias.

5.2.3. Fase de Capacitación, Monitoreo Continuo y Mejora Continua: Cultura de Compliance

Esta fase es vital para asegurar la sostenibilidad del modelo y su adaptación a un entorno de ciberseguridad en constante cambio.

Capacitación Empresarial Integral y Fomento del Compliance Digital:

Formación Continua del Personal: Sesiones de capacitación periódicas y obligatorias para todos los empleados de la empresa, desde la alta dirección hasta el personal operativo. Los

temas deben incluir la identificación de técnicas de phishing/smishing, prácticas seguras de manejo de datos, protocolos de reporte de incidentes, y la importancia del cumplimiento de las políticas de seguridad de la información.

Concienciación y Educación al Consumidor: Desarrollo e implementación activa de campañas informativas y recursos educativos (guías, videos, infografías) dirigidos a los usuarios de la plataforma. Estas campañas deben instruir a los consumidores sobre cómo proteger sus credenciales, reconocer intentos de suplantación, validar la autenticidad de las comunicaciones de la empresa y los pasos para reportar cualquier actividad sospechosa. Una base de usuarios informada es la primera línea de defensa contra muchos ataques.

Monitoreo Legal y Tecnológico Constante:

Vigilancia Normativa y Jurisprudencial: Establecer un mecanismo de seguimiento continuo de los cambios en la legislación ecuatoriana e internacional sobre ciberseguridad, protección de datos y comercio electrónico, así como de la evolución de la jurisprudencia relevante.

Monitoreo de Amenazas Avanzado con Tecnologías Emergentes: Integración de herramientas de Inteligencia Artificial (IA) y Machine Learning (ML) para el monitoreo proactivo. Estas tecnologías pueden analizar grandes volúmenes de datos transaccionales y de comportamiento del usuario para detectar patrones anómalos, identificar actividades fraudulentas o intentos de phishing en tiempo real, permitiendo una respuesta inmediata. La IA puede aprender de ataques previos para mejorar la detección futura.

Auditorías Periódicas y Pruebas de Estrés: Realización regular de auditorías de seguridad internas y externas, así como pruebas de estrés y de penetración, para evaluar la eficacia de las medidas de protección implementadas y la resiliencia de los sistemas ante nuevas amenazas.

Adaptación y Mejora Continua: Fomentar una cultura organizacional que promueva la revisión y el ajuste constante de las políticas, protocolos y tecnologías de seguridad con base en la evolución de las ciberamenazas, los cambios normativos y las lecciones aprendidas de incidentes previos. Este ciclo de mejora continua es indispensable en un entorno digital tan dinámico.

5.3. IMPLICACIONES JURÍDICAS Y OPERACIONALES DEL INCUMPLIMIENTO: LECCIONES APRENDIDAS

La no implementación de un modelo de asesoría jurídica integral y las medidas de compliance digital propuestas puede acarrear consecuencias severas que van más allá de la pérdida de una transacción. El caso de Tiendex S.A. en Ecuador en 2021 sirve como un claro ejemplo ilustrativo de los riesgos. Esta empresa enfrentó pérdidas significativas y fue sancionada por la Superintendencia de Protección de Datos precisamente por la falta de un protocolo adecuado de verificación de identidad en sus contratos electrónicos. El perjuicio no fue solo económico directo, sino que se extendió al daño reputacional, la pérdida de confianza de los clientes y la posible paralización de operaciones.

Más allá de casos puntuales, el incumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), en escenarios donde la suplantación de identidad deriva en una filtración de datos personales, puede resultar en multas administrativas de hasta el diez por ciento (10%) de la facturación anual de la empresa, una sanción considerable que puede comprometer seriamente la viabilidad económica, especialmente de las MIPYMES. Además, las empresas pueden enfrentar demandas civiles por daños y perjuicios por parte de los usuarios afectados, y la pérdida de la confianza del consumidor, que es un activo intangible de valor incalculable en el comercio digital, puede llevar a una erosión irreversible de la base de clientes y la cuota de mercado.

5.4. IMPORTANCIA ESTRATÉGICA DEL COMPLIANCE DIGITAL EN EL ENTORNO ECUATORIANO

El compliance digital, entendido como la adhesión a las normas y principios éticos en el entorno digital, trasciende de ser una mera obligación legal para convertirse en una estrategia competitiva y un pilar de la sostenibilidad empresarial en el mercado ecuatoriano y global.

Fortalecimiento de la Confianza y la Reputación: Las empresas que demuestran un compromiso proactivo y visible con la seguridad de los datos y la prevención del fraude generan una mayor confianza en sus usuarios y stakeholders. Esta confianza se traduce en

lealtad del cliente, una mejor imagen de marca y una ventaja competitiva en un mercado donde la ciberseguridad es una preocupación creciente para los consumidores.

Mitigación Efectiva de Riesgos: Un programa de compliance digital robusto reduce significativamente la probabilidad de ocurrencia de incidentes de suplantación de identidad y, en caso de que ocurran, minimiza su impacto y sus consecuencias negativas (financieras, legales y reputacionales).

Preparación para el Futuro y Adaptabilidad: Al mantener un monitoreo constante de la evolución normativa y tecnológica, las empresas con un sólido compliance están mejor preparadas para anticipar futuras regulaciones y adoptar nuevas tecnologías de seguridad, asegurando su resiliencia en un entorno digital cambiante.

5.4.1. Recomendaciones Específicas: Hacia una Mejora Normativa y Contractual

Para complementar la propuesta de asesoría empresarial, se formulan las siguientes recomendaciones dirigidas a los actores del sistema jurídico y empresarial:

- Clarificación Legislativa y Desarrollo Jurisprudencial: Se insta a la Asamblea Nacional y a la Corte Nacional de Justicia a considerar el desarrollo de una normativa más específica y una jurisprudencia que defina claramente la responsabilidad de los intermediarios en el comercio electrónico ante la suplantación de identidad, estableciendo estándares de diligencia debida y mecanismos de prueba adecuados.
- Establecimiento de Cláusulas Contractuales Tipo: Se sugiere que organismos como la Cámara Ecuatoriana de Comercio Electrónico (CECE) o la Defensoría del Pueblo promuevan el desarrollo de modelos de cláusulas contractuales estandarizadas para transacciones electrónicas. Estas cláusulas deberían abordar explícitamente la verificación de identidad, la gestión de la suplantación, los mecanismos de autenticación y la atribución de responsabilidades en caso de fraude, proporcionando mayor seguridad jurídica a ambas partes.

5.4.2. Incentivos y Apoyos Interinstitucionales para la Implementación en MIPYMES

Reconociendo las limitaciones de las MIPYMES, es fundamental el apoyo interinstitucional:

- Programas Gubernamentales de Fomento: Se recomienda que entidades gubernamentales como el Ministerio de Producción, Comercio Exterior, Inversiones y

Pesca (MPCEIP) y la Corporación Financiera Nacional (CFN) diseñen e implementen programas de apoyo financiero (subsidios, líneas de crédito blandas) y técnico para que las MIPYMES puedan invertir en soluciones de ciberseguridad (ej., sistemas MFA, softwares de detección de IA/ML) y acceder a servicios de asesoría jurídica especializada en derecho digital.

- Alianzas Público-Privadas y Gremiales: Los gremios empresariales (ej., Cámaras de Comercio, CECE) pueden desempeñar un rol crucial. Se recomienda que establezcan alianzas con expertos en ciberseguridad y abogados especializados para ofrecer capacitaciones, talleres y recursos (ej., plantillas de políticas de privacidad y términos de uso) a sus miembros a costos accesibles, fomentando la adopción de buenas prácticas de compliance digital de manera colectiva y sectorial.

5.4.3. Consideraciones Éticas y de Privacidad en la Implementación de Soluciones de Seguridad

En la implementación de medidas para combatir la suplantación de identidad, es imperativo mantener un equilibrio delicado entre la eficacia de la seguridad y el respeto a los derechos fundamentales de los usuarios, particularmente el derecho a la privacidad y la protección de datos personales.

Principio de Proporcionalidad y Necesidad: Cualquier medida de seguridad (ej., el uso de biometría, el monitoreo intensivo de transacciones) debe ser proporcional al riesgo que se busca mitigar y estrictamente necesaria para alcanzar el fin legítimo de prevención del fraude. No se deben recolectar más datos de los estrictamente necesarios para el propósito.

Transparencia y Consentimiento Informado: Las empresas deben ser plenamente transparentes con sus usuarios sobre cómo se recopilan, procesan y utilizan sus datos personales para fines de seguridad y prevención de fraudes. Siempre que sea legalmente requerido, se debe obtener el consentimiento informado de los usuarios para el procesamiento de sus datos, explicando claramente las implicaciones y los beneficios de seguridad.

Análisis de Impacto en la Protección de Datos (DPIA): Para la implementación de nuevas tecnologías o procesos que impliquen un alto riesgo para los derechos y libertades de los interesados (como la biometría o el monitoreo avanzado), se recomienda la realización de un

Análisis de Impacto en la Protección de Datos, conforme a las directrices de la LOPDP, para identificar y mitigar proactivamente los riesgos de privacidad.

5.5. RECOMENDACIONES PARA FUTURAS INVESTIGACIONES

La presente investigación ha abierto nuevas avenidas para el estudio en el campo del derecho digital en Ecuador. Se sugieren las siguientes líneas de investigación futuras:

- Estudios Empíricos sobre la Percepción y Desafíos de las MIPYMES: Realizar investigaciones de campo (encuestas, entrevistas) con propietarios y gerentes de MIPYMES ecuatorianas para obtener datos primarios sobre sus percepciones de riesgo, los desafíos prácticos que enfrentan en la implementación de medidas de ciberseguridad, y la viabilidad o impacto real de las soluciones propuestas en este estudio.
- Análisis Comparado de Modelos de Responsabilidad en América Latina: Profundizar en un estudio comparativo de la evolución jurisprudencial y normativa sobre la responsabilidad de los intermediarios del comercio electrónico en otros países de América Latina (ej., Chile, Perú, México), para identificar mejores prácticas y posibles adaptaciones para el contexto ecuatoriano.
- Impacto Legal de Tecnologías Emergentes en la Identidad Digital: Investigar el potencial y los desafíos jurídicos que tecnologías como blockchain (para identidades descentralizadas) o la computación cuántica podrían presentar en la prevención de la suplantación de identidad y la protección de transacciones en el comercio electrónico.
- Evaluación de la Eficacia de las Campañas de Concienciación al Consumidor: Realizar estudios para medir el impacto de las campañas de educación y concienciación sobre ciberseguridad implementadas por empresas o el gobierno en la reducción de incidentes de suplantación de identidad por parte de los usuarios finales.

6. Conclusiones

A lo largo de este estudio, se ha efectuado un análisis centrado en la suplantación de identidad electrónica dentro del entorno del comercio digital, examinando sus repercusiones jurídicas, económicas y empresariales. De igual forma, se ha explorado la pertinencia de implementar

estrategias de asesoría legal orientadas a contrarrestar este problema y reforzar la protección en las operaciones electrónicas. Como resultado de esta investigación, se han identificado una serie de hallazgos clave que se detallan a continuación.

Primera.- La suplantación de identidad electrónica representa una amenaza creciente en el contexto del comercio electrónico, afectando no solo la seguridad de las transacciones, sino también la confianza de los consumidores y la sostenibilidad del ecosistema digital. Los datos analizados a lo largo del estudio evidencian que este fenómeno ha evolucionado en complejidad, aprovechando vacíos legales, deficiencias técnicas y limitaciones institucionales para operar con relativa impunidad. Como indicó López (2021), "la sofisticación de las técnicas de suplantación ha superado la capacidad de respuesta de muchos marcos normativos tradicionales, dejando a las víctimas en una situación de alta vulnerabilidad".

Segunda.- Desde el punto de vista jurídico, el análisis del marco normativo nacional revela avances importantes, como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Sin embargo, esta normativa no contempla de forma específica y actualizada los delitos de suplantación de identidad digital, lo cual limita su eficacia. En este sentido, Pérez (2023) destaca que "la tipificación penal en muchos países latinoamericanos no se adapta a las nuevas formas de fraude en línea, lo que obstaculiza su persecución efectiva".

Tercera.- Las investigaciones recientes también permiten observar que los usuarios y empresas aún desconocen los mecanismos de protección y denuncia frente a estos delitos, lo que incrementa su exposición al riesgo. Asimismo, los órganos judiciales enfrentan barreras estructurales, como la falta de personal especializado en ciberseguridad, escasa coordinación internacional y procesos obsoletos de recolección de evidencia digital. Como lo afirma el

informe de la CEPAL (2020), “la resiliencia digital de América Latina depende en gran medida de la inversión en capacidades institucionales y tecnológicas”.

Cuarta.- En respuesta a este escenario, resulta imprescindible fortalecer las medidas de asesoría jurídica empresarial como una estrategia integral para prevenir y mitigar los riesgos asociados a la suplantación de identidad. Esto incluye la implementación de protocolos de verificación de identidad, uso de tecnologías de autenticación robustas, educación digital a los usuarios y una adecuada asesoría legal que oriente a las empresas sobre las responsabilidades legales y mecanismos de defensa jurídica. Tal como lo sostiene Hernández (2022), “la protección jurídica proactiva es clave para garantizar entornos comerciales digitales más seguros y sostenibles”.

Quinta.- En este contexto, no es suficiente con reformar el marco legal; resulta imprescindible que el sector empresarial adopte una postura activa frente a los riesgos digitales, implementando medidas técnicas y organizacionales que fortalezcan sus sistemas de verificación, monitoreo y respuesta ante intentos de suplantación. Esta corresponsabilidad no solo minimiza las brechas de seguridad, sino que también aporta sostenibilidad al entorno comercial digital.

Sexta.- Asimismo, el Estado debe asumir un rol dinámico en la regulación y supervisión, garantizando que la legislación evolucione al ritmo de los avances tecnológicos y de las nuevas modalidades delictivas. Ello implica invertir en capacidades institucionales, fomentar la formación especializada en ciberseguridad y promover la cooperación entre sectores público, privado y académico, a fin de consolidar una infraestructura jurídica y tecnológica resiliente.

Séptima.- Finalmente, es indispensable actualizar la legislación penal ecuatoriana, tipificando de manera específica la suplantación de identidad electrónica como delito autónomo,

incorporando sanciones proporcionales y promoviendo la cooperación internacional para su combate efectivo. La articulación entre el sector público, el privado y la academia será fundamental para enfrentar este reto y promover una cultura de ciberseguridad centrada en la protección de los derechos digitales. En palabras de García y Romero (2019), “la transformación digital solo será exitosa si se garantiza un entorno legal confiable y adaptado a los desafíos del siglo XXI”.

Referencias bibliográficas

Bibliografía básica

ASAMBLEA NACIONAL DEL ECUADOR. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

ASAMBLEA NACIONAL DEL ECUADOR. (2014). Código Orgánico Integral Penal (COIP).

BRIONES, R. (2020). El Derecho en la sociedad digital. 1ª ed. Quito: Jurídica EC.

CALDERÓN, J. (2021). Ciberdelitos y suplantación de identidad en entornos digitales. 1ª ed. Bogotá: Legis.

CEDEÑO SARMIENTO, C. A., BOLAÑOS BURGOS, F., MENDOZA ARTEAGA, A. G., & SALTOS RIVAS, W. R. (2020). Estudio exploratorio de la seguridad del DNI electrónico para su aplicación en Ecuador. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 4(1), 64.

ESPARZA CRUZ, N. K. (2017). El Comercio Electrónico en el Ecuador. Journal of Science and Research: Revista Ciencia e Investigación, 2(6), 29–32.

FERNÁNDEZ SALMERÓN, M. (2020). Derecho y tecnologías de la información: protección de datos y privacidad. 2ª ed. Madrid: Dykinson.

GUERRERO-CORTEZ, V., TINGO-HERRERA, J., GALLEGOS-VARGAS, M., & CARRIÓN-AGUILAR, R. (2022). El comercio electrónico ventajas y desventajas. 593 Digital Publisher CEIT, 7(5-1), 250-261.

GUTIÉRREZ JARAMILLO, N. D., BARRUETO PÉREZ, M. T., & ORELLANA ULLOA, M. N. (2020). La fiscalidad del Comercio Electrónico en el contexto tributario ecuatoriano. Quipukamayoc, 28(57), 67-74.

HEREDIA PINCAY, D. E., & VILLARREAL SATAMA, F. L. (2022). El comercio electrónico y su perspectiva en el mercado ecuatoriano. ComHumanitas: Revista Científica de Comunicación, 13(1), 1-33.

LOPEZ RODRÍGUEZ, A. (2019). Protección jurídica del consumidor en el comercio electrónico. 1ª ed. Barcelona: Atelier.

MACÍAS-LARA, R. A., BONÉ ANDRADE, M. F., ANGULO, F. Q., LOOR, J. J. M., ESTUPIÑAN-TROYA, G., & RODRÍGUEZ VIZUETE, J. D. (2022). Casos frecuentes, penalización y prevención

de los delitos informáticos en el Ecuador: una breve revisión sistemática. Sapienza: International Journal of Interdisciplinary Studies, 3(2), 231-243.

MONDRAGÓN, N. (2020). Generación de identidad digital para el acceso a los servicios ciudadanos digitales en Colombia. Universidad de los Andes Colombia.

PESÁNTEZ-CALVA, A. E., ROMERO-CORREA, J. A., & GONZÁLEZ-ILLESCA, M. L. (2020). Comercio electrónico B2B como estrategia competitiva en el comercio internacional: Desafíos para Ecuador. INNOVA Research Journal, 5(1), 72–93.

QUISPE FERNÁNDEZ, G. M., ARELLANO CEPEDA, O. E., RODRÍGUEZ, E. A., & CRUZ PARRA, J. F. (2023). La rentabilidad y el comercio electrónico en las PYMES en el Ecuador. Caso emprendimientos en empresas de alimentos y bebidas. Ciencia Digital, 7(2), 82-94.

RIVERO, D. C. (2010). LA ATRIBUCIÓN DEL RIESGO DE SUPLANTACIÓN DE IDENTIDAD EN LA BANCA ELECTRÓNICA. En A. Madrid Parra (Dir.), M. J. Guerrero Lebrón & Á. M. Pérez Rodríguez (Coords.), Derecho del sistema financiero y tecnología (pp. 237-258). Marcial Pons, ediciones jurídicas y sociales.

ROMERO ROSALES, M., & RIBADENEIRA MOLESTINA, T. (2000). El comercio electrónico en Ecuador: régimen jurídico y comentarios. Iuris Dictio, 1(2).

TORRES, A. Y SÁNCHEZ, M. (2022). La responsabilidad civil en el entorno digital. 2ª ed. Lima: Grijley.

ZAMBRANO VELASCO, B., CASTELLANOS ESPINOZA, E. B., & MIRANDA GUATUMILLO, M. A. (2021). El E-Commerce en las empresas ecuatorianas: Un análisis de los informes de la Cámara Ecuatoriana de Comercio Electrónico (CECE) en el marco de la pandemia covid-19. Revista Publicando, 8(29), 13-20.

Bibliografía complementaria

Almeida, J. (2021). *Asesoría jurídica empresarial: principios, funciones y estrategias*. 1ª ed. Quito: Ediciones Jurídicas Cevallos.

Castillo, D. (2020). *La ciberseguridad y el derecho: implicaciones jurídicas*. 1ª ed. Bogotá: Temis.

De Miguel, A. (2019). *Comercio electrónico y contratación digital*. 2ª ed. Madrid: Civitas.

Pérez Luño, A. E. (2021). *Derecho y tecnología: retos actuales*. 1ª ed. Sevilla: Editorial Universidad de Sevilla.

Velázquez, M. (2019). *Responsabilidad penal y delitos informáticos*. 1ª ed. México D.F.: Porrúa.

Rebollo Delgado, P. (2020). *Derecho y nuevas tecnologías*. Madrid: Editorial Reus

Legislación citada

Asamblea Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Asamblea Nacional del Ecuador.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal (COIP)*. Asamblea Nacional del Ecuador.

Ley Orgánica de Protección de Datos Personales, República del Ecuador, 2021.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos - RGPD).

Jurisprudencia referenciada

Sentencia No. 227-20-JP/20. *Corte Constitucional del Ecuador*.

Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), *Asunto C-131/12, Google Spain SL vs Agencia Española de Protección de Datos*, 2014.

Sentencia de la Corte Suprema de Justicia de Colombia, Sala Penal, Radicado 52819, sobre responsabilidad penal por suplantación de identidad digital, 2019.

Referencias adicionales

ASAMBLEA NACIONAL DEL ECUADOR. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Asamblea Nacional del Ecuador.

ASAMBLEA NACIONAL DEL ECUADOR. (2014). *Código Orgánico Integral Penal*. Asamblea Nacional del Ecuador.

CIESPAL. (2022). *Impacto de los delitos cibernéticos en el comercio electrónico en Ecuador*. CIESPAL.

COMISIÓN FEDERAL DE COMERCIO (FTC). (2021). *Phishing*. Comisión Federal de Comercio (FTC) de Estados Unidos.

CYBERSECURITY VENTURES. (2020). *El costo global del cibercrimen alcanzará los 10.5 billones de dólares anuales para 2025*. Cybersecurity Ventures.

DINARDAP. (2025). *Informe sobre el estado actual de la suplantación de identidad electrónica en Ecuador*. Quito: DINARDAP.

KASPERSKY. (2020). *Phishing: Definición, modalidades y prevención*. Kaspersky.

LÓPEZ, M. (2020). *Ciberseguridad en el entorno empresarial ecuatoriano: Riesgos y soluciones legales*. Editorial Jurídica Andina.

MORGAN, S. (2020). *Cibercrimen: Una amenaza global en ascenso*. Cybersecurity Ventures.

OEA. (2020). *Informe sobre ciberdelincuencia en América Latina*. Organización de Estados Americanos (OEA).

PAREDES, J. (2021). *Compliance digital: Estrategias para mitigar el riesgo de delitos informáticos en el entorno corporativo ecuatoriano*. Editorial Jurídica Andina.

PAREDES, J. (2023). *Análisis de riesgos jurídicos en entornos digitales para MIPYMES*. Quito: Universidad Central del Ecuador.

REINOSO, A. (2021). *La educación jurídica preventiva frente a los delitos cibernéticos en América Latina*. Editorial Jurídica.

SUPERINTENDENCIA DE PROTECCIÓN DE DATOS (2021). *Informe sobre sanciones por incumplimiento de políticas de privacidad en empresas digitales*.

STAMFORD ADVOCATE. (2023). *Phishing en DoorDash: Caso de suplantación de identidad que afectó a más de 700 conductores*. Stamford Advocate.

SUPERTEL. (2019). *Desafíos en la regulación de delitos informáticos en Ecuador*. Superintendencia de Telecomunicaciones de Ecuador.

UNCTAD. (2021). *El comercio electrónico global: Tendencias y estadísticas*. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo.

ISO/IEC 27001:2013. *Information security management systems*. Ginebra: ISO/IEC.

Listado de abreviaturas

COIP	Código Orgánico Integral Penal
ISO	Organización Internacional de Normalización
IEC	Comisión Electrotécnica Internacional
MYPES	Micro, Pequeñas y Medianas Empresas
OEA	Organización de los Estados Americanos
SPD	Superintendencia de Protección de Datos
SUPERTEL	Superintendencia de Telecomunicaciones de Ecuador
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
UNIR	Universidad Internacional de La Rioja