LEX, Revista de Investigación en Ciencias Jurídicas
Volumen 9, N° 34 / julio-septiembre 2026
ISSN-e: 2631-2735 / pp. 1-18
https://doi.org/10.33996/revistalex.v9i34.565
Artículo de investigación

CC BY

LEX Revista de Investigación en Ciencias Jurídicas
https://revistalex.org

El phishing: desafío jurídico ante la ciberestafa en la banca digital ecuatoriana

Phishing: The Legal Challenge of Cyber Fraud in Ecuadorian Digital Banking

Adrian Josue Burgasi Cunalata
adrianburgasi@gmail.com
Mauro Antonio Carrero Pirela
mauro.carrero@uleam.edu.ec

Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador

https://doi.org/10.33996/revistalex.v9i34.565

Palabras clave:
Apropiación Fraudulenta por Medios Electrónicos; Código Orgánico Integral Penal; Ciber estafa; Phishing bancario; Responsabilidad cuasi-objetiva.

Keywords:
Fraudulent Appropriation by Electronic Means; Comprehensive Organic Criminal Code; Cyber fraud; Bank phishing; Quasi-strict liability.

Historia del artículo:
Artículo recibido: 10 de julio 2026 /
Aceptado: 04 de septiembre 2026 /
Publicado: 30 de septiembre 2026

Cómo citar:
Burgasi Cunalata, A. J., & Carrero Pirela, M. A. (2026). El phishing: desafío jurídico ante la ciberestafa en la banca digital ecuatoriana. *Revista Lex, 9*(34), 1-18. https://doi.org/10.33996/revistalex.v9i34.565

Resumen

El crecimiento del phishing en la banca digital ecuatoriana expone serias tensiones normativas frente a la vulnerabilidad informática. El objetivo de la investigación fue analizar la respuesta dogmático-penal, probatoria e institucional al phishing, contrastando los artículos 186, 190, 234, 455 y 49 del Código Orgánico Integral Penal (COIP), con datos de la Fiscalía General del Estado (2015-2025). El estudio se realizó mediante un enfoque dogmático, constitucional y de derecho comparado, complementado con análisis estadístico procesal y estándares de informática forense. Se evidenció que la Estafa (Art. 186 COIP) es la quinta infracción más frecuente, con 212.537 casos y 99,1% de no flagrancia, mientras que la Apropiación Fraudulenta por Medios Electrónicos (Art. 190 COIP) registró 28.995 casos y un crecimiento del 275,8%. La Interceptación Ilegal de Datos (Art. 230 COIP) apenas sumó 732 causas, confirmando que el phishing reposa en la ingeniería social. Exigir extractos en digitales sin cadena de custodia impone a las víctimas una prueba diabólica, vulnerando garantías procesales. Se concluye que existe una insuficiencia normativa penal específica y que la tutela judicial efectiva no puede depender de la mera represión penal individual, sino de la adopción de un régimen garantista de responsabilidad cuasi-objetiva.

Abstract

The rise of phishing in Ecuadorian digital banking exposes serious regulatory tensions regarding cybersecurity vulnerabilities. The objective of this research was to analyze the legal, evidentiary, and institutional response to phishing, comparing Articles 186, 190, 234, 455, and 49 of the Comprehensive Organic Criminal Code (COIP) with data from the Attorney General's Office (2015-

2025). The study was conducted using a legal, constitutional, and comparative law approach, complemented by procedural statistical analysis and forensic computing standards. It was found that fraud (Art. 186 COIP) is the fifth most frequent offense, with 212,537 cases and a 99.1% rate of non-flagrant offenses, while fraudulent appropriation by electronic means (Art. 190 COIP) registered 28,995 cases and a 275.8% increase. The Illegal Interception of Data (Art. 230 COIP) only accounted for 732 cases, confirming that phishing relies on social engineering. Demanding digital statements without a chain of custody imposes an impossible burden on victims, violating due process guarantees. It is concluded that there is a lack of specific criminal law and that effective judicial protection cannot depend on mere individual criminal repression, but rather on the adoption of a system of quasi-strict liability that guarantees due process.

Introducción

La transformación digital de la banca en el Ecuador ha experimentado una aceleración vertiginosa e irreversible, impulsada tanto por la necesidad de inclusión financiera como por el entorno derivado de la pandemia de COVID-19, fenómeno que, a nivel global, redundó en un incremento sustancial de los ciberataques contra el sector financiero. La masificación de la banca por internet y de los monederos electrónicos ha reconfigurado la relación entre el cuentahabiente y la entidad financiera, desplazando el vector de riesgo desde la presencia física en agencias hacia la exposición permanente del usuario en entornos digitales (Alawida et al., 2022).

No obstante, este despliegue tecnológico ha provocado una proliferación exponencial de la cibercriminalidad sofisticada, entre cuyas modalidades destaca el phishing, técnica de ingeniería social orientada a manipular la psiquis del usuario para vulnerar sus mecanismos de autenticación, credenciales confidenciales, códigos One-Time Password (OTP) y tokens de seguridad, y obtener así acceso ilícito al patrimonio. La literatura especializada coincide en señalar que el phishing se ha consolidado como la amenaza de mayor frecuencia y sofisticación contra la banca digital, reforzada por el desarrollo de la inteligencia artificial generativa que perfecciona la verosimilitud del engaño (Naqvi et al., 2023; Schmitt & Flechais, 2024).

Esta realidad traslada el problema del plano estrictamente informático al ámbito del derecho, configurando un desafío de primer orden para garantizar prerrogativas constitucionales fundamentales como el derecho a la propiedad, la protección de datos personales y la seguridad jurídica. En el caso ecuatoriano, la promulgación de la Ley Orgánica de Protección de Datos Personales ha consolidado el marco de tutela del habeas data, integrándose al sistema de garantías reconocidas en el artículo 66, numeral 19, de la Constitución (Asamblea Nacional del Ecuador, 2021; Abad Arévalo et al., 2023).

Sin embargo, la articulación entre este marco protector y la dogmática penal sustantiva permanece fragmentada frente a las modalidades fraudulentas digitales.

La problemática central radica en el desfase entre la sofisticación de estos ataques y las categorías de la dogmática penal clásica, originando una dicotomía sobre la subsunción típica en el Código Orgánico Integral Penal (COIP): si los hechos constituyen una estafa tradicional mediada por engaño (art. 186) o una apropiación fraudulenta por medios electrónicos mediante la alteración o uso indebido de sistemas (art. 190) (Asamblea Nacional del Ecuador, 2014; Altamirano Zavala, 2025). Esta encrucijada dogmática no es privativa del ordenamiento ecuatoriano; la doctrina comparada ha evidenciado dificultades análogas para delimitar el fraude informático frente a la estafa convencional, atendiendo a la naturaleza del bien jurídico tutelado y al papel del error en la consumación (Junta de Política y Regulación Financiera, 2021; Mayer Lux & Toso Milos, 2024). De manera complementaria, se ha profundizado el análisis sobre la imputación objetiva en los fraudes electrónicos como herramienta para racionalizar la atribución de responsabilidad entre autor, víctima y entidad financiera, así como sobre los límites de la responsabilidad civil de la banca por los daños derivados del phishing (Corte Constitucional del Ecuador, 2024; De la Maza & Mosqueira, 2024; Collantes Rodríguez, 2025).

La encrucijada se profundiza al evaluar la atribución de responsabilidad institucional frente a la alegada negligencia del cuentahabiente en la custodia de sus claves, cuestión que introduce un debate central sobre la distribución del riesgo en las relaciones bancarias digitales. La gravedad del fenómeno se corrobora en las cifras oficiales de la Fiscalía General del Estado (2015–2025), donde el delito de estafa se ubica en el quinto lugar nacional de denuncias con 212.537 noticias del delito, superando a infracciones con alto componente físico y evidenciando una crisis sistémica de persecución penal e indefensión de las víctimas ante la pérdida patrimonial (Fiscalía General del Estado, s. f.). Esta tendencia se inscribe en un panorama regional de crecimiento sostenido del cibercrimen en América Latina, donde las modalidades de fraude electrónico han adquirido una dimensión espacial y demográfica que demanda respuestas integrales (Domínguez Arteaga & Vera Vázquez, 2022; Tixi et al., 2023).

A esta complejidad dogmática se añade la dificultad probatoria: la persecución penal del phishing bancario reposa sobre evidencia digital cuya validez exige una cadena de custodia tecnológica rigurosa, cuyos estándares han sido desarrollados recientemente por la doctrina procesal (Jamardo Lorenzo, 2024). La ausencia de protocolos forenses estandarizados en el sistema ecuatoriano amplifica la asimetría probatoria del usuario frente a la institución financiera y debilita la tutela judicial efectiva. La tipificación de los delitos informáticos en el COIP, pese a su avance, presenta vacíos que dificultan una persecución eficaz (Portilla et al., 2025).

Frente a este escenario, es necesario conocer ¿qué criterios dogmático-penales, probatorios y de responsabilidad institucional permiten determinar la subsunción típica del phishing bancario en el COIP ecuatoriano y delimitar la responsabilidad de las entidades financieras, en armonía con la tutela constitucional y los estándares del derecho comparado? En coherencia, el objetivo general de la investigación consiste en analizar la respuesta dogmático-penal, probatoria e institucional al phishing, contrastando los artículos 186, 190, 234, 455 y 49 del Código Orgánico Integral Penal con datos de la Fiscalía General del Estado (2015–2025). El estudio se justifica en la necesidad apremiante de dotar a operadores de justicia, litigantes y al sector bancario de criterios dogmáticos unificados que armonicen la tutela judicial efectiva con la seguridad técnica. Delimitar con precisión los alcances de los artículos 186 y 190 del COIP y mitigar la asimetría probatoria del usuario resulta indispensable no solo para garantizar la reparación integral de los afectados, sino también para salvaguardar la confianza pública y la estabilidad del sistema financiero digital ecuatoriana.

Método

La investigación se desarrolló entre septiembre de 2025 y julio de 2026, con participación de la Universidad Laica Eloy Alfaro de Manabí y consulta de información de la Fiscalía General del Estado en Manta. Adoptó un enfoque mixto: cualitativo, para interpretar normas, jurisprudencia y estándares de evidencia digital; y cuantitativo, para describir las noticias del delito registradas entre 2015 y 2025. Fue un estudio jurídico-dogmático, documental, descriptivo-analítico, comparado y propositivo. Su diseño fue no experimental, longitudinal retrospectivo para la serie fiscal y secuencial e integrado, pues la revisión jurídica orientó la clasificación de datos y estos se interpretaron a la luz del marco normativo.

La búsqueda documental partió de tres ejes: subsunción del phishing en el COIP; obtención, preservación y valoración de evidencia digital; y responsabilidad de autores, usuarios y entidades financieras. Se consideraron como fuentes primarias la legislación ecuatoriana, la jurisprudencia seleccionada, los estándares técnicos y las estadísticas oficiales; como fuentes secundarias, la literatura académica sobre phishing, fraude digital, prueba y responsabilidad bancaria citada en el artículo. Se utilizaron términos en español e inglés, combinados según cada eje: «phishing bancario», «fraude informático», «ciberestafa», «estafa», «apropiación fraudulenta por medios electrónicos», «evidencia digital», «cadena de custodia», «responsabilidad bancaria», «phishing bank», «cyber fraud» y «digital evidence». Para la búsqueda jurídica se añadieron los artículos 186, 190, 234, 455 y 49 del COIP y las disposiciones constitucionales pertinentes. Se priorizaron fuentes identificables, verificables y directamente relacionadas con el problema, así como textos oficiales frente a fuentes secundarias cuando abordaban el mismo asunto.

La selección atendió a pertinencia temática, identificación de autor o entidad responsable, disponibilidad de información verificable y utilidad para el contexto ecuatoriano o la comparación jurídica. Se excluyeron duplicados y materiales sin relación sustantiva con los ejes. La extracción registró fuente, fecha, jurisdicción, regla aplicable, elementos del tipo penal, tratamiento probatorio y datos relevantes. El análisis normativo examinó conducta, engaño, error, disposición patrimonial, uso de medios electrónicos y exigencias de prueba en los artículos del COIP considerados. El componente constitucional permitió contextualizar la tutela judicial efectiva, la propiedad y la protección de datos. La comparación se concentró en la Sentencia N.º 571/2025 del Tribunal Supremo de España; sus criterios se usaron como referencia interpretativa, sin trasladarlos automáticamente al ordenamiento ecuatoriano. El RFC 3227 se examinó como referente técnico para preservación y tratamiento de evidencia digital, no como norma penal nacional.

El componente empírico utilizó las Noticias del Delito del Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado, correspondientes a 2015–2025. La unidad de observación fue cada noticia registrada, no una sentencia ni necesariamente un hecho probado. Los datos se organizaron por año, infracción y variables disponibles, como flagrancia, grado de ejecución y distribución territorial. Se revisó la consistencia de las categorías y totales. El análisis estadístico fue descriptivo: frecuencias, porcentajes y cambios temporales. No se realizaron pruebas de significación ni inferencias causales. Las cifras se interpretaron conforme a las categorías administrativas y no se asumió que cada registro de estafa correspondiera a un caso de phishing. Finalmente, se integraron los resultados mediante triangulación temática entre el análisis dogmático, la serie fiscal y los requerimientos técnico-probatorios. La síntesis examinó la delimitación entre estafa y apropiación fraudulenta, la dificultad de investigar hechos no flagrantes, la asimetría en el acceso a registros y la atribución de responsabilidad institucional. Se distinguieron datos, interpretaciones jurídicas y propuestas. El alcance es analítico y contextual: los registros disponibles no permiten medir todos los ataques de phishing, identificar autores ni determinar por sí solos la negligencia de una víctima o entidad financiera.

Resultados

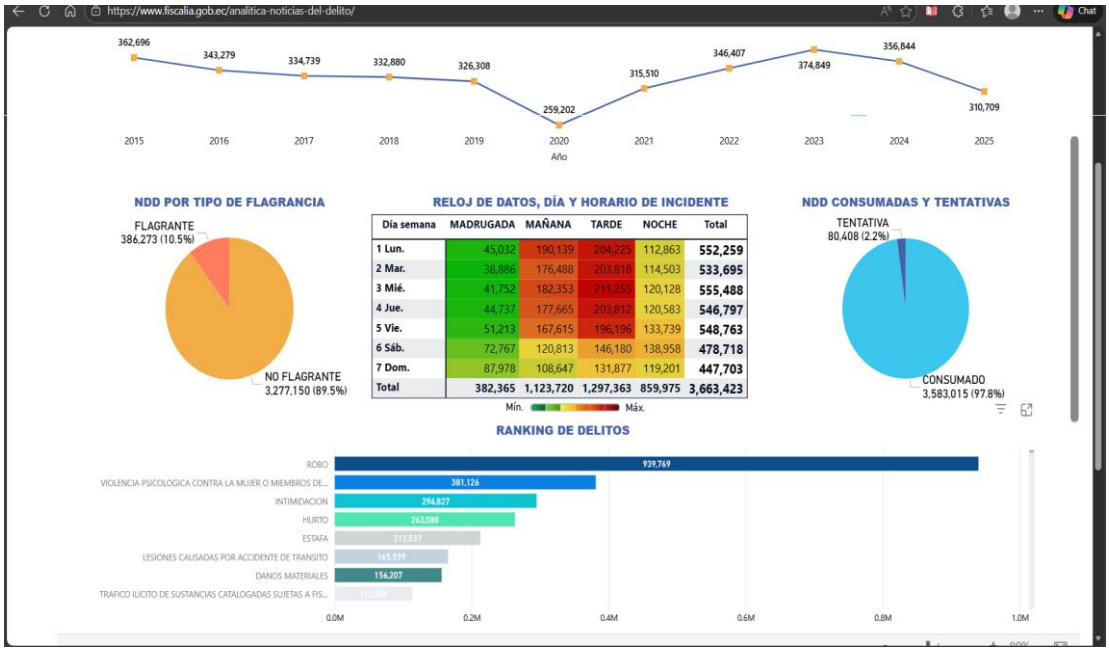
El presente apartado de resultados muestra el análisis criminológico y estadístico de la ciberdelincuencia patrimonial en el Ecuador (FGE 2015–2025), examina cuantitativamente la serie temporal 2015–2025 del SIAF de la Fiscalía General del Estado, con el fin de describir la evolución, distribución territorial y tendencias del phishing bancario y de otras formas de ciberdelincuencia patrimonial. Analiza la cadena criminológica del phishing y la distorsión procesal por subsunción típica y articula la revisión dogmática del COIP con el Examen Empírico en la Fiscalía.

Además, aborda la tensión dogmática entre estafa y apropiación fraudulenta, el régimen probatorio digital y la prueba diabólica, la responsabilidad cuasi-objetiva bancaria, el criminal compliance de la persona jurídica y la descomposición del nexo causal conforme al derecho comparado. La articulación de ambos niveles de análisis permite sostener que el phishing bancario no opera como un evento penal aislado, sino como un proceso lesivo y complejo que fractura las categorías procesales clásicas, impone cargas probatorias desproporcionadas a los usuarios y deja desprovistas de tutela judicial a las víctimas, configurando una crisis estructural en la respuesta del sistema de justicia ecuatoriano.

Análisis Criminológico y Estadístico de la Ciberdelincuencia Patrimonial en el Ecuador (FGE 2015–2025)

A nivel macro, el procesamiento de denuncias formalizadas que recoge la Figura 1 muestra que la Estafa (art. 186 del COIP) constituye la quinta infracción penal más frecuente en Ecuador, con 212.537 Noticias del Delito (NDD) en el período 2015–2025. Esta cifra la ubica por detrás de delitos de alta frecuencia fáctica como robo, violencia psicológica, intimidación y hurto, pero por delante de las lesiones por accidentes de tránsito (165.599 NDD) y del tráfico ilícito de sustancias catalogadas sujetas a fiscalización (113.385 NDD). La misma figura revela una tasa de no flagrancia del 89,5% y un 97,8% de delitos consumados, patrones que coinciden con la naturaleza encubierta y remota del phishing bancario. Asimismo, la serie temporal 2015–2025 presenta fluctuaciones constantes, con un pico en 2023 y un descenso hacia 2025, lo que refleja la persistente vulnerabilidad patrimonial frente a la estafa informática.

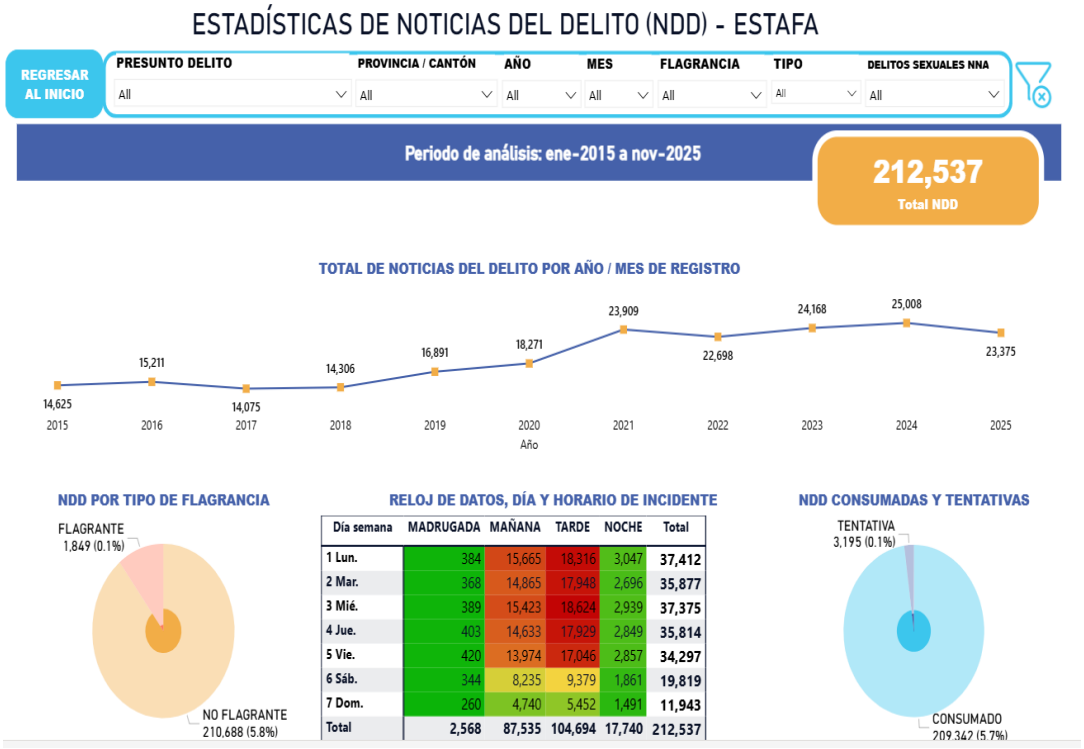
Figura 1. *Ranking Nacional de Noticias del Delito y Distribución de Flagrancia en Ecuador (2015–2025)*



Nota. Datos extraídos del Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía Fiscalía General del Estado (s. f.).

El análisis desagregado de la base de datos de la Fiscalía General del Estado, presentado en la Figura 2, revela dos indicadores críticos que definen la naturaleza asíncrona, remota y clandestina del fraude financiero telemático: la ausencia casi absoluta de flagrancia y la alta efectividad en la consumación del delito. Mientras que el promedio general de no flagrancia a nivel nacional se sitúa en el 89,5% (Figura 1), al filtrar los datos exclusivamente para el delito de Estafa, este índice se eleva hasta un 99,1% (210.688 NDD), registrándose una flagrancia marginal de apenas el 0,9% (1.849 NDD). Esta asimetría confirma que el anonimato digital y el distanciamiento espacial y temporal entre el agresor y la víctima imposibilitan la neutralización del delito en el acto de su comisión, consolidando así su carácter estructuralmente clandestino.

Figura 2. *Consumación y Reloj de Datos en el Delito de Estafa en Ecuador (2015–2025)*



Nota. Datos tomados de la Analítica de Noticias del Delito de la Fiscalía General del Estado (s. f.).

El análisis de la ejecución delictiva, contextualizado por la evolución temporal que muestra la Figura 3, revela un crecimiento sostenido de las denuncias por Estafa (art. 186 COIP), alcanzando un pico de 25.008 casos en 2024. En cuanto a su consumación, el 98,5% de las noticias del delito corresponden a actos plenamente consumados (209.342 NDD), frente a un residual 1,5% que quedó en grado de tentativa (3.195 NDD). Esta desproporción corrobora la efectividad de las maniobras de ingeniería social desplegadas en los ataques de phishing: una vez que la víctima entrega sus credenciales inducida por el engaño, la transferencia y el vaciado de las cuentas bancarias se concretan de forma inmediata y definitiva en el sistema financiero.

Figura 3. *Evolución Temporal de Noticias del Delito por Estafa (Art. 186 COIP)*



Nota. Registro histórico del SIAF Fiscalía General del Estado (s. f.).

La Figura 4 presenta la evolución temporal de las Noticias del Delito (NDD) por el delito de Apropiación Fraudulenta por Medios Electrónicos (Art. 190 COIP) durante el período 2015–2025. El gráfico de líneas muestra un comportamiento inicial a la baja (de 1.259 casos en 2015 a 959 en 2017), seguido de una tendencia ascendente sostenida que se acelera significativamente en 2020, alcanza un pico histórico en 2021 con 5.236 NDD, y tras un descenso en 2022 (3.136 NDD), retoma una curva de crecimiento constante hasta proyectar 4.732 NDD en 2025. En total, acumula 28.995 NDD por este tipo penal en la década. El incremento porcentual entre 2015 y 2025 es de 275,8%, lo que evidencia la aceleración exponencial de este delito, que emerge como el termómetro técnico más preciso para medir la consumación del phishing bancario en el país.

Figura 4. *Evolución Temporal del Delito de Apropiación Fraudulenta por Medios Electrónicos (Art. 190 COIP)*



Nota. Datos recopilados de la Fiscalía General del Estado (s. f.).

La Figura 5 presenta la evolución temporal de las NDD por el delito de Acceso No Consentido a un Sistema Informático (Art. 234 COIP) durante el período 2015–2025. Las estadísticas de la Fiscalía General del Estado evidencian una aceleración drástica en la apropiación fraudulenta: en 2015 se iniciaron 1.259 NDD; tras un intervalo de estabilidad moderada entre 2016 y 2018 (con registros de 959 a 1.451 causas anuales), el delito experimentó una escalada a partir de 2019 con 1.739 NDD y 2.281 NDD en 2020.

El año 2021 marcó un récord histórico con 5.236 denuncias, motivado por la digitalización bancaria forzosa durante la emergencia sanitaria del COVID-19 y la inserción de usuarios con escasa alfabetización digital. Posteriormente, el delito se estabilizó en umbrales elevados (3.136 NDD en 2022; 3.449 NDD en 2023; 3.701 NDD en 2024) y experimentó un nuevo repunte proyectado de 4.732 NDD para 2025. En el acumulado decenal de 28.995 causas, la apropiación fraudulenta creció un 275,8%, consolidándose como la infracción cibernética de mayor impacto económico directo para los cuentahabientes del Ecuador.

De manera complementaria, la Figura 5 evidencia el comportamiento del delito de Acceso No Consentido a un Sistema Informático (Art. 234 COIP), que refleja el ingreso ilegítimo de los atacantes a plataformas de home banking mediante claves robadas o tokens capturados. La tendencia muestra un ascenso superior al 500% en la última década, pasando de 142 causas en 2015 a 292 en 2020, 484 en 2023 y un récord de 941 denuncias en 2024, con 859 registros a noviembre de 2025. Este comportamiento ratifica la automatización y el perfeccionamiento técnico de las redes delictivas mediante bots para la suplantación masiva de identidades digitales.

Figura 5. *Evolución Temporal del Delito de Acceso No Consentido a un Sistema Informático (Art. 234 COIP)*



Nota. Analítica de la Fiscalía General del Estado (s. f.).

En contraposición, la Figura 6 examina el delito de Interceptación Ilegal de Datos (Art. 230 COIP), cuyo volumen acumulado es de apenas 732 NDD entre 2015 y 2025, con fluctuaciones anuales que oscilan entre 43 y 86 casos. Esta marginalidad cuantitativa arroja una conclusión criminológica fundamental: las redes de phishing en Ecuador no sustentan su modus operandi en la intercepción técnica compleja de paquetes de datos en tránsito, sino en la manipulación psicológica del usuario mediante ingeniería social, a través de enlaces engañosos, páginas espejo, mensajería de texto (smishing) y llamadas telefónicas fraudulentas (vishing).

Figura 6. *Evolución Temporal del Delito de Interceptación Ilegal de Datos (Art. 230 COIP)*



Nota. Estadística del SIAF (Fiscalía General del Estado, s. f.).

En consecuencia, el phishing bancario se revela no como un problema de vulneración de infraestructura tecnológica, sino como una patología de la confianza digital, lo que explica por qué los esfuerzos de persecución penal resultan insuficientes cuando se concentran en el rastreo técnico y no en la prevención del engaño.

Tensión Dogmática: Estafa Tradicional (Art. 186 COIP) frente a Apropiación Fraudulenta por Medios Electrónicos (Art. 190 COIP)

El análisis de adecuación típica arroja como resultado que la Estafa tradicional (Art. 186 COIP) no se ajusta plenamente al phishing bancario. Su estructura exige un engaño intersubjetivo que induzca a la víctima a realizar voluntariamente un acto de disposición patrimonial perjudicial. En el phishing, en cambio, el error se agota en la entrega inconsciente de credenciales, y el apoderamiento lo ejecuta el atacante mediante el sistema bancario automatizado, el cual no puede ser inducido a error en sentido psicológico-penal. Frente a esta limitación, el Art. 190 COIP describe con precisión la fase lesiva al sancionar el uso fraudulento de sistemas informáticos y la utilización indebida

de claves obtenidas ilegítimamente. Sin embargo, se identifica una asimetría punitiva: mientras la Estafa prevé cinco a siete años de privación de libertad, la Apropiación Fraudulenta contempla uno a tres años, lo que permite acceder con facilidad a medidas sustitutivas y genera que los operadores de justicia califiquen los hechos como estafa ordinaria, sacrificando la precisión dogmática.

Régimen Probatorio Digital: Protocolo RFC 3227 y la Nulidad de la Prueba Diabólica

El examen del régimen probatorio evidencia que la práctica bancaria de remitir extractos transaccionales en PDF carece de eficacia probatoria formal conforme al Art. 500 del COIP, que exige informe pericial informático con cadena de custodia y fijación de hash. Se constata que la metodología forense aplicable debe seguir el principio de volatilidad de la RFC 3227, iniciando por memoria RAM, caché y registros temporales, para luego abordar discos y logs del banco. Asimismo, el análisis revela que someter a la víctima a demostrar que no realizó la transferencia o que su equipo no estaba infectado constituye una prueba diabólica o de hechos negativos, vulnerando el debido proceso (Art. 76, num. 7, lit. h CRE). La carga de certificar la inviolabilidad de los canales digitales y la ausencia de anomalías recae sobre la entidad financiera, que ostenta el control exclusivo de la infraestructura.

Hacia un Régimen de Responsabilidad Cuasi-Objetiva Bancaria (Doctrina Comparada de la STS 571/2025)

El análisis jurisprudencial comparado identifica que la STS 571/2025 del Tribunal Supremo (2025), establece un estándar de responsabilidad cuasi-objetiva bancaria. Sus postulados principales son: la presunción de falta de autorización ante una transacción no reconocida, la inversión de la carga de la prueba sobre el banco, la obligación de reintegrar los fondos salvo prueba de dolo o negligencia grave del usuario, y la nulidad de cláusulas contractuales que pretenden deslindar la responsabilidad de la entidad. Se concluye que esta doctrina resulta aplicable en Ecuador conforme a los artículos 66 (numerales 19 y 26) y 82 de la CRE, pues la banca, al imponer canales electrónicos para reducir costos, asume una posición de garante sobre la custodia de los depósitos. La adhesión al Convenio de Budapest (Dictamen N.º 1-24-TI/24) complementa este régimen al facilitar la cooperación internacional.

Criminal Compliance y la Responsabilidad Penal de la Persona Jurídica (Art. 49 COIP)

El análisis del Art. 49 del COIP confirma que las personas jurídicas de derecho privado pueden ser penalmente responsables por delitos cometidos en su beneficio mediante la acción u omisión de sus directivos. En el fraude bancario digital, la atribución se fundamenta en la teoría del defecto de organización: si la entidad omite invertir en ciberseguridad o ignora auditorías sobre vulnerabilidades, facilita la consumación de apropiaciones fraudulentas (Art. 190 COIP) y accesos no consentidos (Art. 234 COIP). Se identifican como controles mínimos exigibles la autenticación biométrica distribuida y

los motores de prevención de fraude basados en aprendizaje automático. Acreditada la falta de control, el juzgador puede imponer las sanciones del Art. 70 COIP, y la articulación con el Art. 77 COIP permite que la reparación integral de la víctima no quede supeditada a la captura de redes transnacionales.

La Descomposición Dogmática del Phishing ante el Nexo Causal (Art. 455 COIP) y el Derecho Comparado

El análisis de imputación objetiva evidencia que el phishing fragmenta el engaño y el apoderamiento, tensionando el principio de tipicidad. En la Estafa clásica (Art. 186 COIP), los verbos simular o inducir a error exigen una relación intersubjetiva que en el phishing no se configura plenamente. En cambio, el Art. 190 COIP acierta al emplear los verbos utilizar fraudulentamente, emplear y procurar la transferencia no consentida, consolidando el nexo causal del Art. 455 COIP: la introducción no autorizada de credenciales es la causa necesaria e inmediata del menoscabo patrimonial. El examen comparado muestra que España, mediante el Art. 248.2 del Código Penal, y Estados Unidos, a través del Wire Fraud (§ 1343), la CFAA (§ 1030) y el Aggravated Identity Theft (§ 1028A), han segmentado o unificado la respuesta punitiva. Se concluye que Ecuador requiere unificar su respuesta penal sustantiva para evitar la desestimación o el archivo de causas por ruptura del nexo causal frente a tipos penales inadecuados.

En general, el análisis estadístico evidencia el crecimiento del phishing bancario, con 212.537 estafas y 28.995 apropiaciones fraudulentas, mientras la interceptación ilegal apenas suma 732 casos. Dogmáticamente, la estafa clásica no se ajusta al phishing, la prueba digital impone una prueba diabólica a las víctimas y se requiere responsabilidad cuasi-objetiva bancaria, criminal compliance y unificación del nexo causal conforme al derecho comparado.

Discusión

Los hallazgos confirman que el phishing bancario en Ecuador constituye una modalidad lesiva estructural y no un fenómeno penal aislado, pues su evolución cuantitativa, dogmática y procesal fractura las categorías clásicas del derecho punitivo. La articulación entre las Noticias del Delito de la FGE (2015–2025) y el Examen Empírico en la Fiscalía permite sostener que la ciberestafa patrimonial combina anonimato digital, ingeniería social y asimetría de información, imponiendo cargas probatorias desproporcionadas a las víctimas. Este apartado contrasta esos resultados con literatura internacional y doctrina comparada para situar la crisis ecuatoriana en un marco analítico más amplio y proponer reformas.

El incremento del 275,8% en la Apropiación Fraudulenta por Medios Electrónicos del Art. 190 COIP entre 2015 y 2025 y la tasa de no flagrancia del 99,1% en Estafa del Art. 186 COIP convergen con la literatura que documenta el desplazamiento del fraude hacia

entornos digitales asíncronos. La aplicación de la Teoría de las Actividades Cotidianas en Japón por Suzuki et al. (2025), evidencia que la victimización cibernética se asocia con exposición digital y baja supervisión tecnológica, rasgos materializados en Ecuador por el uso masivo de banca electrónica sin filtros suficientes.

La marginalidad de la Interceptación Ilegal de Datos del Art. 230 COIP, con apenas 732 NDD decenales, confirma que la cadena del phishing reposa en la manipulación psicológica y no en el ataque técnico. La victimización se explica, según Stalans et al. (2023), por factores cognitivos y emocionales como urgencia percibida y sesgos de confirmación, más que por sofisticación técnica. Los hallazgos de Ribeiro et al. (2024), demuestran que la susceptibilidad depende de autoeficacia percibida y exposición previa, no de variables demográficas. La revisión sistemática de Kavvadias y Kotsilieris (2025), confirma que los factores psicológicos predicen la vulnerabilidad con mayor potencia que los sociodemográficos. Desde la actividad rutinaria cibernética, Gan et al. (2024), demuestran que la exposición a atacantes motivados y la ausencia de capitales guardianes digitales explican la victimización.

En el plano dogmático, la asimetría punitiva entre Estafa tradicional del Art. 186 COIP, con 5 a 7 años, y Apropiación Fraudulenta por Medios Electrónicos del Art. 190 COIP, con 1 a 3 años, reproduce un problema de subsunción típica. La tesis de Sánchez Salazar et al. (2025), sostiene que la fragmentación del iter criminológico del phishing entre tipos penales analógicos genera impunidad práctica, pues los operadores prefieren calificar los hechos como estafa ordinaria para preservar la pena mayor y sacrifican precisión técnica. Los trabajos de Ruiz y Solis (2024) y Eslava-Zapata et al. (2024), documentan que la tipificación fragmentada en América Latina dificulta la imputación del nexo causal y propicia el archivo de causas.

Para el Equipo Giménez Salinas (2026), la segmentación operada en España mediante el Art. 248.2 del Código Penal y en Estados Unidos mediante Wire Fraud, CFAA y Aggravated Identity Theft ilustra rutas viables para unificar la respuesta sustantiva en Ecuador y reconstruir el nexo causal del Art. 455 COIP sobre la introducción no autorizada de credenciales como causa inmediata del menoscabo patrimonial.

Respecto al régimen probatorio, la práctica bancaria de remitir extractos en PDF sin cadena de custodia vulnera el Art. 500 del COIP y expone a las víctimas a una prueba diabólica, al obligarlas a demostrar que no realizaron la transferencia o que su equipo no estaba infectado. La advertencia de D'Anna et al. (2023), señala que la cadena de custodia forense debe actualizarse conforme al principio de volatilidad de la RFC 3227 y a estándares de integridad hash, dado que la evidencia digital es especialmente frágil. La omisión del peritaje informático formal anula la eficacia probatoria del extracto e invierte de facto la carga sobre el usuario, contraviniendo el Art. 76, numeral 7, literal h de la Constitución. La certificación de la inviolabilidad de los canales digitales debe recaer sobre la entidad financiera, que ostenta el control exclusivo del sistema.

La doctrina de responsabilidad cuasi-objetiva de la STS 571/2025 del Tribunal Supremo (2025), ofrece un paradigma trasplantable al ordenamiento ecuatoriano. Sus postulados de presunción de falta de autorización, inversión de la carga probatoria sobre el banco y reintegro salvo dolo o negligencia grave del usuario son coherentes con los Arts. 66, numerales 19 y 26, y 82 de la CRE. El examen de Horder (2025), sobre el Economic Crime and Corporate Transparency Act 2023 del Reino Unido defiende la responsabilidad de la persona jurídica fundada en el defecto de organización. Aplicada al Art. 49 del COIP, esta perspectiva permite atribuir responsabilidad a las entidades que omiten autenticación biométrica distribuida o motores de prevención basados en aprendizaje automático, y articula las sanciones del Art. 70 con la reparación integral prevista en el Art. 77 del COIP para las víctimas. La adhesión al Convenio de Budapest reforzaría este régimen al facilitar la cooperación internacional.

Conclusiones

El presente estudio cumplió con el objetivo de examinar integralmente la respuesta dogmática, procesal y constitucional del ordenamiento jurídico ecuatoriano frente al phishing en la banca digital, demostrando que la persecución punitiva individual clásica resulta insuficiente e ineficaz para garantizar la tutela judicial efectiva y la restitución del patrimonio de las víctimas.

Se evidenció que la mecánica lesiva del phishing, fundamentada en la convergencia de la ingeniería social sobre la voluntad del usuario y la intrusión técnica automatizada en los sistemas financieros, expone un desfase en el COIP. Aunque el artículo 190 del COIP tipifica la apropiación fraudulenta por medios electrónicos, su reducida escala penal no guarda proporcionalidad con la magnitud del perjuicio económico ni con el daño a la confianza pública, incentivando calificaciones erróneas en la fase preprocesal que conducen a la impunidad y al archivo sistemático de las causas.

Ante esta realidad, resulta imperativa una reforma legislativa que establezca circunstancias agravantes específicas para los delitos patrimoniales cometidos mediante tecnologías de la información que afecten al sistema financiero, equiparando su punibilidad a la del delito de estafa y graduando la sanción en función del impacto económico sustraído.

Asimismo, reconociendo que el derecho penal opera como última ratio, el Estado ecuatoriano debe estructurar una política criminal preventiva sustentada en programas nacionales de alfabetización digital y ciberseguridad ciudadana para mitigar la vulnerabilidad frente a la manipulación psicológica. Por su parte, el Consejo de la Judicatura y la Fiscalía General del Estado deben priorizar la capacitación especializada y permanente de jueces y fiscales en informática forense, con el propósito de garantizar

una correcta calificación típica inicial y una valoración técnica de la prueba digital basada en su naturaleza lógica, la cadena de custodia y el estándar RFC 3227.

Para cerrar la brecha de indefensión patrimonial, el sistema regulatorio y jurisprudencial ecuatoriano debe incorporar formalmente la doctrina comparada de la STS 571/2025 del Tribunal Supremo de España, transitando definitivamente del esquema de imputación de culpa subjetiva sobre el usuario hacia un modelo garantista de responsabilidad cuasi-objetiva bancaria, trasladando la carga de la prueba hacia quien está en posibilidad de proporcionarla. Esto obligará a las entidades financieras, por el riesgo profesional que introducen y explotan en el mercado, a asumir el deber reforzado de custodia e implementar barreras tecnológicas avanzadas, tales como la autenticación biométrica distribuida y motores de detección de anomalías transaccionales en tiempo real. Futuras investigaciones deberían evaluar la eficacia de los programas de compliance bancario en la reducción de la victimización y el impacto del Convenio de Budapest sobre la cooperación internacional en causas transfronterizas.

Acerca de

Contribución de los autores: Los autores contribuyeron a la conceptualización del estudio, al desarrollo metodológico, al análisis e interpretación de los datos, a la redacción del manuscrito y a la revisión crítica de su contenido intelectual. Ambos autores aprobaron la versión final para su publicación.

Financiamiento: Los autores declaran que no recibieron financiamiento para esta investigación.

Conflicto de interés: Los autores declaran no tener conflicto de intereses para la publicación del presente artículo científico.

Certificación ética: El protocolo del presente estudio fue sometido a revisión y aprobado por el Comité de Ética en Investigación de la Universidad, en cumplimiento de los principios éticos y normativas institucionales aplicables.

Referencias

Abad Arévalo, D., Peñaherrera Toapaxi, D., & Campos-Miño, S. (2023). Bases legales para la investigación científica en Ecuador: Ley orgánica de protección de datos personales. *MetroCiencia, 31*(1), 3–6. https://revistametrociencia.com.ec/index.php/revista/article/view/552

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences, 34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Altamirano Zavala, A. M. (2025). La apropiación fraudulenta por medios electrónicos y el bien jurídico protegido. *Ciencia Latina Revista Científica Multidisciplinar, 9*(3), 11420–11437. https://doi.org/10.37811/cl_rcm.v9i3.19080

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal. Registro Oficial, Suplemento n.º 180.* https://www.asambleanacional.gob.ec/es/multimedios-legislativos/35153-codigo-organico-integral-penal-1

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No. 459.* https://www.gob.ec/sites/default/files/regulations/2022-08/Ley-Org%C3%A1nica-Protecci%C3%B3n-Datos-Personales.pdf

Collantes Rodríguez, K. L. (2025). La imputación objetiva frente a los fraudes electrónicos: Evidencia de reformas normativas en un estudio de revisión sistemática. *Aula Virtual, 6*(13), 1869–1884. https://doi.org/10.5281/zenodo.17443011

Corte Constitucional del Ecuador. (2024). *Dictamen 1-24-TI/24: Convenio sobre Ciberdelincuencia.* https://www.corteconstitucional.gob.ec/kilur-archivo/dictamen-1-24-ti-24/

D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare, 11*(5), Article 634. https://doi.org/10.3390/healthcare11050634

De la Maza, I. A., & Mosqueira, B. L. (2024). El phishing más allá de la Ley N.º 20.009: El riesgo para quien lo controla. *Revista Justicia & Derecho, 7*(1), 1–24. https://doi.org/10.32457/rjyd.v7i1.2525

Domínguez Arteaga, R. A., & Vera Vázquez, R. (2022). Análisis espacial del ciberfraude al comercio electrónico: Consideraciones en agenda política Tamaulipeca. *PODIUM, (41), 21*–40. https://doi.org/10.31095/podium.2022.41.2

Equipo Giménez Salinas. (2026, 4 de junio). *El fraude bancario digital: Un desafío común con respuestas regulatorias divergentes entre España, la Unión Europea y Estados Unidos.* Giménez-Salinas. https://gimenez-salinas.es/fraude-bancario-digital-responsabilidad-banco/

Eslava-Zapata, R., Rojas-Hermida, C. J., & García-Peñaloza, J. E. (2024). Variables asociadas a los delitos informáticos en Latinoamérica. *Academia & Derecho, 17*(28), 1–21. https://doi.org/10.18041/2215-8944/academia.28.11822

Fiscalía General del Estado. (s. f.). Analítica noticias del delito. https://www.fiscalia.gob.ec/analitica-noticias-del-delito/

Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: Predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model. *Humanities and Social Sciences Communications, 11*, Article 1552. https://doi.org/10.1057/s41599-024-04083-1

Horder, J. (2025). Corporate criminal liability under the Economic Crime and Corporate Transparency Act 2023. *Legal Studies, 45*(1), 133–148. https://doi.org/10.1017/lst.2024.46

Jamardo Lorenzo, A. (2024). La configuración de la cadena de custodia tecnológica en el ordenamiento jurídico español. *Ius et Scientia, 10*(2), 101–122. https://doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Junta de Política y Regulación Financiera. (2021, 30 de diciembre). *Resolución No. JPRF-F-2021-008.* https://www.bce.fin.ec/storage/JPRF/2021/JPRF-F-2021-008.pdf

Kavvadias, A., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences, 15*(4), Article 2236. https://doi.org/10.3390/app15042236

Mayer Lux, L. V., & Toso Milos, Á. (2024). La facilitación de medios al interior de la empresa para la comisión de un fraude informático: Problemas dogmáticos y relativos al compliance. *Revista Chilena de Derecho y Tecnología, 13*, Artículo e72932. https://doi.org/10.5354/0719-2584.2024.72932

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security, 132*, Article 103387. https://doi.org/10.1016/j.cose.2023.103387

Portilla, R. E., Menza, E. J., & Portilla, M. P. (2025). Delitos informáticos en el Código Orgánico Integral Penal: Una revisión sobre acceso no autorizado, fraude digital y ciberseguridad en Ecuador. *Pro Sciences: Revista de Producción, Ciencias e Investigación, 9*(60), 114–127. https://journalprosciences.com/index.php/ps

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security, 136*, Article 103558. https://doi.org/10.1016/j.cose.2023.103558

Ruiz, P., & Solis, J. C. (2024). Fraude informático en la modalidad de phishing en Lima. *Revista Escpogra PNP, 3*(2), 143–155. https://doi.org/10.59956/escpograpnpv3n2.12

Sánchez Salazar, P. M., Araujo Arízaga, A. A., & Salinas Herrera, F. M. (2025). Responsabilidad penal por manipulación digital con fines delictivos: Una mirada desde el derecho digital comparado en América Latina. *Cuestiones Políticas, 43*(83), 42–55. https://doi.org/10.5281/zenodo.17756519

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, Article 324. https://doi.org/10.1007/s10462-024-10973-2

Stalans, L., Chan-Tin, E., Hart, A., Moran, M., & Kennison, S. (2023). Predicting phishing victimization: Comparing prior victimization, cognitive, and emotional styles, and vulnerable or protective e-mail strategies. *Victims & Offenders, 18*(7), 1216–1235. https://doi.org/10.1080/15564886.2023.2218369

Suzuki, A., Shikata, K., & Shimada, T. (2025). Patterns and predictors of cyber fraud victimization: Testing routine activity theory and general theory of crime in Japan. *Journal of Economic Criminology, 9*, Article 100186. https://doi.org/10.1016/j.jeconc.2025.100186

Tixi, S. G., Merizalde, M. L., Romero, A. J., & Jordán, G. V. (2023). Los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 8*(1), 51. https://doi.org/10.35381/racji.v8i1.3339

Tribunal Supremo (Sala de lo Civil). (2025, 9 de abril). *Sentencia núm. 571/2025 (Recurso de casación núm. 1151/2023).* https://vlex.es/vid/1078350756

 Este artículo está bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0).