UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO EN LÍNEA

MARCO JURÍDICO ECUATORIANO VERSUS CONVENIO DE BUDAPEST: ANÁLISIS COMPARATIVO DE LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN PHISHING TRANSFRONTERIZO DURANTE EL PERÍODO 2020-2024

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

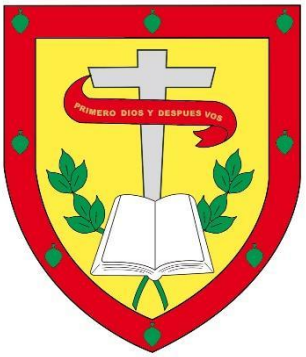
AUTOR: DAYANARA JACQUELINE REYES QUEZADA

DIRECTOR: ABG. CRISTIAN ANDRÉS PALACIOS RODAS MGS.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO EN LÍNEA

MARCO JURÍDICO ECUATORIANO VERSUS CONVENIO DE BUDAPEST: ANÁLISIS COMPARATIVO DE LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN PHISHING TRANSFRONTERIZO DURANTE EL PERÍODO 2020-2024

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

AUTOR: DAYANARA JACQUELINE REYES QUEZADA

DIRECTOR: ABG. CRISTIAN ANDRÉS PALACIOS RODAS MGS.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

DAYANARA JACQUELINE REYES QUEZADA portador(a) de la cédula de ciudadanía Nº **0706699758**. Declaro ser el autor de la obra: **"Marco jurídico ecuatoriano versus convenio de Budapest: análisis comparativo de la recolección de evidencia digital en phishing transfronterizo durante el período 2020-2024"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **23 de octubre de 2025**

F: .....

Dayanara Jacqueline Reyes Quezada

C.I. **0706699758**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente trabajo de investigación fue desarrollado por **Dayanara Jacqueline Reyes Quezada** con número de cédula **0706699758** con el tema **"Marco jurídico ecuatoriano versus Convenio de Budapest: análisis comparativo de la recolección de evidencia digital en phishing transfronterizo durante el período 2020-2024"**, bajo mi supervisión.

DR CRISTIAN ANDRÉS PALACIOS RODAS

DOCENTE TUTOR

Dedicatoria

Con el corazón lleno de gratitud, dedico este logro primeramente a Dios, por ser mi guía constante, por darme fortaleza en los momentos de duda y por iluminar mi camino con fe y esperanza. Gracias por enseñarme que cada esfuerzo tiene su recompensa. A la persona en la que me he convertido, por la determinación de continuar, por no rendirse ante las adversidades y por transformar cada caída en una oportunidad para crecer. A mis padres, por su amor incondicional, comprensión y apoyo constante; por ser mi mayor inspiración y motivo para seguir adelante. A mis hermanos, por su cariño, consejos y aliento que fortalecieron mi espíritu en los momentos más difíciles. Y a mi fiel compañero Tommy, por su silenciosa compañía y ternura, por estar a mi lado en cada noche de esfuerzo y estudio, recordándome que el amor también se demuestra en los pequeños gestos.

Resumen

El estudio tuvo como finalidad analizar la regulación del phishing transfronterizo y la recolección de evidencia digital en el marco jurídico ecuatoriano, contrastándolo con los estándares internacionales del Convenio de Budapest, a fin de identificar vacíos normativos y limitaciones en la aplicación práctica. Se realizó investigación cualitativa documental mediante búsqueda sistemática en bases de datos Scielo, Redalyc, Google Scholar y repositorios universitarios ecuatorianos, período enero 2020-diciembre 2024. Términos de búsqueda: "phishing Ecuador", "evidencia digital", "Convenio Budapest", "ciberdelincuencia" en español e inglés. Criterios de inclusión: artículos peer-reviewed, tesis maestría/doctorado, documentos oficiales. Exclusión: fuentes sin validación académica, anteriores a 2020. El análisis evidenció que el COIP tipifica conductas asociadas al phishing, pero mantiene un enfoque sancionatorio sin lineamientos técnicos claros para la recolección y preservación de evidencia digital. Por otro lado, el Convenio de Budapest establece mecanismos avanzados de cooperación y conservación de datos que resultan más efectivos frente a la volatilidad de la información. También se identificaron vacíos normativos en la normativa ecuatoriana, especialmente en materia de jurisdicción y coordinación interinstitucional. Se concluye que Ecuador enfrenta limitaciones estructurales y normativas para la persecución del phishing transfronterizo. La adhesión al Convenio de Budapest surge como una alternativa viable, siempre que se complemente con reformas internas, fortalecimiento institucional y desarrollo de protocolos técnicos que garanticen la validez de la evidencia digital en procesos judiciales internacionales.

Palabras claves: *Phishing transfronterizo, Evidencia digital, Cooperación internacional.*

Abstract

This research aimed to analyze regulations of transnational phishing and the collection of digital evidence within the Ecuadorian legal framework, contrasting them with the international standards of the Budapest Convention, to identify normative gaps and limitations in practical application. A qualitative documentary study was conducted through a systematic search in databases such as SciELO, Redalyc, Google Scholar, and Ecuadorian university repositories, during the period January 2020-December 2024. Searching terms included "phishing Ecuador," digital evidence," "Budapest Convention," and "cybercrime," in Spanish and English. Inclusion criteria: peer-reviewed articles, Master's degree/PhD theses, and official documents. Exclusion: sources lacking academic validation, before 2020. This analysis revealed that the Comprehensive Organic Penal Code (COIP, by its Spanish acronym) criminalizes behavior associated with phishing, but maintains a punitive approach without clear technical guidelines for the collection and preservation of digital evidence. On the other hand, the Budapest Convention establishes advanced mechanisms for cooperation and data preservation that are more effective against the volatility of information. Additionally, regulatory gaps were identified in Ecuadorian legislation, particularly regarding jurisdiction and inter-institutional coordination. The conclusion is that Ecuador faces structural and regulatory gaps for the prosecution of transnational phishing. Adherence to the Budapest Convention emerges as a viable alternative, provided it is complemented by local reforms, institutional reinforcement, and the development of technical protocols that guarantee the validity of digital evidence in international judicial proceedings.

Keywords: *Transnational phishing, digital evidence, international cooperation*

Marco jurídico ecuatoriano versus Convenio de Budapest: análisis comparativo de la recolección de evidencia digital en phishing transfronterizo durante el período 2020-2024

Ecuadorian legal framework versus the Budapest Convention: Comparative analysis of the collection of digital evidence in cross border phishing during the period 2020-2024

Introducción

En la actualidad, el phishing transfronterizo se ha establecido como uno de los peligros cibernéticos más relevantes, caracterizado por utilizar técnicas fraudulentas para obtener claves y datos personales. Este delito no solamente genera un deterioro financiero en las víctimas, sino también se presenta como un reto para la justicia penal, ya que la evidencia digital puede estar distribuida en distintas jurisdicciones y su conservación rápida es fundamental para la acción procesal.

En Ecuador, el Código Orgánico Integral Penal (COIP, 2014), establece como delito situaciones relacionadas con la estafa digital, el ingreso a sistemas y la intervención ilegal de información. Sin embargo, el marco penal vigente todavía demuestra vacíos y carencias en los procesos técnicos para recolectar, conservar y acceder a pruebas digitales, lo cual es una barrera para la comprobación de evidencia en los procedimientos legales cuando los ataques son ocasionados fuera del ámbito ecuatoriano.

Por su parte, el Convenio de Budapest (2001), plantea normas concretas para la conservación inmediata de datos y al mismo tiempo buscando la cooperación internacional relacionada con delitos informáticos. Estas acciones han reforzado la veracidad y el seguimiento de pruebas en situaciones transnacionales. Pese a ello, el Ecuador no ha implementado estas reglamentaciones, lo cual demuestra la importancia de analizar jurídicamente ambos cuerpos legales.

Bajo este contexto, la importancia de la presente investigación se encuentra en que el phishing transfronterizo no solamente es un problema técnico, sino también representa un desafío en el ámbito jurídico que requieren respuestas sincronizadas. La comparación entre el sistema penal de Ecuador y el Convenio de Budapest posibilitará

la identificación de oportunidades estratégicas, las cuales servirán como un esquema sólido para optimizar la normativa ecuatoriana.

A través de esta problemática, se origina la pregunta de investigación: ¿Cuáles son las principales brechas y desafíos del marco jurídico ecuatoriano en la recolección de evidencia digital para casos de phishing transfronterizo, en comparación con los estándares y principios clave del Convenio de Budapest durante el periodo 2020-2024? En relación con el objetivo general del estudio, se busca analizar la comparación de ambos marcos jurídicos para identificar los vacíos y las buenas prácticas de la investigación penal.

Además, por medio de los objetivos específicos se busca identificar las disposiciones normativas, describir los principios y estándares específicos del Convenio de Budapest relativos a la recolección y preservación de evidencia digital transfronteriza y analizar las brechas y convergencias entre el marco jurídico ecuatoriano y los principios del Convenio de Budapest para observar las fortalezas y debilidades del sistema nacional.

En cuanto a la metodología, la investigación adopta un enfoque cualitativo, descriptivo-explicativo y comparativo para contrastar la legislación y práctica ecuatoriana con el Convenio de Budapest. Se aplicará un método jurídico-comparativo para establecer similitudes, diferencias, brechas y convergencias entre la normativa. Dogmático-Jurídico para el análisis profundo de la normativa ecuatoriana y los artículos específicos del Convenio de Budapest relacionados con la recolección de evidencia digital. Finalmente, documental para la recopilación y análisis crítico de jurisprudencia nacional relevante y doctrina especializada sobre el tema.

Finalmente, el desarrollo del estudio está estructurado en cinco ítems claves como la evolución del phishing transfronterizo como delito cibernético, el marco

jurídico ecuatoriano, los estándares internacionales del Convenio de Budapest, comparación de ambos marcos normativos y la demostración de casos relacionado con el tema abordado. De tal manera, el artículo proporciona un rol académico significativo y práctico enfocado para mejorar la respuesta de casos nacionales frente a los ciberdelitos.

Metodología

La presente investigación se desarrolló bajo un diseño metodológico de naturaleza cualitativa, ya que busca comprender en profundidad los fenómenos jurídicos, tecnológicos y sociales involucrados en la recolección de evidencia digital transfronteriza y su impacto en el debido proceso penal.

Por otra parte, también se encuentra catalogado dentro de un enfoque descriptivo-explicativo para caracterizar los desafíos y comprender las relaciones causales entre la dificultad de obtención de evidencia y las afectaciones al debido proceso. Además, se emplea un enfoque comparativo para contrastar la legislación y práctica ecuatoriana con el Convenio de Budapest.

El tipo y método de investigación utilizado para el proyecto es jurídico-comparativa para establecer similitudes, diferencias, brechas y convergencias entre la normativa ecuatoriana y el Convenio de Budapest. Procedimiento: Se definirá un conjunto de categorías y principios clave de la recolección de evidencia digital y se compararán sus tratamientos en ambos cuerpos normativos.

Además, el método dogmático-jurídico ayudó al análisis de manera profunda de la normativa ecuatoriana (COIP, y del Convenio de Budapest) y los artículos específicos del Convenio de Budapest relacionados con la recolección de evidencia digital y documental para la recopilación y análisis crítico de jurisprudencia nacional relevante y doctrina especializada sobre el tema.

Las técnicas utilizadas incluyeron el análisis contenido cualitativo aplicado a las normativas, sentencias y doctrina, para identificar categorías, patrones, brechas y convergencias en la recolección de evidencia digital. La elaboración de matrices comparativas siendo una técnica clave para contrastar de manera estructurada los artículos y principios del marco ecuatoriano y el Convenio de Budapest en relación con

la recolección de evidencia y la revisión bibliográfica sistemática para identificar y seleccionar la doctrina y jurisprudencia más relevante y actualizada.

Los instrumentos utilizados para el proyecto investigativo es la matriz análisis normativo la cual sirvió para desglosar y comparar artículos específicos del COIP y del Convenio de Budapest en cuanto a procedimientos, requisitos y principios de recolección de evidencia digital. Incluirá columnas para la norma/artículo, descripción, procedimiento, requisitos, y su paralelo/contraste con el otro marco. Además, de la ficha de análisis jurisprudencial/doctrinal para extraer información relevante de sentencias y textos académicos que aborden la recolección de evidencia digital en phishing transfronterizo, identificando criterios de aplicación, desafíos y limitaciones.

El universo de estudio para esta investigación está formado por el conjunto de normativas legales ecuatorianas relevantes para la evidencia digital y el proceso penal como es el caso del Código Orgánico Integral Penal. Así también, con estudios relacionados con ciberdelitos y evidencia digital, además del Convenio de Budapest sobre Ciberdelincuencia, y la doctrina jurídica y académica nacional e internacional publicada en el ámbito del derecho informático, procesal penal y cooperación internacional en ciberdelincuencia en los últimos cuatro años.

Dada a la naturaleza documental de la investigación, no se seleccionará una muestra cómo se acostumbra de manera estadística tradicional. En su lugar, se realizará una selección intencional y profunda de la literatura más relevante y actualizada en del periodo 2021-2025 que aborde los desafíos de la evidencia digital transfronteriza, el impacto en el debido proceso penal, y el rol del Convenio de Budapest. Esto incluirá artículos de revistas científicas indexadas, informes de organismos internacionales como es el caso del Consejo de Europa, el UNODC, la INTERPOL, y normativas ecuatorianas que traten sobre la obtención de evidencia digital. g

En relación con el análisis de datos, se codificó la información investigada mediante triangulación, fuentes revisadas enfocadas en doctrinas y normativas aplicando comparación para identificar los elementos y patrones jurídicos. Finalmente, se incorporaron una narrativa de manera coherente y lógica.

Desarrollo

Phishing transfronterizo y su evolución como delito cibernético

De acuerdo con Clancy (2023), el phishing transfronterizo tuvo sus primeras apariciones en la década de los noventa a través de e-mail que tienen como finalidad estafar a las personas con enlaces engañosos. Ahora bien, el crecimiento del comercio digital y la ampliación internacional de la web 2.0 expandieron significativamente la cobertura de estas prácticas.

Además, la evolución del phishing transfronterizo no solamente demuestra la perfección de los métodos digitales, sino también la programación del internet y la carencia de regulaciones ante esta problemática a nivel global. Por consiguiente, la limitación de controles en el contexto internacional posibilitó que actos ilícitos simples proviniera de una amenaza global, lo que impidió actuar de manera rápida a los cuerpos jurídicos tradicionales.

Posteriormente Casey (2011), señaló que la evolución de phishing transfronterizo apareció con el surgimiento de sitios web maliciosos parecida a páginas en líneas certificadas, enfocadas en persuadir a los usuarios. En particular, con la expansión de las redes sociales y la comunicación rápida por medio de mensajería, los ciberdelincuentes desarrollaron nuevos métodos para el obtener datos. Asimismo, aunque los organizamos mejoraron sus mecanismos de defensa, los delincuentes aplicaron software malicioso para conseguir información de las víctimas en tiempo real.

Desde este criterio, lo más fundamental no solamente es la evolución de la tecnología, sino también la manera en que los atacantes informáticos mejoraron la forma de interacción digital para tener un mayor alcance en la sociedad. De este modo, el uso de plataformas multimedia y de correo electrónicos generó las rutas necesarias

para el robo de datos de los usuarios. Esto demuestra que esta problemática no se enfoca en sistemas vulnerables, sino en cómo se manipula al usuario.

De igual forma, un estudio realizado por las Naciones Unidas contra la Droga y el Delito (UNODD, 2022), detalló que otra etapa de la evolución del phishing transfronterizo se distingue por la expansión de técnicas como el *smishing* (mensajes de texto) y el *vishing* (llamadas automatizadas). A la par, los ciberdelincuentes acuden a la clonación de plataformas online y a la utilización de bitcoin para disimular las transacciones. Esto demuestra que los métodos estratégicos defensivos progresan, mientras que los hackers demuestran adaptarse a nuevas situaciones para realizar sus ataques.

Pese a lo anterior, se muestra que las respuestas de organismos no se han adelantado con la misma agilidad. Por otra parte, detectar nuevos métodos como la utilización de criptomonedas no soluciona problemas como la deficiencia en las regulaciones y la sincronización de las entidades gubernamentales para afrontar este impacto. Esto demuestra que esta problemática no radica solamente en la innovación de los ciberdelincuentes para cometer el robo de datos digitales, sino también en el retraso de las normativas para responder a este tipo de situación.

En esa línea, un informe de la Organización Internacional de Policía Criminal (Interpol, 2024), demostró que los ciberdelincuentes que aplican el phishing transfronterizo operan en diversas jurisdicciones donde coordinan con servidores de diferentes naciones para realizar sus ataques en distintas regiones de un país, aprovechándose de las carencias normativas y la falta de sincronización de los Estados ante este tipo de situación.

Si bien suele sostenerse que el origen del phishing transfronterizo se origina por las deficiencias normativas y en la evolución digital, tal enfoque es limitado debido a

que excluye otros factores como la educación y capacitación tecnológica para la prevención de ataques digitales. En este contexto, enfocarse solamente en elementos jurídicos y técnicos reduce la responsabilidad social en el desarrollo de conciencia en relación con este tipo de delitos.

En definitiva, la efectividad para contrarrestar esta situación en la sociedad dependerá de la formación proporcionada a los usuarios, lo cual ayudará a identificar los riesgos y prevenir caer en estos engaños digitales. Por tanto, enfocar únicamente esta problemática a lo legal y tecnológico encamina a un entiendo parcial de este fenómeno.

Marco jurídico ecuatoriano para recolección de evidencia digital

Cabe destacar que la Constitución de la República del Ecuador (2008), asegura proteger los datos personales, el acceso a la información, a la intimidad y el respeto al debido proceso de los ciudadanos.

Estos principios plantean que obtener y valorar las pruebas deberán ejecutarse con argumentos de legalidad y confiabilidad, lo cual significa una relevancia en enfoques digitales donde el phishing transfronterizo pone en riesgo los datos personales y existe directrices rigurosas en la obtención de evidencia digital.

Por otra parte, en el contexto penal ecuatoriano el Código Orgánico Integral Penal (COIP, 2014), expone las conductas en las que surgen de manera sospechosa los sistemas informáticos o de telecomunicación para adueñarse o traspasar bienes sin consentimiento, lo cual significa un atentado ante la confianza en las plataformas digitales. Esta norma se tiene el enfoque más cercano al phishing transfronterizo dentro de la jurisdicción del país, ya que demuestra el aprovechamiento ilícito de datos personales de usuario para actos indebidos (Art.190).

Ahora bien, esto refleja una dificultad importante, debido a que la normativa ecuatoriana no establece claramente la dimensión territorial de su aplicación. En casos

de phishing transfronterizo, los ataques informáticos suelen aparecer mediante servidores u otros factores como responsables fuera del país, lo cual dificultan con exactitud que la normativa resulte competente para procesar estos ataques digitales. En consecuencia, el sistema penal del país demuestra limitaciones y carencias para penalizar casos phishing transfronterizo, lo que demuestra la importancia de cooperación con organismos internacionales que fortalezcan la eficiencia de la norma ecuatoriana.

Asimismo, dentro de la misma normativa se identifican otros actos ilícitos como la usurpación, donde el COIP (2014), busca resguarda la propiedad de los ciudadanos y al mismo tiempo proporcionar estabilidad social ante la apropiación indebida de inmuebles y de los derechos reales correspondientes (Art. 200).

En este enfoque, se demuestra que el sistema normativo está desactualizado al limitarse únicamente a bienes patrimoniales y no abordar contextos tecnológicos, donde en situaciones de phishing transfronterizo los robos se relacionan directamente con el despejo de cuentas bancarias o de datos personales. De ahí que esta limitación debilita el sistema penal ecuatoriano ante estos casos, dejando vacíos que podrían sancionar a personas involucradas a ciberdelitos en el Ecuador.

En concordancia con lo analizado, el Código Orgánico Integral Penal (2014), penaliza la divulgación ilícita de información encontrada en archivos o en bases de datos, cuando esta es dispersada sin consentimiento y con el objetivo de atentar contra la intimidad de una persona. Esta disposición demuestra las intenciones de los delitos cibernéticos, los cuales buscan conseguir de manera inadecuada los datos privados de usuarios para ser usadas con fines maliciosos, afectando así de manera directa los derechos claves en el ámbito digital (Art. 229).

A pesar de lo anterior, el artículo se limita es castigar la propagación y robo de datos sin establecer mecanismos que garanticen proteger de manera eficaz la intimidad de las personas en contextos internacionales. En situaciones de phishing transfronterizo, la información extraída puede expandirse de manera masiva en redes internacionales, vulnerando a los usuarios a riesgos donde sus datos personales pueden ser utilizados con fines maliciosos. Por lo tanto, esta carencia de alcance jurídico minimiza la capacidad del sistema penal de Ecuador para resguardar los derechos de las víctimas ante la obtención ilegal de datos.

En este sentido, el COIP (2014), tipifica como delito la intercepción ilícita de datos en diversas modalidades, desde la clonación de tarjetas, el desarrollo de páginas web falsas y el desvío de conversaciones para el espionaje. Estos actos se relacionan directamente con los métodos aplicados por los ciberdelincuentes en el phishing transfronterizo (Art. 230).

Aunque la normativa penaliza explícitamente estos actos, todavía se presenta una limitación para las sanciones al no plantear directrices para preservar y resguardar la evidencia digital en el contexto ecuatoriano. En casos de phishing transfronterizo es muy complicado asegurar la autenticidad de los datos interceptados o sitios engañosos desarrollados en estructuras digitales internacionales dentro de un procedimiento judicial de Ecuador. Así, este vacío en la jurisdicción ecuatoriana minimiza la eficiencia de esta disposición ante la complejidad de estos casos.

Como fase subsiguiente, el mismo marco normativo determina el acceso no autorizado a sistemas digitales, donde describir la conducta de intervenir sin autorización o apropiarse de información en contra de la voluntad del usuario (Código Orgánico Integral Penal, 2014, Art 234). Este tipo de acceso es la que genera los casos phishing transfronterizo, en el que, mediante la usurpación de datos personales, los

ciberdelincuentes suelen vaciar cuentas bancarias o divulgar o vender datos de los ciudadanos a otras entidades.

Sin embargo, el enfoque del artículo carece de previsiones acerca de la cooperación internacional, la cual es fundamental para el rastreo de robos tecnológicos en que en contextos de phishing transfronterizo se originan en direcciones IP extranjeras. La falta de mecanismos procesales de sincronización representa una barrera para la validación de pruebas digitales cuando los ataques de phishing vienen de diversas jurisdicciones. Esto refleja una vacío que limita la eficacia de la norma penal ecuatoriana ante este tipo de caso.

De manera complementaria el Código Orgánico Integral Penal (2014), penaliza la falsificación digital, enfocadas en la eliminación o modificación de contenido tecnológico con el objetivo de desarrollar archivos no genuinos o introducir errores en las relaciones jurídicas (Art. 234.1).

En este sentido, la normativa tampoco plantea cómo debe validarse la autenticidad de archivos digitales demostrado como una evidencia. En contextos de phishing transfronterizo, estos casos adquieren gran importancia, ya que los documentos pueden ser modificados o clonados en diversos aspectos tecnológicos, solicitando así pericias elaboradas en sincronización con organismos internacionales que ayuden a la certificación de validez en los procesos jurídicos del país.

Desde una perspectiva procesal, el COIP (2014), establece las atribuciones que tiene el fiscal, donde se resalta la preservación obligatoria de evidencia digital por medio cadena de custodia relacionados a casos de allanamiento de dispositivos tecnológicos. Esto demuestra un avance fundamental debido a que proporciona una normativa adecuada para asegurar los indicios digitales, a pesar de aquello, su eficacia es cuestionado cuando las pruebas son identificadas en el extranjero (Art. 444).

En consecuencia, la normativa no desarrolla procesos explícitos para contextos en que las pruebas se encuentran en servidores internacionales, lo cual restringe su eficiencia ante el phishing transfronterizo. En este tipo de situación, la cooperación y sincronización internacional es necesaria para resguardar la verificación de registros. Por ello, aunque se reconoce lo fundamental que es la cadena de custodia, su uso práctico en casos iliciticos globales aun demuestra carencias.

Estándares internacionales específicos del Convenio de Budapest

En primera instancia, el Convenio de Budapest (2001), establece la conservación inmediata de datos digitales, incluyendo el registro de tráfico tecnológico, con la finalidad de evitar que las pruebas desaparezcan o sean manipuladas antes que los organismos especializados puedan utilizarlas (Art.16).

Conviene subraya que, al movilizar esta acción a la práctica, en especial en situaciones de phishing transfronterizo, aparecen inconvenientes relacionados a la desigualdad de los Estados para llevar un ordenamiento ejecutivo rápido para conservar datos. Esta diferencia conlleva el peligro en que la evidencia no se establezca de forma adecuada o incluso pueda perderse en normativas con menor eficacia en ámbitos tecnológicos.

Seguidamente, en este tratado internacional se regula la conservación y revelación inmediata de la información traficada de manera digital (Convenio de Budapest, 2001, Art. 17). Esta resolución ayudará a la identificación de los proveedores de servicios que suelen intervenir en las conversaciones y seguir la ruta de esta mediante diversas redes.

Su contribución es fundamental en casos de phishing transfronterizo, debido a que brinda la ruta necesaria para desarrollar la cadena de transmisión y al mismo tiempo poder identificar a los actores que posibilitan el robo y la divulgación de datos digitales.

En tal sentido, este modelo mejora la cooperación y sincronización inmediata entre los organismos internacionales y las entidades de un país, facilitando así penalizar los casos de robos cibernéticos, siendo una herramienta crucial para coordinación conjunto ante este tipo de persecución.

De forma complementaria, dentro de esta misma normativa internacional, se plantea que todas las autoridades podrán intervenir en tiempo real el contenido de las comunicaciones digitales que se encuentren relacionadas con actos ilícitos graves (Convenio de Budapest, 2001, Art 21). Esta disposición proporciona a los Estados la posibilidad de aplicar métodos técnicos y de reclamar la cooperación de proveedores en servicios digitales, con términos de confidencialidad.

La aplicación de esta disposición adquiere relevancia ante en caso de phishing transfronterizo, debido a que ayudará a los organismos a capturan rápidamente los datos que son intercambiados mediante la ejecución de los ataques informáticos. De tal modo, se proporciona al estudio una ventaja significativa que posibilitará una reacción rápida ante los delitos cibernéticos internacionales, optimizando la prevención y los métodos para evitar las acciones ilegales que por su dinámica podrían desaparecer inmediatamente.

Adicionalmente, el Convenio de Budapest (2001), incorpora los principios que buscan las asistencias de indagación internacional. Estos engloban desde la utilización equipos de comunicación rápidos y seguros hasta la necesidad de reducir las barreras que podrían retrasar la cooperación entre países (Art. 25).

En situaciones de phishing transfronterizo, esta disposición adquiere gran relevancia práctica al plantear rutas legales y procesos reconocidos que ayuden a los organismos intercambiar evidencias digitales de manera válida. Con estos procesos se

podrá impedir que las pruebas tecnológicas queden en la impunidad y se asegure que pueda ser usada de eficientemente en actuaciones judiciales internacionales.

De igual modo, el tratado internacional de ciberseguridad y delincuencia dispone la confidencialidad y al mismo tiempo restringir la utilización de datos repartidos entre Estados (Convenio de Budapest, 2001, Art. 28). En este sentido la normativa plantea que la divulgación de información debe condicionarse a su uso exclusivo para el proceso que pueda solicitarse, asegurando así su carácter hermético.

En este contexto, la previsión toma gran importancia al implementarse en situaciones de phishing transfronterizo, donde la confianza jurídicos entre los países dependerá de la seguridad donde los datos o información no sean aplicada de manera inadecuada. La carencia de estas garantías puede deteriorar la cooperación internacional y poner en peligro la validez de las evidencias como la credibilidad de los procedimientos normativos.

Por otra parte, de forma puntual en contexto de cooperación, el Convenio de Budapest (2001), otorga a los países la posibilidad de solicitar a otra la conservación inmediata de información de datos almacenados y obtenido dentro de un territorio (Art. 29). Esto demuestra que la parte requerida tiene la responsabilidad de resguardar la información mediante un tiempo inicial, con el objetivo de impedir su pérdida mientras se establece los procedimientos de asistencia mutua entre el organismo internacional y el país que lleva el caso de ciberdelincuente.

No obstante, al movilizar el contexto del artículo de phishing transfronterizo aparecen diversas dudas acerca de su eficacia real. El mecanismo dependerá que los Estados pueda actuar de manera inmediata y cuente con las herramientas técnicas necesaria, lo cual en ciertas ocasiones no suele ocurrir. Cuando existen limitaciones

burocráticas o la carencia de entidades políticas, la conservación de información de datos podría volverse inoperante y comprometer las evidencias claves.

En última instancia, el Convenio de Budapest (2001), como instrumento internacional dispone que cuando los Estados puedan detectar proveedores internacionales en la transmisión de una comunicación, los organismos deberán demostrar rápidamente los datos claves para interceptarlo (Art. 30).

Dentro de la práctica, el desafío principal ante los casos de phishing transfronterizo no es solamente la inmediatez en la proporcionalidad de la información, sino también en la carencia de garantías acerca de la completitud, debido a que los proveedores en diversas jurisdicciones trasladan datos en partes. Por tal motivo, es complicado reconstruir de forma íntegra el camino del ataque ante este tipo de problema, por lo cual se debilitaría la solidez de las evidencias digitales.

Análisis comparativo de procedimientos de recolección

Para elaborar el análisis comparativo de los procesos de recolección se tomaron en consideración las fases de conservación, acceso y cooperación prevista en el Código Orgánico Integral Penal y el Convenio de Budapest, lo que permitió visualizar como cada cuerpo jurídico estructura el manejo de la información digital.

Tabla 1.

Conservación.

Procedimiento	Marco legal Ecuador	Marco legal Budapest	Análisis técnico–jurídico
Conservación de datos	Art. 444 COIP: El fiscal puede solicitar al juez la orden para la preservación de evidencia digital en dispositivos incautados, garantizando la cadena de custodia.	Art. 16: Conservación inmediata de datos electrónicos hasta 90 días.	El COIP exige incautación física y autorización judicial, lo que retrasa la preservación de datos. El Convenio de Budapest permite conservación remota, inmediata y transfronteriza,
	Art. 230 COIP: Penaliza la interceptación ilegal de datos.	Art. 17: Revelación rápida de datos de tráfico.	

	Art. 234 COIP: Sanciona el acceso no consentido a sistemas informáticos.	Art. 29: Solicitudes de conservación entre Estados parte.	reduciendo el riesgo de pérdida de evidencia.

Fuente: Código Orgánico Integral Penal (2014); Convenio de Budapest (2001).
Nota. Diferencias técnicas en métodos de conservación digital comparados.
Elaborado por: Dayanara Quezada.

La conservación de datos en el ámbito de Ecuador demuestra un esquema limitado ante los dinamismos vigentes de la ciberdelincuencia, ya que se prioriza un enfoque que busca responder rápidamente lo que requiere el ámbito digital actualmente. Es importante mencionar que esta rigidez ocasiona vacíos en el cuidado y protección de las pruebas, en especial cuando son datos almacenados en el exterior.

Tabla 2.

Acceso.

Procedimiento	Marco legal Ecuador	Marco legal Budapest	Análisis técnico–jurídico
Acceso a sistemas	Art. 234 COIP tipifica como delito el acceso no consentido a un sistema informático o telemático, sancionando la intrusión con pena privativa de libertad.	Art. 21 Convenio de Budapest faculta a las autoridades a obtener datos en tiempo real y obliga a los proveedores a colaborar en la interceptación o acceso autorizado.	El COIP penaliza la intrusión, pero no otorga procedimientos ágiles de acceso controlado para la investigación. El Convenio de Budapest, en cambio, establece mecanismos inmediatos y cooperación obligatoria de
	Art. 234.1 sanciona la falsificación informática mediante la manipulación o creación de datos digitales no genuinos.		

			proveedores, lo que facilita la obtención oportuna de evidencia.

Fuente: Código Orgánico Integral Penal (2014); Convenio de Budapest (2001).
Nota. Diferencias técnicas en métodos de conservación digital comparados.
Elaborado por: Dayanara Quezada.

El acceso a sistemas digitales establece un dilema entre la protección de derechos claves y la eficiencia en la persecución penal ecuatoriana. De tal manera que las normativas nacionales suelen basarse en sancionar la intrusión, al mismo tiempo demuestran debilidades al no estructurar rutas rápidas que ayuden a las autoridades actuar eficazmente.

Tabla 3.

Cooperación.

Procedimiento	Marco legal ecuatoriano	Marco legal Budapest	Análisis técnico-jurídico
cooperación internacional	Art. 448 COIP establece que la Fiscalía dirige el sistema de investigación con apoyo de la Policía, pero la cooperación con otros Estados depende de tratados bilaterales y suele ser lenta.	Art. 25 Convenio de Budapest obliga a las Partes a prestarse asistencia mutua en investigaciones de delitos informáticos. Art. 28 y 29 permiten confidencialidad y conservación rápida de datos entre Estados.	El COIP carece de mecanismos ágiles y depende de trámites diplomáticos tradicionales, lo que retrasa la obtención de pruebas. El Convenio de Budapest prevé cooperación inmediata y estandarizada, facilitando la respuesta a delitos transfronterizos.

Fuente: Código Orgánico Integral Penal (2014); Convenio de Budapest (2001).
Nota. Diferencias técnicas en métodos de conservación digital comparados.

Elaborado por: Dayanara Quezada.

La cooperación internacional en materia tecnológica sigue siendo una de las carencias principales dentro del sistema penal ecuatoriano, ya que los procedimientos se enfocan en realizar trámites diplomáticos que disminuyen la calidad de la investigación. Esta lentitud se diferencia con la dinámica acelerada de los delitos digitales, donde las pruebas pueden desaparecer inmediatamente.

Casos representativos de phishing transfronterizo

Durante el mes de agosto de 2023, ESET (Seguridad Esencial Contra Amenazas en Evolución) Latinoamérica advirtió acerca de una amplia campaña de suplantación de identidad que impactaba a usuarios ecuatorianos de la plataforma de correo Zimbra Collaboration (Primicias, 2023). El ataque mediante la entrega de correos electrónicos que contenían archivos HTML (Lenguaje de Marcado de Hipertexto) a modo de archivo adjunto que llevaban a páginas web fraudulentas, con el fin de obtener credenciales y nombres de usuario.

Como consecuencia de la situación anterior, la Fiscalía General del Estado emprendió una investigación previa a fin de determinar posibles responsabilidades penales. Desde el inicio de la actuación, la propia institución encontró problemas a la hora de poder acceder a los datos digitales, ya que estos se encontraban en servidores de terceros situados en otras jurisdicciones, fuera de la normativa procesal de Ecuador.

Con vistas a superar estos límites, la Fiscalía se ocupó debidamente de solicitar asistencia internacional, si bien la respuesta tardó más de lo que hubiera sido deseable y sobrepasó los plazos útiles para la conservación de las evidencias. Mientras tanto, buena parte de los registros electrónicos se sobrescribió o bien se borró, lo que arruinó el sustentado probatorio.

El final fue un archivo de la causa por insuficiencia probatoria, en resumen, no se había sido capaz de preservar de forma oportuna la evidencia digital y, además, no existen mecanismos normativos para la cooperación inmediata como los previstos en el Convenio de Budapest. Ese desenlace quiere poner en evidencia cómo las barreras legales afectan directamente a la efectividad de la investigación en casos de ciberdelincuencia transfronteriza.

En 2025, la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador se pronunció sobre un nuevo y arriesgado tipo de phishing transfronterizo que amenazaba a los empleados de sectores estratégicos a través de la utilización de datos de carácter personal como nombres y cédulas, mediante el envío de mensajes de ciberataques con links o archivos para la instalación de troyanos (Gómez, 2025).

La Fiscalía General del Estado, siendo un organismo del Estado, procedió a la apertura de una investigación previa bajo los preceptos del COIP. Dispuestas las diligencias pertinentes, aparecieron los primeros inconvenientes en la acción, debido a que los primeros dispositivos afectados para la investigación habían sido dañados o limpiados, lo que dificultó la obtención de imágenes forenses para poder sostener la acusación.

Debido a la complejidad del caso, la Fiscalía requirió la colaboración de proveedores de mensajerías y correos corporativos localizados en el exterior de territorio ecuatoriano, lo que motivó procesos de cooperación internacional que duraron vario meses, cuya duración dificultó preservar los registros electrónicos íntegros, por lo cual la prueba fue declarada irrelevante.

En fin, de cuentas, el proceso fue sobreseído por falta de prueba suficiente por las lagunas que le son inherentes al marco jurídico nacional para abordar ataques que

traspasan fronteras, existiendo la necesidad de herramientas internacionales como el Convenio de Budapest.

En el año 2024, el Ministerio de Telecomunicaciones y Servicios Postales del Ecuador (2024) avisó a la población acerca de campañas de phishing que hacían uso de direcciones falsas, haciéndose pasar por el organismo oficial de envíos. La Fiscalía General del Estado efectúo la apertura de la investigación previa una vez presentada la correspondiente denuncia, rigiéndose, en el presente caso, por la figura del fraude electrónico tipificada en el COIP.

El reto procesal estuvo dado por la capacidad de identificar y de conservar registros DNS (Sistema de Nombres de Dominio) y logs (archivos de registro) asociados a los dominios alojados en servidores internacionales, pues limitó la capacidad de las autoridades de procurarse las pruebas de forma inmediata para la determinación de los responsables de la estafa. Lo anterior muestra la dependencia al uso de la cooperación con los registradores externos, que sólo fueron capaces de responder cuando los ataques ya habían tenido lugar, limitándose a las pruebas una vez que la información ya estaba alterada o dada de baja.

Durante la tramitación la fiscalía requirió medidas técnicas consistentes en auditoría informática entre ellas certificación de URLS (Localizador Uniforme de Recursos) fraudulentas, capturas del tráfico de red, preservaciones de certificados SSL (Capa de Conexión Segura). En el desarrollo del proceso judicial la carencia de protocolos estandarizados para la autenticación de la evidencia digital en tiempo real en consecuencia de que gran parte de ésta no haya podido ser presentada en juicio.

En segunda se expone la falta de progreso y el archivo del asunto por infracción de pruebas y por la informalidad de dicha prueba por tenerla la existencia de falta de integridad y cadena de custodia. Esta situación ponía de manifiesto la urgencia de contar

con un marco normativo más ágil para permitir recoger y dar validez a las pruebas en el Ecuador, tal y como se viene aplicando en el marco de la convención de Budapest, de conformidad con los estándares internacionales.

Resultados

A través de la búsqueda inicial se pudo identificar 92 documentos, de los cuales 30 cumplió con los criterios de inclusión relacionado al tema abordado. La gran cantidad de los estudios identificados se centraron entre el periodo 2020 y 2024, con predominio de investigaciones jurídicas elaboradas en América Latina (61%) y Europa (26%). Entre los documentos más importante se encuentran las normativas como el Convenio de Budapest, el Código Orgánico Integral Penal e información proveniente de revistas indexadas como Redalyc y Scielo.

Por medio del análisis temático se pudo agrupar los hallazgos en cuatro categorías claves como:

1. Delitos informáticos relacionados al phishing transfronterizo (n=8): estudios enfocados en la apropiación indebida de datos e información de manera ilegal, así como la falsificación digital y tecnológica.
2. Mecanismos internacionales en la obtención de evidencia tecnológica (n=7): estudios acerca de las medidas del Convenio de Budapest como la conservación de información e interceptación de datos en tiempo real.
3. Limitaciones y barreras normativas en ámbitos transfronterizos (n=9): Estudios que proporcionan información acerca de a ausencia de lineamientos técnicos, sincronización y cooperación en el contexto ecuatoriano.
4. Enfoque doctrinarias en relación con la ciberdelincuencia (n=6): Información que distinguen el marco jurídico nacional con las normas internacionales, donde se muestran vacíos y desafíos en la aplicación práctica ante casos phishing transfronterizo.

Se detectó vacíos dentro los estudios identificados acerca de protocolos preventivos, preservación y validación de pruebas digitales en relación con el phishing transfronterizo, así como cooperación y coordinación internacional ante este tipo de situaciones. Es importante mencionar que ciertos estudios presentaron un enfoque transversal, lo que significa que pueda vincularse con más de una categoría plateada. Sin embargo, se realizó la categorización de cada documento según a la categoría en la cual se relacionaba. Esto demuestra las coincidencias numéricas en su totalidad de los documentos.

Bajo este contexto, se consiguió como resultado los siguientes hallazgos:

- Mediante el análisis documental se revisaron 30 documentos en su totalidad. La clasificación fue la siguiente:
    - Normativa e información de organismos internacionales: 7 documentos (25%) entre los cuales se encuentra el Código Orgánico Integral Penal, Constitución de la República del Ecuador, Convenio de Budapest y otras entidades internacionales como la UNODC, Iinteropol, FBI y Council of Europe.
    - Doctrina: 23 documentos (75%), los cuales están conformados por artículos de revistas indexadas, ensayos y libros donde abordan el problema de la ciberdelincuente en Ecuador y de manera internación.
- Vacíos normativos identificados: Se observaron 15 aspectos puntuales que carecen en la regulación y sanción relacionada al phishing transfronterizo en el Código Orgánico Integral Penal frente al Convenio de Budapest. Los puntos más relevantes son los siguientes:

    - Carencia de normativa clara acerca de la cooperación y coordinación transfronteriza en tiempo real.
    - Ausencia de un mecanismo para la conservación de datos e información de manera rápida.
    - Deficiencia de estándares para validar los casos en el ámbito ecuatoriano al entorno internacional.
- Convergencias: Se identificó 8 principios comunes entre ambas normativas analizadas entre las cuales se determinó los siguientes puntos:
    - Delito informático como fenómeno global.
    - Tipificación de conductas relacionadas al acceso sin consentimiento.
    - Proteger la confidencialidad y los datos personales de los usuarios.
    - Regular la interceptación de comunicación vía online.
    - Importancia de la cadena de custodia en la evidencia tecnológica.
    - Responsabilidad de los proveedores de servicios de internet.
    - Necesidad de mecanismos de cooperación judicial.
    - Preservación de los derechos clave mediante la investigación.
- Además, mediante el análisis se pudo determinar que COIP abordar temas relacionados con acciones y conductas informáticas en sus siguientes artículos:
    - Artículo 190
    - Artículo 229

    - Artículo 230
    - Artículo 234
    - Artículo 234.1
    - Artículo 444
    - Artículo 448
- En el Convenio de Budapest se identificaron 8 artículos, los cuales se enfocan en la conservación, revelación e interceptación de información y de datos digitales en sus siguientes artículos:
    - Artículo 16
    - Artículo 17
    - Artículo 18
    - Artículo 21
    - Artículo 25
    - Artículo 28
    - Artículo 29
    - Artículo 30
- Se identificaron cinco coincidencias normativas en la regulación acerca de la intercepción de datos personales, comunicación y protección.

Discusión

Los resultados permiten concluir que esta impunidad organizacional con delitos informáticos queda incentivada en el marco de la globalización, es decir, la razonabilidad de los vacíos del COIP en relación con la cooperación internacional determina que sea menos efectiva la respuesta al phishing de orden transfronterizo (Acosta et al., 2020). Una dosis de información adicional le da Benavides et al. (2020), quienes detectaron ciertos patrones en los ataques que demanda respuestas en la esfera informacional homogéneas. En este sentido, Bustillos y Rojas (2023), insisten en que, si no hay una cultura de ciberseguridad desde donde aplicar las normas, estas pierden efectividad, lo cual a su vez conecta con el hallazgo de que el usuario se comporta como el eslabón más débil.

Campos et al. (2024), subrayan que la ingeniería social no ha dejado de ser la técnica fundacional del phishing, lo que sirve para aseverar que las debilidades no son solo jurídicas, sino también sociales. Casey (2011), asegura que la efectividad de la prueba digital debe cumplir con estándares internacionales regulares, el problema está íntimamente vinculado a la falta de protocolos en Ecuador, en función de los cuales se garantizaría la conservación rápida de los datos. Clancy (2023), asegura que los riesgos aumentan en función de la progresiva evolución tecnológica, lo que es suficiente para hacer notar lo que el artículo 229 del COIP resulta demasiado limitante, sin la adecuada delimitación internacional de los casos de ingeniería social.

La normativa ecuatoriana, aunque reconoce derechos procesales fundamentales, presenta vacíos en cuanto a la regulación de procedimientos técnicos orientados a la preservación de la evidencia digital. Mientras el Código Orgánico Integral Penal (2014), aborda ciertas conductas delictivas informáticas, su alcance resulta limitado frente a las necesidades de un entorno tecnológico en constante evolución. En contraste, el

Convenio de Budapest (2001), ofrece directrices más precisas sobre conservación y cooperación internacional, estableciendo estándares que facilitan la investigación de delitos cibernéticos. En este sentido, Ordóñez (2024), argumenta que la falta de armonización entre estas normativas debilita la colaboración judicial y reduce la eficacia de la evidencia en casos transnacionales, lo que pone de manifiesto la urgencia de actualizar el marco legal ecuatoriano para responder de manera efectiva a los desafíos digitales.

El Council of Europe (2024), señala que la cooperación internacional, la cual versa sobre el conjunto de relaciones que se dan entre los Estados en las controversias de orden internacional, es el pilar básico de toda estrategia contra la ciberdelincugencia, esto se encuentra en consonancia con la Oficina Federal de Investigación (FBI, 2025), que por su parte menciona que, si no se produce una preservación inmediata, la evidencia digital se perderá. Flores et al. (2024), argumentan que para el caso ecuatoriano, el marco normativo no se encuentra alineado a marcos de alcance global, por lo que se acerca a la complejidad del phishing. Mendoza (2024), se suma al acotar que en el marco de Latinoamérica, incluido el marco ecuatoriano, los marcos normativos están desfasados con respecto a la evolución criminal, lo que garantizan vacíos frente a los delitos tecnológicos.

Freire et al. (2024), reafirman que es indispensable implementar una continua actualización del marco normativo legal con el fin de responder a la innovación criminal. Fuentes (2025), incluso reconoce que el COIP contempla avances en la tipificación, pero no en cuanto a los protocolos de cooperación. Hernández y Baluja (2021), concluyen que las redes sociales se han determinado como un canal por excelencia para el phishing (cosa que indica la insuficiencia de sancionar únicamente la conducta de interceptar comunicaciones), mientras que Maldonado & Peña (2023),

también se hacen eco de este argumento al conseguir que el impacto económico y social de los delitos informáticos consigan un marco normativo más robusto.

Morales (2025), sostiene que la brecha tecnológica entre naciones establece las condiciones a partir de las cuales pueden ser eficaces las disposiciones jurídicas; en la misma línea Maldonado (2025), evidencia el aumento de ciberataques en Ecuador y la falta de reformas legales que permitirían combatirlos. Sin embargo, Ortiz (2020), agrega que la inflexibilidad del derecho penal ecuatoriano le impide adaptarse a los avances de las nuevas modalidades delictivas.

En conjunto, los resultados evidencian un consenso entre los autores respecto a las deficiencias normativas y la necesidad de cooperación internacional frente a los delitos informáticos. Ponce (2024), advierte que la legislación ecuatoriana no responde con la rapidez necesaria ante la evolución de los ataques digitales, lo que genera vulnerabilidad jurídica. En concordancia, Raza (2021), enfatiza que la tutela de los datos personales debe convertirse en un eje esencial de la cooperación judicial, pues su adecuada protección fomenta la confianza transfronteriza. Esta idea se complementa con Rosas y Pila (2022), quienes sostienen que la falta de garantías efectivas en materia de privacidad debilita dicha confianza entre los Estados, obstaculizando los esfuerzos colaborativos. En suma, la interacción de estas perspectivas revela que la efectividad de la cooperación internacional depende de la actualización legislativa y de la consolidación de mecanismos sólidos de protección de datos personales

La Naciones Unidas contra la Droga y el Delito (UNODD, 2022), buscar la homologación de las leyes nacionales con los instrumentos de naturaleza global, y así refrendar el papel del Convenio de Budapest (2001), adoptado por el Consejo de Europa. La Organización Internacional de Policía Criminal (Interpol, 2024), indica que el *phishing* se extiende y que la falta de coordinación entre los países favorece la

impunidad en algún punto de los tipos penales. La Organización de los Estados Americanos (OEA, 2020), añade que en América Latina, una de las muchas preocupaciones es que hay una fragmentación normativa, lo que ha impedido realizar políticas conjuntas para el control y la respuesta de incidentes delictivos en línea o delitos cibernéticos en general.

El Ministerio del Interior (2024), proporciona estadísticas que evidencian un aumento de los casos de phishing en Ecuador, dado que no es una problemática únicamente internacional, sino también nacional. Estas estadísticas corroboran que los vacíos del COIP son mucho más que una cuestión teórica, son vacíos que comportan consecuencias en la protección de las víctimas.

Los informes internacionales institucionales avalan estas observaciones. El Council of Europe (2024) y la European Union Agency for Criminal Justice Cooperation (2021), postulaban que la cooperación judicial es preciso que sea libre de interferencias burocráticas. Combinada con la Oficina Federal de Investigación (FBI, 2025) y las Naciones Unidas contra la Droga y el Delito (UNODD, 2022), se puede afirmar que sin coordinación interestatal y sin estándares técnicos comunes, la normativa nacional pierde su sentido frente a la globalidad del phishing.

Conclusiones

A través del análisis realizado se pudo identificar 15 vacíos normativos encontrados en el Código Orgánico Integral Penal, los cuales son una barrera para la persecución eficaz del phishing transfronterizo. Entre los vacíos más importantes se encuentra la carencia de mecanismo de conservación de personales de manera rápida, la carencia de protocolos adecuados para interceptar ataques en tiempo real y la inexistencia de rutas de cooperación y coordinación inmediata entre las jurisdicciones.

En contraste con el Convenio de Budapest refleja que mientras este organismo internacional proporciona procesos lógicos y estructurados, la normativa de Ecuador aún mantiene un enfoque inadecuado para llevar casos de delitos informáticos a nivel internacional. Como resultado, en casos transfronterizo las pruebas digitales suelen perderse o no tiene validez procesal en el contexto ecuatoriano, lo cual debilita la capacidad para sancionar casos de phishing transfronterizo en el país.

Para superar estas barreras, es necesario la modificación de disposiciones del Código Orgánico Integral Penal, especialmente en su artículo 444, con el objetivo de aplicar reglas puntuales acerca de la preservación de pruebas digitales. Asimismo, es fundamental elaborar una unidad que se especialice en caso de ciberdelitos con enfoque técnico y jurídico, el cual debería ser respaldado por un presupuesto adecuado.

Es importante mencionar que estos hallazgos son sustentados mediante la revisión documental y en análisis de casos en el contexto ecuatoriano, donde el Ecuador perdió evidencia fundamental debido a la deficiencia jurídica en relacionado con el tema abordado. Finalmente, es necesario que se implemente los estándares de organismos internacionales como el del Convenio de Budapest para asegurar procedimientos judiciales efectivos y una protección adecuada a los datos de los ciudadanos en el ámbito digital.

Referencias

Acosta, M., Benavides, M., y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 1-15. https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Benavides, E., Fuertes, W., y Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencias Informáticas, 13*(1), 97-104 . https://doi.org/https://doi.org/10.18779/cyt.v13i1.357

Bustillos, O., y Rojas, J. (2023). Cómo promueven los estados la ciberseguridad de las pymes. *Interfases, 5*(17), 21-37. https://www.redalyc.org/journal/7301/730178910002/730178910002.pdf

Campos, M., Moreno, R., y Jiménez, B. (2024). Detección de fraudes y estafas basadas en ingeniería social en Ecuador. *Revista InveCom, 5*(3), 1–8. https://doi.org/https://doi.org/10.5281/zenodo.14263156

Casey, E. (2011). *Digital Evidence and Computer Crime.* Academic Press. https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

Clancy, T. (2023). *Cyber crime and digital evidence.* https://cap-press.com/pdf/9781531024970.pdf?srsltid=AfmBOor6XCOsgio7Vd3_cF-HxoiX0zqXcvoJF4WTdhNA8niAKmyemplb

Código Orgánico Integral Penal. (2014). *Registro Oficial Suplemento 180.* https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Constitución de la República del Ecuador. (2008). *Registro Oficial 449*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Convenio de Budapest. (2001). *Convention on Cybercrime ETS No. 185*. https://rm.coe.int/1680081561

Council of Europe. (2024). *New report on search and seizure of stored computer data in 74 countries: a critical step in combatting cybercrime and obtaining electronic evidence*. https://www.coe.int/en/web/portal/-/new-report-on-search-and-seizure-of-stored-computer-data-in-74-countries-a-critical-step-in-combatting-cybercrime-and-obtaining-electronic-evidence

European Union Agency for Criminal Justice Cooperation. (24 de Noviembre de 2021). *Cross-border access to electronic evidence: update and impact of the pandemic on data requests*. https://www.eurojust.europa.eu/news/cross-border-access-electronic-evidence-update-and-impact-pandemic-data-requests?

FBI. (24 de Abril de 2025). *La Oficina del FBI en Denver Advierte Sobre Estafas al Usar Los Conversores de Archivos en Línea*. https://www.fbi.gov/contact-us/field-offices/denver/news/la-oficina-del-fbi-en-denver-advierte-sobre-estafas-al-usar-los-conversores-de-archivos-en-lnea

Flores, L., Carrión, K., y Rivera, J. (2024). Fundamentos jurídicos para la inclusión del delito de phishing en el código penal ecuatoriano. *Revista Dilemas Contemporáneos: Educación, Política y Valores, 4*(113), 1-26. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4515

Freire, J., Villalobos, M., Morales, J., Nieves, L., y Ferruzola, E. (2024). La responsabilidad penal derivada de los delitos de apropiación ilícita a través de medios. *Sinergia Académica, 7*(7), 513-530. https://sinergiaacademica.com/index.php/sa/article/view/390

Fuentes, E. (2025). Criminalidad en el ciberespacio: tipificación de delitos informáticos y desafíos. *Polo del Conocimiento, 10*(6), 2342-2350. https://polodelconocimiento.com/ojs/index.php/es/article/view/9817/html

Gómez, A. (14 de Enero de 2025). *Spear Phishing, una nueva modalidad de ciberdelito que amenaza a Ecuador*. https://www.ecuavisa.com/noticias/seguridad/ciberdelito-spear-phishing-ecuador-KC8620590

Hernández, A., y Baluja, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. *Revista Cubana de Ciencias Informáticas, 15*(2), 413-441. https://www.redalyc.org/journal/3783/378370462024/378370462024.pdf

Interpol. (4 de Agosto de 2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Interpol. (11 de Marzo de 2024). *Evaluación mundial de interpol sobre la amenaza que plantean las estafas*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Evaluacion-de-INTERPOL-sobre-estafas-un-peligro-mundial-incrementado-por-la-tecnologia

Maldonado, F., y Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Revista Portal de la Ciencia, 4*(3), 325-337. https://institutojubones.edu.ec/ojs/index.php/portal/article/view/394

Maldonado, L. (2025). Elementos criminógenos de las tecnologías de la información y proliferación de la delincuencia informática. *Investigación, Tecnología e Innovación, 17*(23), 41-51. https://revistas.ug.edu.ec/index.php/iti/es/article/view/1945

Mendoza, M. (2024). Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal. *Código Científico Revista De Investigación, 5*(E3), 480–498. https://doi.org/https://doi.org/10.55813/gaea/ccri/v5/nE3/328

Ministerio del Interior. (2024). *Análisis de la ciberdelincuencia* . https://www.ministeriodelinterior.gob.ec/wp-content/uploads/downloads/2025/07/Boletin-La-nueva-era-de-la-ciberdelincuencia-el-lado-oscuro-de-la-Inteligencia-Artificial.pdf

Morales, O. (2025). Ciberfraude: Principales Métodos de Ataque y Estrategias para su Prevención. *Ciencia Latina Revista Científica Multidisciplinar, 9*(3), 4901-4921. https://doi.org/https://doi.org/10.37811/cl_rcm.v9i3.18122

OEA. (2 de Julio de 2020). *Ciberseguridad riesgos, avances y el camino a seguir en América Latina Y El Caribe.* https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Ordóñez, L. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. *Reincisol, 3*(5), 1447–1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158

Ortiz, N. (2020). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos, 4*(1), 100–111. https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio, 1*(58), 119–123. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667

Primicias. (25 de Agosto de 2023). *Ecuador es atacado por una campaña masiva de phishing*. https://www.primicias.ec/noticias/tecnologia/ecuador-ataque-phishing-usuarios/

Razza, C. (2021). *La transferencia internacional de datos personales en Ecuador.* Editorial UDLA. https://www.udlaediciones.com.ec/wp-content/uploads/2023/01/Transferencia-internacional-de-datos-personales-en-Ecuador.pdf

Rosas, G., y Pila, G. (2022). La protección de datos personales en Ecuador Una revisión histórica-normativa de este derecho fundamental en el país suramericano. *Revista Internacional de Cultura Visual, 13*(2), 2-16. https://dialnet.unirioja.es/servlet/articulo?codigo=8942345

Servicios Postales del Ecuador. (2 de julio de 2024). https://www.serviciopostal.gob.ec/sin-categoria/informacion-a-la-ciudania-casos-de-suplantacion-de-informacion-phishing/?utm_source=.com

UNODD. (2022). *Compendio de ciberdelincuencia organizada.* Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

https://www.unodc.org/documents/Cybercrime/tools-and-resources/compendio_de_delincuencia_organizada_es.pdf