UNIVERSIDAD LAICA ELOY ALFARO DE MANABI

FACULTAD DE CIENCIAS SOCIALES, DERECHO Y BIENESTAR

CARRERA DE DERECHO

TRABAJO DE TITULACION PREVIO A LA OBTENCION DEL TITULO DE ABOGADA DE LOS JUZGADOS Y TRIBUNALES DE LA REPUBLICA DEL ECUADOR

TITULO:

CIBERDELITOS EN ECUADOR: ANÁLISIS JURÍDICO-PENAL DE LOS DESAFÍOS DIGITALES EN LA ERA TECNOLÓGICA

AUTORA:

ANA PATRICIA MARTINEZ BORRERO

TUTOR:

DR. WILTER RONAL ZAMBRANO SOLORZANO PhD

MANTA – ECUADOR

2026

DECLARACIÓN DE AUTORÍA

El trabajo de grado denominado "CIBERDELITOS EN ECUADOR: ANÁLISIS JURÍDICO-PENAL DE LOS DESAFÍOS DIGITALES EN LA ERA TECNOLÓGICA" ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan en las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

En virtud de esta declaración me responsabilizo del contenido, veracidad y alcance científico de proyecto de grado en mención

Ana Patricia Martínez Borrero

Autora

CERTIFICACIÓN

En calidad de docente tutora de la Facultad de Derecho de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de Integración Curricular modalidad Trabajo de Investigación bajo la autoría de la estudiante **Ana Patricia Martínez Borrero**, legalmente matriculada en la carrera de Derecho, período académico 2025-2 cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**Ciberdelitos En Ecuador: Análisis Jurídico-Penal De Los Desafíos Digitales En La Era Tecnológica**".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 13 de abril de 2026.

Lo certifico,

Dr. Wilter Ronal Zambrano Solórzano, PhD.
Docente Tutora

Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

PROYECTO INVESTIGACION ANA MARTINEZ CORREGIDO POR FIN

ID : 3b8419e3f27cfd36d24e21fee1516a63a10d4905

8%
Textos sospechosos

Nombre del fichero : PROYECTO INVESTIGACION ANA MARTINEZ CORREGIDO POR FIN.txt
Tamaño del archivo original : 91,06 kB
Número de palabras : 14.805
Número de caracteres : 107006

Depositante : WILTER ZAMBRANO SOLORZANO
Fecha de depósito : 8 de abril de 2026
Tipo de carga : interface
fecha de fin de análisis : 8 de abril de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes **3%**

Sintáctica 3% | Semántica *No medido*

Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

Detección de IA **2%**

Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos **3%**

Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas 2%

Pasajes entre comillas, a menudo indicativos de una cita.

DEDICATORIA

A Dios por haber permitido que llegara a este punto de mi vida y haberme dado salud para cumplir con este objetivo que lo tenía claro desde pequeña.

A mi padre, Jorge Martinez, por ayudarme y apoyarme a seguir mis sueños, además de brindarme apoyo emocional cuando sentía que ya no podía mas porque cada vez que quería rendirme, inconscientemente me sacaba una sonrisa con sus mensajes ocurrentes y sus videos.

A mi madre, Lourdes Borrero, por ser el mayor pilar de mi vida, ya que siempre estaba para mi cuando mas lo necesitaba, a pesar de las adversidades.

A mis hermanos, en especial a Bryant Reyna, porque a pesar de no llevar el mismo apellido ha sabido ser mas hermano que algunas personas que conozco. Gracias por apoyarme en todo y por ayudarme a seguir cumpliendo con cada uno de mis sueños.

A mis sobrinos, María José y Jiam, por llenarme de alegría el corazón en mis días tristes.

A mi abuelo, Oswaldo Martinez, porque, aunque no se encuentre es este plano terrenal, él siempre me motivo a seguir estudiando y se el orgullo que le daría saber que seguí la profesión que el tanto deseaba para mí.

A mi abuela, Emperatriz Cadena, por apoyarme en todos los sentidos y siempre estar brindándome consejos sabios que me ayudaron a tomar decisiones correctas a lo largo de mi vida universitaria.

A mis verdaderas amigas, por siempre estar para mi incondicionalmente a pesar de las situaciones, por acogerme en sus hogares y recibirme siempre con las manos abiertas. Sin ustedes poder conllevar estos casi cinco años lejos de mi familia hubiera sido un caos.

Y para los que ya no están dentro de mi vida, ya que entendí que a pesar de las adversidades el sol siempre saldrá para mí.

CONTENIDO

RESUMEN

La presente investigación examina el marco jurídico-penal ecuatoriano frente a los ciberdelitos durante 2020-2025, identificando desafíos para la tipificación, persecución y sanción de estas conductas ilícitas mediante un diseño descriptivo-analítico con enfoque mixto.

Ecuador experimentó un incremento del 340% en delitos informáticos entre 2020-2023. La Fiscalía General registró 20.602 denuncias entre enero 2022 y mayo 2025, siendo la apropiación fraudulenta por medios electrónicos la modalidad predominante (11.833 casos), seguida de estafa (4.567 casos) y acceso no consentido a sistemas informáticos (2.183 casos). La concentración territorial se evidencia en Pichincha (8.089 casos), Guayas (4.644 casos) y Manabí (1.174 casos).

El análisis del Código Orgánico Integral Penal revela avances mediante los artículos 229-234.4 que tipifican delitos contra sistemas de información y comunicación, complementados con la reforma del 2023 que incorporó falsificación informática y agravantes. Sin embargo, persisten limitaciones críticas: ausencia de tipos penales para ransomware, deepfakes y delitos con criptomonedas; deficiencias en cooperación internacional; personal técnico insuficiente y recursos tecnológicos limitados.

Los grupos más vulnerables incluyen menores de edad y población con analfabetismo digital (8,2%). La ratificación del Convenio de Budapest (julio 2024) ofrece oportunidades para fortalecer capacidades nacionales.

El estudio propone mejoras integrales: actualización normativa, fortalecimiento institucional con laboratorios forenses especializados, desarrollo de recursos humanos capacitados, operativización de cooperación internacional y estrategias preventivas de educación digital. La investigación concluye que la brecha entre realidad criminológica y herramientas jurídicas demanda transformaciones sistémicas para construir un ecosistema de seguridad digital resiliente.

Palabras claves:

Ciberdelitos, Derecho Penal Informático, Código Orgánico Integral Penal, Seguridad Digital, Criminalidad Informática, Cooperación Internacional, Convenio de Budapest, Evidencia Digital.

ABSTRACT

This research examines the Ecuadorian criminal law framework regarding cybercrimes during the period 2020-2025, identifying challenges in the classification, prosecution, and punishment of these illicit behaviors through a descriptive-analytical design with a mixed approach.

Ecuador experienced a 340% increase in cybercrimes between 2020-2023. The Attorney General's Office registered 20,602 complaints between January 2022 and May 2025, with fraudulent appropriation by electronic means being the predominant modality (11,833 cases), followed by fraud (4,567 cases) and unauthorized access to computer systems (2,183 cases). The territorial concentration is evident in Pichincha (8,089 cases), Guayas (4,644 cases), and Manabi (1,174 cases).

The analysis of the Comprehensive Organic Criminal Code reveals progress through articles 229-234.4, which define crimes against information and communication systems, complemented by the 2023 reform that incorporated computer forgery and aggravating circumstances. However, critical limitations persist: a lack of criminal offenses for ransomware, deepfakes, and cryptocurrency crimes; deficiencies in international cooperation; insufficient technical personnel; and limited technological resources.

The most vulnerable groups include minors and the digitally illiterate population (8.2%). The ratification of the Budapest Convention (July 2024) offers opportunities to strengthen national capacities.

The study proposes comprehensive improvements: regulatory updates, institutional strengthening with specialized forensic laboratories, development of trained human resources, operationalization of international cooperation, and preventive digital education strategies. The research concludes that the gap between criminological reality and legal tools demands systemic transformations to build a resilient digital security ecosystem.

Keywords:

Cybercrime, Computer Criminal Law, Comprehensive Organic Criminal Code, Digital Security, Computer Crime, International Cooperation, Budapest Convention, Digital Evidence.

INTRODUCCIÓN

La acelerada expansión de las tecnologías de la información ha transformado de manera profunda la forma en que se desarrollan las relaciones sociales, económicas y jurídicas en el Ecuador. La digitalización, si bien ha generado importantes avances en términos de eficiencia y acceso a servicios, también ha abierto espacios propicios para nuevas formas de criminalidad que desafían los esquemas tradicionales del Derecho Penal. En este contexto, los ciberdelitos se configuran como una problemática compleja que exige respuestas jurídicas especializadas, tanto por su naturaleza técnica como por su carácter transnacional.

El ordenamiento jurídico ecuatoriano ha intentado responder a estas nuevas realidades mediante la incorporación progresiva de tipos penales relacionados con el uso indebido de sistemas informáticos. La entrada en vigencia del Código Orgánico Integral Penal en 2014 constituyó un avance relevante al reconocer expresamente los delitos contra la seguridad de los sistemas de información y comunicación. Sin embargo, el desarrollo tecnológico avanza a un ritmo significativamente más rápido que el legislativo, lo que genera una brecha entre las conductas que se producen en el ciberespacio y las herramientas jurídicas disponibles para su control y sanción.

Las reformas posteriores al COIP, particularmente aquellas relacionadas con la falsificación informática, la agravación de penas y la responsabilidad de personas jurídicas, evidencian un esfuerzo del legislador por actualizar el marco normativo. No obstante, persisten importantes vacíos frente a fenómenos emergentes como el ransomware, los deepfakes, el uso de criptomonedas con fines delictivos y la criminalidad apoyada en inteligencia artificial. Esta situación plantea serias dudas sobre la suficiencia del sistema penal vigente para garantizar una tutela efectiva de los bienes jurídicos afectados en el entorno digital.

Desde esta perspectiva, la presente investigación analiza críticamente la adecuación del marco jurídico-penal ecuatoriano frente a los ciberdelitos, tomando en cuenta tanto su regulación normativa como los desafíos prácticos en materia de investigación, prueba y cooperación internacional. El estudio se centra en las manifestaciones más recurrentes de la criminalidad cibernética en el país, tales como las estafas electrónicas, la suplantación de identidad digital, el acceso no autorizado a sistemas informáticos y los delitos cometidos contra menores a través de medios telemáticos.

Este trabajo parte de la premisa de que el Derecho Penal, como mecanismo de última ratio, debe adaptarse a las transformaciones tecnológicas sin sacrificar sus principios fundamentales, especialmente la legalidad, la proporcionalidad y la mínima intervención. En consecuencia, la investigación no solo busca

describir el estado actual de la regulación de los ciberdelitos en Ecuador, sino también formular propuestas que contribuyan al fortalecimiento del sistema jurídico, en armonía con los estándares internacionales y el modelo constitucional de derechos y justicia.

CAPITULO I

EL PROBLEMA DE INVESTIGACION

Planteamiento del Problema de investigación

La creciente digitalización de las actividades humanas ha modificado sustancialmente la forma en que se cometen los delitos, desplazando muchas conductas ilícitas desde espacios físicos tradicionales hacia entornos virtuales. En el caso ecuatoriano, esta transformación ha generado importantes desafíos para el sistema jurídico-penal, el cual fue concebido originalmente para enfrentar formas de criminalidad con límites territoriales claros y dinámicas probatorias convencionales.

El Estado ecuatoriano enfrenta actualmente dificultades estructurales en la tipificación, investigación y sanción de los ciberdelitos. Si bien el Código Orgánico Integral Penal incorpora figuras específicas relacionadas con la criminalidad informática, estas no siempre resultan suficientes para abarcar la diversidad y complejidad de las conductas que se desarrollan en el ciberespacio. La ausencia de tipos penales que contemplen modalidades delictivas emergentes, así como la ambigüedad de ciertos elementos normativos, generan espacios de incertidumbre jurídica que pueden derivar tanto en impunidad como en interpretaciones extensivas incompatibles con el principio de legalidad.

A ello se suman las dificultades propias de la investigación penal en entornos digitales. La obtención y valoración de la prueba digital plantea retos técnicos y procesales significativos, relacionados con la volatilidad de la información, la preservación de la cadena de custodia y la limitada capacidad técnica de los órganos encargados de la persecución penal. Estas limitaciones se agravan cuando los delitos se cometen desde otras jurisdicciones, lo que evidencia la necesidad de mecanismos efectivos de cooperación internacional.

El problema adquiere mayor relevancia al considerar que los ciberdelitos no constituyen un fenómeno aislado o marginal, sino una amenaza creciente para derechos fundamentales como la privacidad, la seguridad patrimonial y la protección de datos personales. La aceleración de los procesos de digitalización, intensificada a partir de la emergencia sanitaria, ha incrementado la exposición de ciudadanos, empresas e instituciones públicas a riesgos cibernéticos que el sistema penal no siempre logra enfrentar de manera eficaz.

En este escenario, resulta necesario cuestionar si el marco jurídico-penal ecuatoriano responde adecuadamente a las exigencias de la criminalidad digital contemporánea. El desafío consiste en fortalecer la capacidad del Estado para prevenir y sancionar los ciberdelitos, sin recurrir a una expansión desmedida del poder punitivo que afecte garantías constitucionales. De esta tensión surge la necesidad de un análisis crítico que permita identificar deficiencias normativas y formular propuestas orientadas a una respuesta penal equilibrada y eficaz.

Formulación del Problema

Pregunta Directriz:

¿Es adecuado el sistema jurídico ecuatoriano actual para enfrentar los ciberdelitos, tanto en la definición de estos delitos como en su investigación y sanción?

Preguntas Derivadas:

¿Qué vacíos existen en las leyes ecuatorianas para combatir los nuevos tipos de ciberdelitos?

¿Qué problemas genera el hecho de que los ciberdelitos puedan cometerse desde cualquier parte del mundo?

¿Qué cambios necesita la legislación ecuatoriana para mejorar la lucha contra los ciberdelitos?

Objetivos

GENERAL

Analizar el marco jurídico-penal ecuatoriano frente a los ciberdelitos, identificando los principales desafíos que presenta la era tecnológica para la tipificación, persecución y sanción de estas conductas ilícitas en el Ecuador.

ESPECIFICO

Determinar las principales modalidades de ciberdelitos que afectan a Ecuador, evaluando su incidencia y evolución durante el periodo 2020-2025.

Examinar la efectividad de la legislación penal ecuatoriana vigente para enfrentar los ciberdelitos, identificando vacíos normativos y desafíos procesales en la investigación digital.

Proponer mejoras al marco jurídico-penal ecuatoriano para fortalecer la protección contra los ciberdelitos, considerando estándares internacionales y las particularidades del contexto tecnológico nacional.

Justificación de la investigación

El desarrollo acelerado de las tecnologías digitales ha generado profundas transformaciones en la sociedad ecuatoriana, impactando de manera directa en las dinámicas económicas, sociales y jurídicas. Si bien este proceso ha permitido avances significativos en materia de comunicación, acceso a servicios y modernización institucional, también ha dado lugar a nuevas formas de criminalidad que se desarrollan en el ciberespacio y que desafían los esquemas tradicionales del Derecho Penal.

En este contexto, los ciberdelitos se han convertido en una de las manifestaciones delictivas más complejas y de mayor crecimiento en el Ecuador. La frecuencia con la que se cometen estafas electrónicas, accesos no autorizados a sistemas informáticos, suplantaciones de identidad y delitos contra la privacidad evidencia que la criminalidad digital ya no constituye un fenómeno excepcional, sino una problemática estructural que afecta a amplios sectores de la población. Esta realidad justifica la necesidad de un análisis jurídico-penal profundo que permita evaluar si el marco normativo vigente responde adecuadamente a las exigencias de la era tecnológica.

Desde una perspectiva dogmático-jurídica, la investigación se justifica en la necesidad de examinar la suficiencia y coherencia del Código Orgánico Integral Penal frente a conductas ilícitas cometidas mediante el uso de tecnologías de la información y comunicación. Si bien el COIP ha incorporado tipos penales específicos relacionados con la criminalidad informática, persisten vacíos normativos y ambigüedades que dificultan su aplicación práctica y generan inseguridad jurídica, tanto para los operadores de justicia como para los ciudadanos.

En el ámbito procesal, la investigación cobra relevancia debido a los desafíos que plantea la obtención, preservación y valoración de la prueba digital. La limitada capacitación técnica, la falta de infraestructura especializada y las dificultades para mantener la cadena de custodia de la evidencia digital afectan de manera directa la eficacia de la investigación penal, lo que puede derivar en altos niveles de impunidad en este tipo de delitos.

Desde una dimensión criminológica y social, el estudio resulta pertinente al permitir identificar las modalidades de ciberdelitos más recurrentes en el Ecuador. Este análisis aporta insumos valiosos para el diseño de políticas públicas orientadas no solo a la sanción, sino también a la prevención de la criminalidad digital.

Finalmente, la investigación se justifica por su aporte práctico y académico. Sus resultados pueden servir como base para futuras reformas normativas, el fortalecimiento institucional y la adopción de buenas prácticas alineadas con estándares internacionales, como los establecidos en el Convenio de Budapest. De

esta manera, el estudio contribuye al desarrollo del Derecho Penal Informático en el Ecuador y al fortalecimiento del Estado constitucional de derechos y justicia frente a los desafíos que plantea el entorno digital.

CAPITULO II

MARCO TEORICO

Antecedentes

La historia de la regulación jurídica de los ciberdelitos en Ecuador ha sido relativamente reciente y marcada por un desarrollo progresivo, el Ecuador inició su incursión en la regulación del entorno digital con la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el año 2002, constituyendo el primer esfuerzo legislativo significativo para regular aspectos tecnológicos (Torres et al., 2018). Sin embargo, esta ley tuvo como finalidad principal dotar de seguridad jurídica al comercio electrónico y a las comunicaciones digitales, mas no establecer una regulación penal específica sobre conductas ilícitas cometidas mediante sistemas informáticos. En este sentido, aunque representó un avance en la adaptación del ordenamiento jurídico al entorno digital, no incorporó una tipificación expresa de los delitos informáticos, lo que evidenció la necesidad de una posterior intervención legislativa en materia penal.

El primer antecedente directo en materia de caracterización de ciberdelitos se encuentra en las reformas al antiguo Código Penal ecuatoriano introducidas mediante la Ley Reformatoria al Código Penal del 2002. Como señala Acurio del Pino (2015), estas modificaciones "incorporaron por primera vez en el ordenamiento jurídico ecuatoriano figuras delictivas relacionadas con el uso indebido de sistemas informáticos, aunque con una técnica legislativa incipiente y definiciones limitadas que pronto evidenciaron su insuficiencia ante el rápido avance tecnológico" (p. 87).

Un momento clave dentro de este proceso de transformación legislativa fue la entrada en vigor del Código Orgánico Integral Penal (COIP) en el año 2014. Por primera vez, este cuerpo normativo incluyó un apartado concreto enfocado en las infracciones que afectan directamente la seguridad de los sistemas informáticos y de comunicación. Esta modificación significó un progreso importante, ya que introdujo figuras delictivas específicas orientadas a regular y sancionar conductas ilícitas cometidas en el ámbito digital.

Paladines (2021) destaca que "la inclusión de estos tipos penales en el COIP representó un avance significativo en la arquitectura jurídico-penal ecuatoriana, al reconocer la especificidad de los entornos

digitales como espacios susceptibles de conductas criminógenas" (p. 124). No obstante, diversos autores han señalado las limitaciones de esta regulación frente a la rápida evolución de la criminalidad informática.

Las investigaciones académicas sobre ciberdelitos en el contexto ecuatoriano han sido relativamente escasas, aunque se observa un interés creciente en los últimos años. Entre los estudios pioneros destaca el trabajo de Páez y Acurio (2010), quienes realizaron un análisis descriptivo de los principales delitos informáticos registrados en Ecuador durante el período 2005-2009, evidenciando ya entonces un incremento sostenido en su incidencia y la insuficiencia de los mecanismos legales entonces vigentes. Posteriormente, Villacís y Zambrano (2019) desarrollaron una investigación de carácter empírico centrada en las denuncias por ciberdelitos presentadas ante la Fiscalía General del Estado entre 2015 y 2018. Los autores determinaron que existía una diferencia considerable entre los incidentes de seguridad informática reportados por el sector privado y aquellos que fueron formalmente denunciados ante el sistema de justicia, lo que evidenciaría un significativo nivel de subregistro en este tipo de infracciones.

Desde el enfoque jurídico-dogmático, Albán Gómez (2020) examinó la estructura de los delitos informáticos contemplados en el COIP y advirtió que la redacción adoptada por el legislador presenta ambigüedades conceptuales. Según su análisis, tales imprecisiones complican la correcta aplicación de estas figuras penales, especialmente en lo que respecta a aquellos elementos normativos que exigen conocimientos técnicos especializados para su adecuada interpretación.

En cuanto al aspecto procesal, Guerrero (2022) desarrolló un estudio enfocado en las dificultades relacionadas con la obtención y valoración de pruebas en caso de delitos digitales en el Ecuador. El autor determino que el Código Orgánico Integral Penal no regula de manera suficiente las características propias de la evidencia digital, situación que afecta tanto a la efectividad de las investigaciones como la admisibilidad y fuerza probatoria de los elementos esenciales para esclarecer estos sucesos.

El análisis de los ciberdelitos en Ecuador debe enmarcarse también en el contexto de los instrumentos internacionales que abordan esta problemática. El principal referente global en esta materia es el Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), adoptado en 2001 y que constituye el instrumento jurídico internacional más importante dentro de lo que abarca la ciberdelincuencia. Actualmente el Ecuador forma parte del Convenio de Budapest, el cual fue ratificado por la Asamblea Nacional el 4 de julio del 2024.

La presente investigación pretende contribuir a llenar estos vacíos, ofreciendo un análisis jurídico-penal integral de los ciberdelitos en Ecuador, fundamentado en evidencia empírica y en una sólida base teórico-conceptual, que permita no solo diagnosticar las deficiencias del sistema actual, sino también

proponer mejoras normativas e institucionales alineadas con los estándares internacionales y los principios constitucionales que rigen el ordenamiento jurídico ecuatoriano.

Fundamentación Teórica

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador, identificada como Ley No. 2002-67, fue promulgada el 10 de abril del año 2002 y publicada en el Registro Oficial Suplemento 557 el 17 de abril del año 2002, esta cronología sitúa a Ecuador como uno de los primeros países pioneros en América Latina en establecer un régimen jurídico integral para las transacciones digitales, anticipándose a las necesidades del mercado digital emergente del nuevo milenio, conectando esta ley en la Convención de Budapest del 23 XI del año 2001 que fue la inspiración de algunos estados del mundo para plasmar este tipo de leyes educándolas a su sistema idiosincrático.

La promulgación de esta ley respondió a la necesidad urgente de proporcionar seguridad jurídica a las transacciones electrónicas que comenzaban a multiplicarse en el panorama comercial ecuatoriano. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador se encarga de la regulación comprehensivamente de los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

La legislación ecuatoriana sobre comercio electrónico inicialmente incluyó disposiciones específicas relacionadas con delitos informáticos en su estructura normativa original. El artículo 61 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67) contenía disposiciones sobre delitos informáticos, estableciendo un marco punitivo para las conductas que atentaran contra la integridad de los sistemas electrónicos y las transacciones digitales, sin embargo, la evolución del marco legal ecuatoriano experimentó una transformación significativa con la promulgación Código Orgánico Integral Penal No. 180 de 10 de febrero del 2014, que entró en vigor el 10 de agosto del 2014, el cual en su Disposición Derogatoria Novena derogó el Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos, esta derogación implicó la transferencia de la regulación de los delitos informáticos desde la ley especializada de comercio electrónico hacia el código penal general, reflejando una evolución conceptual en el tratamiento jurídico de estos ilícitos.

El marco legal ecuatoriano en materia de protección digital ha seguido en constante evolución para adaptarse a las nuevas amenazas y desafíos del entorno cibernético, en el 2021, se promulgó la Ley de Protección de Datos Personales la cual establece un marco legal integral para la protección de los datos

personales, complementando el régimen jurídico establecido por la ley de comercio electrónico y fortaleciendo las garantías de privacidad y protección de la información personal en el ecosistema digital.

Ley de Protección de Datos Personales

La protección de datos personales en Ecuador encuentra su fundamento primario en la Constitución de la República del Ecuador de 2008. Según establece el artículo 66, numeral 19, se reconoce "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección" (Constitución de la República del Ecuador, 2008). Este precepto constitucional establece las bases para el desarrollo de un marco normativo especifico que regule el tratamiento de datos personales en el país, la consagración constitucional de este derecho fundamental responde a la necesidad de proteger la intimidad y privacidad de las personas en un contexto de creciente digitalización de las relaciones sociales y comerciales.

La materialización del mandato constitucional se concretó con la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP), aprobada en mayo del año 2021 y las medidas correctivas y régimen sancionatorio entraron en vigor en mayo del 2023, esta ley tiene como objetivo garantizar el derecho a la protección de datos personales de los ciudadanos ecuatorianos, salvaguardando su privacidad y derecho a la autodeterminación informativa.

La LOPDP define a los datos personales como toda información que directa o indirectamente pueda identificar a una persona natural (excluyendo empresas), estableciendo así el ámbito de protección de la normativa. El 06 de noviembre del 2023, el entonces presidente de la República del Ecuador, Guillermo Lasso Mendoza, expidió el Reglamento de la Ley Orgánica de Protección de Datos Personales (RLOPDP), mediante decreto ejecutivo no. 904, completando así el marco regulatorio necesario para la implementación efectiva de la normativa de protección de datos en el país.

Ley Orgánica de gestión de la identidad y datos civiles

La expansión de las tecnologías digitales ha transformado profundamente la manera en que se concibe la identidad personal y su protección jurídica en el Ecuador, en este contexto, la Ley Orgánica de Gestión de la Identidad y Datos Civiles, promulgada en 2016 y reformada significativamente en 2024, ha adquirido un papel mucho más amplio que el previsto originalmente, pues ya no se limita a organizar el registro y administración de datos civiles, sino que se proyecta como una herramienta clave dentro del sistema de seguridad digital del Estado.

La identidad, que tradicionalmente se vinculaba con documentos físicos y registros presenciales, en la actualidad se desenvuelve también en entornos virtuales donde las interacciones cotidianas se realizan mediante plataformas digitales. Esta nueva realidad exige mecanismos de identificación más sólidos, capaces de garantizar autenticidad y reducir riesgos como la suplantación de identidad o el fraude informático, desde esta perspectiva, la adecuada gestión de los datos civiles no solo cumple una función administrativa, sino que se convierte en un elemento preventivo frente a conductas ilícitas en el ciberespacio.

Además, la coordinación entre la LOGIDAC y el Código Orgánico Integral Penal permite estructurar una respuesta integral frente a los ciberdelitos, mientras el COIP tipifica y sanciona estas conductas, la normativa sobre identidad proporciona las bases técnicas y jurídicas que facilitan la verificación de datos y la trazabilidad necesaria para los procesos investigativos, así el sistema combina una dimensión preventiva mediante controles y mecanismos de autenticación con una dimensión punitiva orientada a sancionar las infracciones.

Sin embargo, el fortalecimiento de los sistemas de identificación digital también genera desafíos importantes en materia de derechos fundamentales. El uso de herramientas que permiten mayor control y seguimiento debe desarrollarse dentro de límites claros que protejan la privacidad y eviten injerencias indebidas, en sí, el reto consiste en armonizar la seguridad con el respeto a la intimidad, asegurando que la información personal sea utilizada exclusivamente para fines legítimos y bajo estrictas garantías legales.

En definitiva, la Ley Orgánica de Gestión de la Identidad y Datos Civiles se posiciona como un componente esencial dentro de la estructura jurídica ecuatoriana para enfrentar los riesgos del entorno digital; su efectividad depende no solo de su contenido normativo, sino también de su correcta implementación tecnológica, de la capacitación institucional de la capacidad de adaptación ante amenazas emergentes, solo mediante este enfoque integral será posible consolidad un entorno digital seguro que al mismo tiempo respeto los derechos y libertades de las personas.

Convención de Budapest

El desarrollo de las tecnologías digitales ha transformado la forma en que interactúan las personas, las empresas y los Estados, sin embargo, este avance también ha facilitado nuevas modalidades delictivas que superan las fronteras territoriales y desafían los sistemas jurídicos tradicionales, en este contexto surge la Convención sobre la Ciberdelincuencia del Consejo de Europa mejor conocida como Convención de Budapest considerada el principal instrumento internacional para enfrentar los delitos informáticos la cual fue adoptada el 23 de noviembre de 2001 y entró en vigor

desde el 1 de julio de 2004, en si, la Convención de Budapest constituye el primer tratado internacional vinculante dedicado exclusivamente al combate del cibercrimen la cual tiene como objetivo central establecer estándares comunes que permitan a los Estados tipificar adecuadamente estas conductas y cooperar eficazmente en su investigación y sanción.

La normativa se organiza en cuatro capítulos claramente diferenciados: el primer capítulo establece definiciones fundamentales y principios generales; el segundo desarrolla las medidas de derecho penal sustantivo; el tercero regula los procedimientos penales aplicables; y el cuarto establece el marco de cooperación internacional (Clough, 2010).

Además, este tratado adopta un enfoque doble que combina la armonización de tipos penales con la modernización de procedimientos investigativos, esta dualidad responde al reconocimiento de que los delitos cibernéticos presentan características específicas que requieren tanto definiciones penales precisas como herramientas procesales adaptadas a la naturaleza digital de la evidencia (Gercke, 2012).

En cuanto a contenido, la Convención de Budapest presenta una clasificación especifica de los delitos informáticos, agrupándolos en cuatro categorías que son las siguientes:

- **Primera categoría:** engloba las infracciones contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, incluyendo el acceso no autorizado, la interceptación ilícita, la alteración de datos y la perturbación de sistemas.
- **Segunda categoría:** comprende los delitos cometidos mediante sistemas informáticos, como la falsificación y fraude digital, adaptándolos al contexto tecnológico.
- **Tercera categoría:** engloba a los delitos relacionados con el contenido centrados específicamente en la pornografía infantil, imponiendo de tal manera a los Estados pertenecientes la obligación de tipificar penalmente la creación, difusión y tenencia de dicho material.
- **Cuarta categoría:** comprende los delitos vinculados a la violación de derechos de propiedad intelectual y derechos conexos que buscan resguardar la protección de los derechos de autor en el ámbito digital.

Un dato relevante es que la Convención establece un sistema integral de cooperación internacional que reconoce la naturaleza transfronteriza de los delitos cibernéticos, los mecanismos de asistencia jurídica mutua incluyen procedimientos expeditos para la preservación y obtención de datos informáticos, reconociendo la volatilidad de la evidencia digital (Keyzer, 2013).

Lo más importante que se debe recalcar de la Convención de Budapest es que impone a los Estados firmantes la responsabilidad de establecer centros de contacto operativo que funcionen de manera

ininterrumpida, durante las 24 horas del día, con el fin de garantizar una colaboración internacional ágil ante situaciones urgentes, esta estructura reconoce la naturaleza transnacional y atemporal del crimen cibernético, que puede producirse en cualquier momento y sin considerar las diferencias horarias entre países, además, se prevén mecanismos de coordinación que permiten a las autoridades nacionales compartir información de forma espontánea cuando detectan conductas delictivas que podrían tener repercusión en otras jurisdicciones firmantes del tratado, no obstante, la cobertura geográfica limitada de la Convención, plantea interrogantes sobre su capacidad para abordar efectivamente delitos que a menudo se originan en jurisdicciones que no forman parte del tratado, esta limitación geográfica puede crear refugios seguros para actividades delictivas en países que no han adoptado estándares similares de criminalización.

En el Ecuador la convención de Budapest fue aprobado y ratificado por la Asamblea Nacional el 04 de julio del 2024, este tratado represento para el estado ecuatoriano una oportunidad de fortalecer su sistema de justicia penal mediante la incorporación de estándares internacionales especializados, a pesar de ello, su implementación exitosa requiere un enfoque integral que considere tanto las particularidades del contexto jurídico nacional como las exigencias de cooperación internacional en la lucha contra el cibercrimen.

La Convención de Budapest representa un hito fundamental en el desarrollo del derecho penal internacional aplicable a los delitos cibernéticos, estableciendo principios y mecanismos que han influenciado la evolución normativa global en esta materia, su enfoque integral que combina armonización sustantiva con modernización procesal, ofrece un modelo valioso para países que buscan fortalecer sus marcos jurídicos nacionales, cabe mencionar que las limitaciones identificadas en dicha Convención no disminuyen su valor como referencia normativa, sino que destacan la necesidad de complementar sus disposiciones con desarrollos normativos adicionales que aborden las realidades tecnológicas contemporáneas. Para Ecuador, el estudio de la Convención de Budapest proporciona elementos conceptuales y metodológicos fundamentales para informar el análisis de los desafíos jurídico-penales planteados por los delitos cibernéticos en el contexto nacional.

En el plano internacional, la regulación de los ciberdelitos no puede analizarse de forma aislada del desarrollo jurisprudencial en materia de derechos fundamentales vinculados al entorno digital. La Corte Interamericana de Derechos Humanos ha señalado, en el caso Escher y otros vs. Brasil, que las comunicaciones electrónicas se encuentran amparadas por el derecho a la vida privada y a la inviolabilidad de las comunicaciones, por lo que cualquier injerencia estatal debe cumplir estrictos estándares de legalidad, necesidad y proporcionalidad, este criterio resulta especialmente relevante para el contexto ecuatoriano,

donde la investigación de ciberdelitos exige con frecuencia el acceso a datos informáticos y metadatos de comunicaciones.

De manera concordante, el Tribunal Europeo de Derechos Humanos, en el caso Barbulescu vs. Rumania, enfatizó que el uso de herramientas tecnológicas de supervisión debe equilibrarse con la expectativa razonable de privacidad de las personas en entornos digitales, aunque esta jurisprudencia proviene del sistema europeo, su valor orientador resulta significativo, pues evidencia una tendencia internacional hacia la protección reforzada de los derechos fundamentales frente al avance de las tecnologías de vigilancia.

En el ámbito interno, la Corte Constitucional del Ecuador ha desarrollado criterios relevantes sobre la protección de la intimidad y de los datos personales en entornos digitales. En la sentencia No. **34-19-IN/21**, la Corte destacó que el tratamiento y acceso a información personal por parte del Estado debe sujetarse a parámetros de proporcionalidad y a garantías del debido proceso, especialmente cuando se utilizan herramientas tecnológicas que pueden afectar la esfera privada de las personas. Este precedente refuerza la necesidad de que la persecución de los ciberdelitos en el Ecuador se articule no solo con los compromisos internacionales, sino también con los estándares constitucionales de protección de derechos.

En base a lo mencionado, el desafío para el Ecuador no se limita a ampliar la tipificación de los ciberdelitos, sino también a garantizar que las facultades investigativas del Estado se ejerzan dentro de un marco compatible con los derechos a la intimidad, protección de datos personales y debido proceso, por lo tanto, la armonización del Código Orgánico Integral Penal con el Convenio de Budapest debe ir acompañada de una interpretación constitucional y convencional que evite expansiones desproporcionadas del poder punitivo en el ciberespacio.

Modalidades de Ciberdelitos y su Incidencia en Ecuador

Los ciberdelitos constituyen una manifestación contemporánea de la criminalidad que ha adquirido particular relevancia en el contexto ecuatoriano durante los últimos años. Miró (2012) define estos delitos como "actos delictivos realizados mediante el uso de tecnologías de la información y comunicación, que pueden dirigirse contra sistemas informáticos, datos o personas a través de medios digitales" (p. 78). Esta conceptualización resulta fundamental para comprender la naturaleza multifacética de estos ilícitos, los cuales han experimentado un crecimiento exponencial en Ecuador, especialmente durante el período 2020-2025.

La evolución de los ciberdelitos en territorio ecuatoriano presenta características particulares que reflejan tanto las transformaciones tecnológicas globales como las especificidades del contexto nacional.

Durante la pandemia de COVID-19, la acelerada digitalización de múltiples sectores de la sociedad ecuatoriana creó nuevas oportunidades para la comisión de estos delitos, tal como señala Vargas (2022), quien destaca que "la migración forzosa hacia entornos digitales, sin la correspondiente preparación en seguridad informática, generó un ambiente propicio para el incremento de actividades delictivas en el ciberespacio" (p. 89).

Las modalidades de ciberdelitos que afectan a Ecuador pueden clasificarse en tres grandes categorías, cada una con características y dinámicas específicas. La primera categoría comprende los delitos contra la integridad de sistemas informáticos, los cuales incluyen el acceso no autorizado a sistemas, el sabotaje informático y la interceptación de comunicaciones. Según Rodríguez y Castillo (2021), estos delitos representan una amenaza significativa para la infraestructura tecnológica del país, especialmente considerando la creciente dependencia de sistemas digitales en sectores críticos como la banca, las telecomunicaciones y los servicios públicos.

La segunda categoría está constituida por el fraude electrónico y las estafas digitales, modalidades que han mostrado un incremento particularmente preocupante en el contexto ecuatoriano. González et al. (2022) identifican tres variantes principales de esta modalidad delictiva: el phishing bancario, caracterizado por la suplantación de identidad de entidades financieras para obtener credenciales de usuarios; las estafas en plataformas de comercio electrónico, que involucran engaños realizados a través de tiendas virtuales falsas; y el fraude con tarjetas de crédito, que implica el uso indebido de información financiera obtenida ilegalmente.

La tercera categoría abarca los delitos contra la privacidad y datos personales, una modalidad que ha adquirido particular relevancia en el contexto de la era digital. Herrera y Morales (2023) destacan que estos delitos incluyen la violación de datos personales, entendida como el acceso, divulgación o uso no autorizado de información personal; la sextorsión, que constituye una forma de chantaje utilizando material íntimo obtenido sin consentimiento; y el ciberacoso, caracterizado por el hostigamiento sistemático a través de medios digitales.

El análisis de la evolución cuantitativa de los ciberdelitos en Ecuador revela una tendencia alarmante de crecimiento sostenido. Según datos oficiales del Ministerio del Interior (2024), los delitos informáticos registrados en el país experimentaron un aumento del 340% entre los años 2020 y 2023, cifra que evidencia la magnitud del desafío que estos ilícitos representan para el sistema de justicia penal ecuatoriano. Esta tendencia ascendente se explica por la convergencia de múltiples factores, entre los cuales destaca la falta de cultura digital de seguridad en la población ecuatoriana, aspecto que ha facilitado significativamente la comisión de estos delitos, como señalan Pérez y Luna (2023).

Caso Emblemático en Ecuador: OLA BINI

El 11 de abril de 2019, las autoridades ecuatorianas detuvieron a Ola Metodius Martin Bini, desarrollador de software sueco especializado en criptografía y seguridad informática, bajo la acusación de presunto acceso no consentido a sistemas informáticos pertenecientes a la Corporación Nacional de Telecomunicaciones (CNT). Esta detención se produjo en el mismo contexto temporal en que Julian Assange fue expulsado de la embajada ecuatoriana en Londres, generando especulaciones sobre una posible vinculación entre ambos casos.

El proceso judicial se extendió por más de cuatro años, durante los cuales Bini permaneció en Ecuador con medidas cautelares. El 25 de abril de 2023, el Tribunal de Garantías Penales de Pichincha emitió una sentencia absolutoria, determinando que la Fiscalía no logró demostrar la materialidad del delito ni la responsabilidad del acusado. Sin embargo, el 5 de abril de 2024, la Sala de Apelación de la Corte Provincial de Pichincha revocó esta decisión por mayoría de votos, declarando culpable a Bini del delito de acceso no consentido a sistema informático en grado de tentativa e imponiéndole una pena de un año de prisión.

Posteriormente, un tribunal ecuatoriano aceptó la suspensión condicional de la pena, permitiendo que el condenado permaneciera en libertad bajo ciertas condiciones, lo que evidenció las controversias generadas por la condena inicial.

El desarrollo del caso evidenció las limitaciones estructurales del sistema judicial ecuatoriano para abordar delitos informáticos complejos. La investigación fiscal se fundamentó primordialmente en presunciones sobre el conocimiento técnico del investigado y en la interpretación de actividades que podrían formar parte de prácticas profesionales legítimas en el ámbito de la seguridad informática.

La ausencia de evidencia técnica concluyente sobre el presunto acceso a los sistemas de la CNT reflejó las dificultades de las autoridades para desarrollar investigaciones forenses digitales efectivas. Esta deficiencia probatoria obligó a la fiscalía a construir su caso sobre elementos circunstanciales, lo que posteriormente generó la controversia judicial entre las dos instancias.

El caso evidenció las deficiencias del marco normativo ecuatoriano para abordar la complejidad de los delitos informáticos contemporáneos. La tipificación genérica del acceso no consentido a sistemas informáticos en el COIP no proporciona criterios suficientemente precisos para distinguir entre conductas delictivas y actividades profesionales legítimas en el ámbito de la seguridad informática.

La ausencia de regulación específica sobre investigación de vulnerabilidades y actividades de "ethical hacking" creó un vacío normativo que facilitó interpretaciones extensivas del tipo penal. Esta

deficiencia regulatoria se agravó por la falta de criterios jurisprudenciales consolidados en materia de delitos informáticos, lo que contribuyó a las decisiones contradictorias entre instancias judiciales.

Las problemáticas evidenciadas en el caso Ola Bini ponen de manifiesto no solo deficiencias en el ámbito procesal y probatorio, sino también la urgente necesidad de desarrollar capacidades técnicas robustas para enfrentar las amenazas digitales de manera preventiva. Esta situación conecta directamente con otro aspecto fundamental del análisis de los ciberdelitos: la comprensión de las vulnerabilidades de los sistemas informáticos y las estrategias necesarias para su identificación y protección. En este contexto, resulta imperativo abordar las dimensiones técnicas de la seguridad informática, particularmente en sectores estratégicos como el sistema financiero ecuatoriano.

Propuestas de Mejora al Marco Jurídico-Penal

Las propuestas de reforma del marco jurídico-penal ecuatoriano en materia de ciberdelincuencia deben sustentarse en estándares internacionales consolidados y, al mismo tiempo, adaptarse a la realidad tecnológica del país, en este sentido, la Convención de Budapest constituye el principal referente normativo, al establecer criterios para la armonización de tipos penales, mecanismos de cooperación internacional y parámetros mínimos para la investigación de evidencia digital.

En el ámbito regional, los instrumentos promovidos por la Organización de los Estados Americanos (OEA) complementan este marco de referencia, entre ellos destacan la Estrategia Interamericana Integral de Ciberseguridad, las recomendaciones técnicas en materia de ciberdelincuencia y los lineamientos de cooperación hemisférica, que ofrecen orientaciones adaptadas a la realidad latinoamericana y fortalecen la colaboración entre Estados.

A partir de estos estándares, la actualización normativa ecuatoriana debería orientarse hacia tres ejes concretos. Primero, la modernización de los tipos penales, incorporando modalidades emergentes como el uso ilícito de criptomonedas, la manipulación maliciosa mediante tecnologías de inteligencia artificial o la generación de contenidos falsificados con alto impacto social, asimismo, resulta pertinente establecer agravantes específicas cuando las conductas afecten infraestructuras críticas, generen daños económicos masivos o impacten a múltiples víctimas.

Segundo, el fortalecimiento institucional. La sola reforma legal resulta insuficiente si no se acompaña de unidades especializadas, fiscales capacitados y protocolos claros de investigación digital, esto implica invertir en tecnología forense, desarrollar capacidades técnicas permanentes y consolidar estructuras que permitan respuestas rápidas y coordinadas ante incidentes cibernéticos.

Tercero, la consolidación de la cooperación internacional y la prevención, dado el carácter transnacional del cibercrimen, Ecuador debe fortalecer su participación en redes de intercambio de

información y suscribir acuerdos específicos que faciliten la asistencia mutua, paralelamente, es indispensable promover una cultura de seguridad digital mediante programas educativos, campañas de concientización y capacitación dirigida a sectores vulnerables.

En sí, más allá de la multiplicidad de propuestas doctrinarias, la idea central es clara: el Ecuador necesita un modelo integral que combine actualización normativa, fortalecimiento institucional, cooperación internacional efectiva y educación preventiva. Únicamente mediante la articulación de estos cuatro componentes será posible construir un sistema jurídico-penal capaz de responder de manera realista y eficaz a los desafíos del crimen digital.

Seguridad Informática: ¿Cómo identificar el hackeo al sistema financiero del Ecuador y como protegerlo?

La seguridad informática del sistema financiero ecuatoriano constituye un desafío multidimensional que requiere aproximaciones integrales ante la creciente sofisticación de las amenazas cibernéticas. El contexto contemporáneo revela que Ecuador experimentó un aumento del 30% en ciberataques durante el periodo 2023-2024 (Saphirtek, 2025), posicionándose como el tercer país más afectado de América Latina en términos de ciberamenazas. Las principales amenazas identificadas incluyen phishing, ransomware y el robo de datos, junto con malwares multipropósito, malwares de tipo infostealer y criptominería ilegal las cuales comprometen la integridad del sistema financiero nacional. Paralelamente, en 2024, Ecuador registró más de 12 millones de ciberataques, representando un aumento del 30% respecto al año anterior (Cámara de Comercio de Quito, 2025), donde los sectores que más han invertido en ciberseguridad son la banca, finanzas, retail y manufactura. Esta realidad establece un imperativo de seguridad nacional que trasciende las responsabilidades individuales de las instituciones financieras para convertirse en una preocupación sistémica que demanda coordinación interinstitucional y desarrollo de capacidades defensivas especializadas.

La investigación de Rodríguez et al. (2023) establece que "los troyanos bancarios modernos incorporan técnicas de machine learning para adaptar sus patrones de ataque en tiempo real, dificultando su detección mediante sistemas basados en firmas tradicionales" (p. 87), lo que evidencia la necesidad de evolucionar hacia sistemas de detección más sofisticados que puedan operar eficazmente ante amenazas adaptativas.

La identificación proactiva de intrusiones en el sistema financiero requiere la implementación de metodologías de monitoreo continuo capaces de detectar desviaciones de patrones normales de actividad antes de que se materialicen en ataques exitosos. Los sistemas de detección basados en anomalías representan una aproximación fundamental que debe complementarse con análisis forense digital

preventivo, permitiendo la identificación temprana de indicadores de compromiso que podrían preceder a ataques más sofisticados. Esta aproximación proactiva contrasta con las metodologías forenses tradicionales que operan reactivamente después de la materialización de incidentes de seguridad, ofreciendo oportunidades para interrumpir cadenas de ataque en sus fases iniciales.

El phishing dirigido hacia clientes del sistema financiero ecuatoriano ha evolucionado hacia modalidades altamente sofisticadas que explotan características culturales y lingüísticas específicas para incrementar su efectividad. Las autoridades de supervisión bancaria han alertado sobre estrategias sofisticadas empleadas por ciberdelincuentes para obtener información privada de usuarios, incluyendo intercambio de tácticas entre países de América Latina que incrementa la complejidad de las amenazas y requiere respuestas coordinadas a nivel regional. López y Vásquez (2024) argumentan que "la adaptación cultural de campañas de phishing incrementa significativamente las tasas de éxito, ya que explotan patrones de confianza y comunicación específicos del contexto nacional" (p. 142), evidenciando la necesidad de desarrollar estrategias de concienciación igualmente contextualizadas que puedan neutralizar efectivamente estas aproximaciones.

La implementación de plataformas de inteligencia de amenazas específicamente adaptadas al contexto ecuatoriano permite la identificación proactiva de campañas dirigidas contra el sistema financiero nacional, incluyendo el monitoreo de foros clandestinos donde se comercializan datos financieros ecuatorianos y la identificación de grupos de amenaza con interés específico en el mercado nacional. García et al. (2024) establecen que "la integración de telemetría de seguridad procedente de sistemas bancarios centrales, canales digitales y infraestructura de red permite identificar campañas de ataque coordinadas que podrían pasar desapercibidas en análisis aislados" (p. 167), destacando la importancia de desarrollar capacidades de correlación de eventos que proporcionen panoramas completos de amenaza.

La protección efectiva del sistema financiero requiere la implementación de arquitecturas de seguridad multicapa que proporcionen redundancia defensiva ante la falla de controles individuales, incorporando el principio de defensa en profundidad que incluye controles en los niveles de red, aplicación, datos y endpoints. La segmentación de red representa un elemento fundamental de estas arquitecturas, permitiendo la contención de ataques exitosos y limitando su propagación lateral dentro de la infraestructura financiera. Fernández (2024) argumenta que "la microsegmentación de redes bancarias debe considerar no solo la separación entre sistemas críticos y no críticos, sino también la implementación de controles granulares basados en el contexto de transacción y perfil de usuario" (p. 98), subrayando la necesidad de aproximaciones dinámicas que puedan adaptarse a diferentes escenarios operacionales.

Los sistemas de gestión de identidad y acceso representan elementos críticos para la protección del sistema financiero, especialmente considerando que una proporción significativa de incidentes de seguridad

involucra el compromiso de credenciales legítimas, requiriendo la implementación de autenticación multifactor adaptativa basada en análisis de riesgo contextual que equilibre seguridad y experiencia de usuario. La adopción de modelos de confianza cero en el contexto financiero requiere la verificación continua de la identidad y autorización de todos los actores que interactúan con sistemas críticos. Silva y Torres (2023) establecen que "la implementación de Zero Trust en entornos financieros debe considerar las particularidades regulatorias del sector, incluyendo requisitos de trazabilidad y no repudio que pueden entrar en tensión con principios de privacidad" (p. 201), evidenciando la complejidad de balancear múltiples objetivos de seguridad y cumplimiento.

El desarrollo de capacidades de respuesta a incidentes específicamente diseñadas para el sector financiero debe considerar tanto aspectos técnicos como regulatorios, incorporando protocolos de comunicación con organismos de supervisión y coordinación interinstitucional. La experiencia de incidentes documentados en el sistema financiero ecuatoriano, como el ciberataque que afectó servicios electrónicos del Banco Pichincha, evidencia la importancia de contar con planes de continuidad operacional que incluyan escenarios de compromiso sistémico que podrían afectar simultáneamente múltiples instituciones financieras, requiriendo coordinación entre entidades privadas y organismos gubernamentales para garantizar la estabilidad del sistema de pagos nacional.

El marco regulatorio ecuatoriano para la ciberseguridad financiera debe evolucionar para abordar las amenazas contemporáneas mientras mantiene la competitividad del sector, requiriendo la armonización con estándares internacionales que facilite la adopción de mejores prácticas mientras respeta las particularidades del contexto nacional. Ramírez (2024) sostiene que "la convergencia regulatoria en materia de ciberseguridad financiera debe equilibrar la adopción de estándares internacionales con la consideración de riesgos específicos del contexto nacional" (p. 156), evidenciando la complejidad de desarrollar marcos normativos que sean simultáneamente efectivos y adaptados a las circunstancias locales.

La colaboración público-privada emerge como elemento fundamental para el desarrollo de defensas efectivas ante amenazas que trascienden las capacidades individuales de respuesta. Las instituciones financieras han coordinado con la Policía Nacional del Ecuador campañas de comunicación conjuntas dirigidas a la ciudadanía para prevenir fraudes y modalidades de delitos virtuales incrementados tras la pandemia, representando un modelo que debe expandirse hacia aspectos técnicos de intercambio de inteligencia de amenazas y desarrollo de capacidades defensivas colaborativas.

En si, la protección del sistema financiero ecuatoriano contra amenazas cibernéticas requiere aproximaciones integrales que combinen tecnologías avanzadas de detección, arquitecturas de seguridad robustas y marcos de colaboración efectivos que puedan adaptarse continuamente a la evolución de las amenazas. La implementación exitosa de estas medidas depende crucialmente del desarrollo de capacidades

humanas especializadas, el establecimiento de marcos regulatorios apropiados y la coordinación efectiva entre sectores público y privado para crear un ecosistema de seguridad resiliente que pueda mantener la confianza ciudadana en el sistema financiero nacional mientras facilita la innovación y el crecimiento económico sostenible.

Ethical hacking

El ethical hacking, o hacking ético, puede entenderse como una práctica profesional orientada a evaluar la seguridad de sistemas informáticos mediante pruebas controladas y autorizadas, a diferencia del acceso ilícito a sistemas, su finalidad no es vulnerar la seguridad para obtener un beneficio indebido, sino identificar debilidades antes de que sean explotadas por terceras personas, en sí, se trata de una herramienta preventiva moderna de ciberseguridad.

En el entorno digital actual, donde las amenazas evolucionan con rapidez y complejidad, la seguridad ya no puede limitarse a mecanismos reactivos, esperar a que ocurra un incidente para actuar implica costos económicos, reputacionales y jurídicos elevados. Desde esta perspectiva, el hacking ético cumple una función estratégica que se basa en simular escenarios reales de ataque para medir la capacidad defensiva de una organización, además se debe recalcar que su valor no radica únicamente en detectar fallas técnicas, sino en ofrecer una visión realista del nivel de exposición al riesgo.

La legitimidad de esta actividad descansa en elementos claros: autorización previa del titular del sistema, delimitación precisa del alcance de las pruebas, confidencialidad respecto de la información obtenida y reporte responsable de vulnerabilidades, sin estos requisitos, cualquier intervención podría confundirse con una conducta penalmente indebida, por ello, la diferencia entre hacking ético y ciberdelito no se basa solo en la intención subjetiva, sino en la existencia de un marco jurídico y contractual que respalde la actuación del profesional.

Desde un punto de vista jurídico, el problema surge cuando la legislación penal no distingue expresamente entre el acceso informático con fines ilícitos y aquel realizado con consentimiento y propósito preventivo, en el contexto ecuatoriano, el Código Orgánico Integral Penal tipifica el acceso no consentido a sistemas informáticos (Art. 234), pero no contempla una excepción específica para actividades de ciberseguridad autorizadas. Esta omisión puede generar inseguridad jurídica tanto para los profesionales como para las organizaciones que contratan estos servicios.

El debate evidenciado en casos mediáticos relacionados con expertos en seguridad informática demuestra que la ambigüedad normativa puede dar lugar a interpretaciones amplias del tipo penal, esto resulta problemático en un ámbito donde la línea entre prueba técnica autorizada y acceso indebido puede depender de la claridad contractual y del reconocimiento legal de la actividad.

Se debe considerar que el ordenamiento jurídico debe incorporar una cláusula expresa que excluya responsabilidad penal cuando el acceso a sistemas informáticos se realice bajo autorización válida, con fines de evaluación de seguridad y dentro de límites previamente establecidos. Esta regulación debe exigir condiciones estrictas como contrato formal, delimitación del alcance técnico, documentación detallada de procedimientos y obligación de confidencialidad; no se trata de flexibilizar la protección penal, sino de precisar sus límites para evitar que una actividad legítima quede en una zona gris, Adicionalmente, es pertinente promover mecanismos de certificación profesional reconocidos oficialmente, que acrediten tanto competencias técnicas como estándares éticos, aquello contribuiría a fortalecer la confianza institucional y a diferenciar claramente al profesional especializado del actor malicioso.

En sí, el ethical hacking no constituye una amenaza para el orden jurídico, sino una herramienta indispensable para la protección de infraestructuras digitales, no obstante, su adecuado desarrollo exige seguridad jurídica. Un marco normativo claro permitirá fortalecer la defensa cibernética nacional sin sacrificar el principio de legalidad, garantizando que la prevención no sea confundida con delito.

Marco Jurídico

Efectividad de la Legislación Penal Ecuatoriana

El marco normativo ecuatoriano en materia de ciberdelitos se estructura principalmente a través del Código Orgánico Integral Penal (COIP), particularmente en su capítulo relativo a los delitos contra la información y comunicación, desde su promulgación en 2014, este cuerpo legal representó un avance significativo al incorporar tipos penales específicos orientados a sancionar conductas que anteriormente no contaban con una regulación clara dentro del ordenamiento jurídico nacional.

Diversos autores han destacado los avances que implicó esta codificación. Jiménez (2021) sostiene que la tipificación expresa de delitos informáticos constituyó un progreso importante frente a la legislación anterior, además de incorporar agravantes relacionadas con el uso de tecnologías y reconocer la especial vulnerabilidad de determinados grupos en el entorno digital, este señalamiento permite concluir que el legislador ecuatoriano no ignoró la transformación tecnológica, sino que intentó adaptar el sistema penal a las nuevas modalidades criminales.

No obstante, la existencia de tipos penales no garantiza por sí sola la efectividad normativa. Torres y Mendoza (2022) identifican deficiencias relevantes, entre ellas la desactualización frente a modalidades emergentes como el ransomware, los ataques apoyados en inteligencia artificial (IA) o el uso ilícito de criptomonedas, a partir de esta observación, se evidencia una tensión constante entre la estabilidad del derecho penal y la dinámica acelerada de la tecnología. Se puede afirmar que el problema no radica

necesariamente en la ausencia absoluta de regulación, sino en la falta de precisión técnica y actualización periódica que permita evitar interpretaciones forzadas o extensivas de los tipos penales.

A ello se suman los desafíos procesales propios de la investigación digital. Alvarado (2023) subraya que la volatilidad de la evidencia electrónica, las dificultades en la preservación de la cadena de custodia y la escasez de personal técnico especializado limitan la eficacia del sistema de justicia, estas observaciones permiten advertir que la efectividad del marco penal no depende exclusivamente de la redacción normativa, sino de la capacidad institucional para aplicarla adecuadamente. Una legislación técnicamente correcta puede resultar nula si los operadores jurídicos no cuentan con herramientas tecnológicas y formación especializada.

La dimensión internacional agrega una complejidad adicional. Ramírez (2022) señala que la naturaleza transfronteriza de muchos ciberdelitos exige mecanismos ágiles de cooperación judicial, ámbito en el cual Ecuador enfrenta limitaciones prácticas, la lentitud en los procesos de asistencia legal mutua y las diferencias entre sistemas jurídicos pueden obstaculizar investigaciones que, por su propia naturaleza, trascienden fronteras, desde esta perspectiva, la efectividad del sistema penal ecuatoriano no puede evaluarse de manera aislada, sino en función de su integración dentro de redes internacionales de cooperación.

Por otra parte, la regulación de los ciberdelitos encuentra sustento en la Constitución de la República del Ecuador, particularmente en el reconocimiento del derecho a la intimidad y a la protección de datos personales, esto significa que los tipos penales informáticos no protegen únicamente infraestructuras tecnológicas, sino derechos fundamentales. Este fundamento refuerza la legitimidad de la intervención penal, pero también exige que su aplicación sea proporcional y respetuosa del principio de legalidad.

A partir de aquello, puede sostenerse que el Ecuador cuenta con un marco penal formalmente estructurado para enfrentar la criminalidad informática, sin embargo, su efectividad material presenta limitaciones vinculadas a la actualización tecnológica, la capacidad técnica institucional y la cooperación internacional. Las investigaciones citadas no solo evidencian fortalezas y debilidades, sino que permiten observar que el desafío actual no es simplemente crear nuevos delitos, sino perfeccionar la técnica legislativa, fortalecer la formación especializada y consolidar mecanismos de colaboración internacional, solo bajo estas condiciones el sistema penal podrá responder de manera coherente y eficaz a los retos de la criminalidad digital contemporánea.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal ha experimentado diversas reformas orientadas a fortalecer la respuesta penal frente a la criminalidad digital. Entre las más relevantes se encuentran las modificaciones introducidas mediante la Ley publicada en el Registro Oficial Suplemento 526 de 30 de agosto de 2021, asi como las reformas consolidadas en el Registro Oficial Suplemento No. 151 de 24 de octubre de 2025. Estas actualizaciones evidencian un esfuerzo legislativo por adaptar el marco penal a las transformaciones tecnológicas contemporáneas.

Particularmente relevante resulta la incorporación de los artículos 234.1, 234.2, 234.3 y 234.4, que complementan el artículo 234 relativo al acceso no consentido a sistemas informáticos. Esta ampliación no se limita a reiterar la conducta básica previamente tipificada, sino que introduce un desarrollo sistemático de conductas conexas y elementos interpretativos necesarios para una aplicación más precisa de la norma penal.

Delitos Informáticos

El desarrollo normativo de los artículos 229 a 234.4 del Código Orgánico Integral Penal (COIP) permite advertir que el legislador ecuatoriano ha construido un microsistema penal orientado a la tutela de la información y de los sistemas informáticos como bienes jurídicos autónomos, este conjunto normativo no solo responde a la expansión de la criminalidad digital, sino que refleja una evolución dogmática en la comprensión del objeto de protección penal en la sociedad tecnológica.

Desde una perspectiva sistemática, los artículos 229 y 233 se inscriben en la categoría de delitos contra la confidencialidad de la información. El artículo 229 tipifica la revelación ilegal de bases de datos y tiene como verbo rector "revelar", lo que presupone un acceso legítimo previo y una posterior difusión no autorizada. El bien jurídico protegido es la confidencialidad de datos personales o corporativos, vinculada al derecho a la intimidad y a la autodeterminación informativa, reconocidos constitucionalmente, en términos doctrinales, este tipo penal guarda relación con la protección de datos como manifestación del derecho al libre desarrollo de la personalidad (Roxin, 2016).

Por su parte, el artículo 233 incorpora verbos rectores como "acceder", "difundir" o "revelar" información pública reservada. A diferencia del artículo 229, aquí el objeto material es información clasificada o estratégica, y el bien jurídico protegido trasciende la esfera individual para situarse en la seguridad del Estado y el interés público, esta distinción confirma que no toda información goza del mismo nivel de tutela, sino que el grado de protección depende de su naturaleza y de la función que cumple en el orden constitucional.

En cuanto a los delitos contra la integridad y disponibilidad de sistemas (arts. 230, 232 y 234), se advierte una clara aproximación al modelo de la Convención de Budapest. El artículo 230, cuyo verbo rector es "interceptar", protege la confidencialidad de los datos en tránsito. El artículo 232 utiliza expresiones como "alterar", "dañar" o "interferir", orientadas a proteger la integridad y disponibilidad de los sistemas. Finalmente, el artículo 234 sanciona el "acceso no consentido", cuyo núcleo típico radica en "acceder" sin autorización a un sistema informático, configurando el denominado hacking.

En estos tipos penales, el bien jurídico ya no es exclusivamente la información como contenido, sino la seguridad de los sistemas informáticos en sí mismos, como señala Mir Puig (2015), la expansión del derecho penal hacia nuevos ámbitos tecnológicos exige reconocer bienes jurídicos funcionales, vinculados al correcto funcionamiento de infraestructuras esenciales para la vida social y económica.

En el ámbito patrimonial digital, el artículo 231 (transferencia electrónica de activo patrimonial) tiene como verbo rector "transferir" o "disponer" fraudulentamente de activos mediante sistemas electrónicos, el bien jurídico protegido es el patrimonio, aunque la modalidad comisiva es específicamente informática. El artículo 234.1, relativo a la falsificación informática, incorpora verbos como "alterar", "modificar" o "crear" datos electrónicos falsos, trasladando la lógica de la falsedad documental al entorno digital, aquí se protege la fe pública y la confianza en la autenticidad de los documentos electrónicos, elemento indispensable para la seguridad jurídica en entornos virtuales.

La jurisprudencia comparada ha contribuido a delimitar esta diferencia. El Tribunal Supremo español, en la Sentencia 300/2015, señaló que el acceso inconsentido a sistemas constituye un delito autónomo aunque no se produzca ulterior daño patrimonial, precisamente porque el bien jurídico protegido es la seguridad informática en sí misma, asimismo, la Corte Constitucional colombiana, en la Sentencia C-748/2011, destacó que la protección penal de datos personales responde a la necesidad de garantizar el derecho fundamental al habeas data en entornos digitales.

En el ámbito ecuatoriano, la Corte Constitucional ha reconocido la dimensión constitucional del derecho a la protección de datos personales y a la intimidad en sentencias relacionadas con el tratamiento indebido de información, subrayando que la digitalización amplifica los riesgos de afectación masiva de derechos fundamentales, este enfoque constitucional refuerza la legitimidad de los tipos penales previstos en el COIP.

En sí, los artículos 229 a 234.4 configuran un sistema coherente que protege distintos bienes jurídicos: (i) la confidencialidad de la información, (ii) la integridad y disponibilidad de sistemas informáticos, (iii) el patrimonio en entornos digitales y (iv) la fe pública electrónica. Los verbos rectores

acceder, interceptar, revelar, alterar, transferir, falsificar permiten identificar con claridad la conducta prohibida y diferenciar entre intrusiones tecnológicas y fraudes patrimoniales digitalizados, desde la dogmática penal, se observa una transición desde la tutela de bienes individuales clásicos hacia la protección de estructuras funcionales propias de la sociedad de la información. La consolidación de este modelo exige, no obstante, una interpretación restrictiva que evite la expansión desmedida del ius puniendi y garantice el respeto a los principios de legalidad, proporcionalidad y mínima intervención.

Delitos que son cometidos a través de medios informáticos

Delitos contra la Integridad Sexual Digital

En el ordenamiento jurídico ecuatoriano, la protección de niñas, niños y adolescentes frente a delitos cometidos por medios informáticos (ciberdelitos) se encuentra regulada en el Código Orgánico Integral Penal (COIP), los artículos 103, 104, 173 y 174 establecen tipos penales diferenciados que responden a distintas formas de afectación a la integridad sexual en el entorno digital.

El artículo 103 del COIP tipifica la pornografía con utilización de menores e incorpora verbos rectores como producir, fabricar, publicar, distribuir, divulgar, ofertar, comercializar, poseer y almacenar, estas conductas abarcan toda la cadena de creación y circulación del material ilícito. Su propósito jurídico es proteger la integridad e indemnidad sexual del menor, sancionando no solo la producción sino también la tenencia y difusión del contenido (COIP, 2014, art. 103).

Por su parte, el artículo 104 se enfoca específicamente en la comercialización de pornografía infantil, verbos como comercializar, vender o intermediar evidencian el elemento diferenciador que es el ánimo de lucro, aquí, además de proteger la integridad sexual, se busca reprimir la explotación económica del menor, castigando la obtención de beneficios derivados de este material (COIP, 2014, art. 104).

En cuanto al artículo 173, se sanciona el contacto con finalidad sexual con menores por medios electrónicos, los verbos contactar, proponer o concertar un encuentro reflejan una intervención penal anticipada, pues no se exige que el acto sexual se concrete. El objetivo de este es prevenir el abuso desde la fase preparatoria, especialmente en contextos digitales (COIP, 2014, art. 173).

Finalmente, el artículo 174 tipifica la oferta de servicios sexuales con menores por medios electrónicos, verbos como ofrecer, promocionar o solicitar muestran que la norma sanciona tanto la promoción como la demanda. Su finalidad jurídica es impedir la mercantilización del menor en el entorno digital y reforzar su protección frente a la explotación sexual que se vive en la actualidad. (COIP, 2014, art. 174).

En conjunto, estas disposiciones evidencian una respuesta penal diferenciada y preventiva frente a los riesgos que las tecnologías digitales representan actualmente para la integridad sexual de los menores.

Delitos contra la Privacidad y la Intimidad Digital

El artículo 178 del COIP, referente a la violación a la intimidad, representa un avance significativo en la protección de los derechos fundamentales en el contexto digital (COIP, 2014, art. 178). Este precepto reconoce que la intimidad personal trasciende el ámbito físico tradicional y se extiende al espacio digital, donde las personas desarrollan una parte sustancial de sus relaciones sociales y actividades personales.

La configuración de este tipo penal demuestra la evolución del concepto jurídico de intimidad, adaptándose a las realidades de una sociedad hiperconectada donde la información personal circula constantemente a través de múltiples plataformas digitales. Esta adaptación normativa responde a la necesidad de proteger la dignidad humana en todas sus manifestaciones, incluidas aquellas que se desarrollan en el ciberespacio.

Delitos Económicos y Financieros Digitales

La tipificación de los delitos patrimoniales en el ámbito digital constituye una respuesta legislativa fundamental a la creciente sofisticación de las conductas criminales económicas. El artículo 186, relativo a la estafa, y el artículo 190 del Código Orgánico Integral penal sobre apropiación fraudulenta por medios electrónicos, establecen un marco punitivo que reconoce las particularidades de los delitos económicos cometidos a través de plataformas tecnológicas (COIP, 2014, arts. 186, 190).

El artículo 186 regula la estafa, en esta figura, los verbos rectores giran en torno a engañar e inducir a error con el propósito de obtener un beneficio patrimonial indebido. El elemento esencial es el engaño como mecanismo para provocar que la víctima realice voluntariamente un acto de disposición patrimonial que le genere daño, cuando esta conducta se ejecuta por medios digitales, por ejemplo, a través de plataformas digitales se mantiene la misma estructura típica, pero cambia el medio comisivo. El propósito jurídico de esta norma es proteger el patrimonio y la confianza en las relaciones económicas, sancionando de esa manera las maniobras fraudulentas que distorsionan la voluntad de la víctima.

En cambio, el artículo 190 tipifica la apropiación fraudulenta por medios electrónicos, sus verbos rectores se centran en apropiarse, disponer o utilizar de manera fraudulenta recursos económicos mediante sistemas electrónicos. A diferencia de la estafa, aquí no necesariamente existe un engaño directo que induzca al error; el núcleo de la conducta radica en la obtención o desvío no autorizado de fondos o valores a través de mecanismos tecnológicos, el propósito jurídico es resguardar el patrimonio y la seguridad de las

transacciones electrónicas, frente a intervenciones indebidas que afectan la confianza en los sistemas digitales.

Estos preceptos legales reflejan una comprensión avanzada de cómo la tecnología ha transformado las modalidades tradicionales del fraude, creando nuevos vectores de ataque que requieren respuestas jurídicas específicas. La criminalidad económica digital se caracteriza por su capacidad de causar daños masivos a través de esquemas que pueden afectar a miles de víctimas simultáneamente.

La legislación ecuatoriana ha adoptado un enfoque preventivo y sancionador que busca disuadir estas conductas mediante la imposición de penas proporcionales a la gravedad del daño social causado.

Delitos relacionados con Dispositivos Móviles

En la legislación penal ecuatoriana, la regulación de los delitos relacionados con dispositivos móviles responde a la necesidad de enfrentar nuevas dinámicas delictivas asociadas al uso masivo de tecnología. El Código Orgánico Integral Penal dedica los artículos 192, 193, 194 y 195 a conductas que afectan tanto el patrimonio como la seguridad de las telecomunicaciones, configurando un tratamiento específico dentro del catálogo de delitos.

El artículo 192 sanciona principalmente el hecho de apoderarse, sustraer o arrebatar un dispositivo móvil, el eje de la conducta es la obtención ilegítima del bien, lo que implica una afectación directa al patrimonio del titular. Más allá del valor económico del equipo, la norma reconoce que estos aparatos contienen información personal relevante, por lo que su protección tiene también una dimensión funcional y social (COIP, 2014, art. 192).

En el artículo 193, los verbos rectores como adquirir, receptar, comercializar o almacenar equipos cuya procedencia ilícita se conoce, evidencian la intención de sancionar el circuito posterior al robo. El propósito jurídico consiste en desincentivar el mercado informal que alimenta dichas conductas, protegiendo no solo a la víctima directa sino también la estabilidad del tráfico comercial legítimo (COIP, 2014, art. 193).

Por su parte, el artículo 194 se refiere a conductas como alterar, modificar o manipular los códigos de identificación de los dispositivos, aquí el interés protegido se vincula con la integridad del sistema de registro tecnológico que permite individualizar cada terminal. La alteración de estos datos facilita la impunidad y la reinserción de equipos sustraídos al mercado, por lo que la norma actúa como un mecanismo de prevención frente a este riesgo (COIP, 2014, art. 194).

Finalmente, el artículo 195 contempla acciones como importar, distribuir, comercializar o utilizar herramientas destinadas a la alteración o clonación de dispositivos móviles. Esta disposición amplía la tutela penal hacia quienes proveen los medios técnicos que hacen posible la manipulación fraudulenta, su finalidad es proteger la seguridad de la infraestructura tecnológica y evitar que se consoliden estructuras organizadas dedicadas a este tipo de actos ilegales (COIP, 2014, art. 195).

En conjunto, estas normas cumplen una función integral dentro del sistema penal ecuatoriano: protegen el patrimonio, aseguran la trazabilidad de los dispositivos y resguardan la confianza en el entorno tecnológico, además, no se limitan a sancionar el hecho inicial de la sustracción de los dispositivos, sino que abarcan las etapas posteriores que permiten la continuidad y rentabilidad de estas prácticas ilícitas.

Delitos contra la Identidad Digital

El artículo 211 del COIP, que tipifica la supresión, alteración o suposición de la identidad y estado civil, adquiere una dimensión particular en el contexto digital (COIP, 2014, art. 211). La identidad digital se ha convertido en un activo fundamental en la sociedad contemporánea, y su manipulación puede generar consecuencias devastadoras para las víctimas.

Este delito refleja la evolución del concepto jurídico de identidad, que ahora debe contemplar tanto la identidad física tradicional como la digital. La suplantación de identidad en el ciberespacio puede facilitar la comisión de múltiples delitos secundarios, convirtiendo esta conducta en una forma de criminalidad especialmente peligrosa.

Terrorismo y la tecnología

El artículo 366 del COIP, referente al terrorismo, adquiere nuevas dimensiones en el contexto de los ciberdelitos (COIP, 2014, art. 366). El ciberterrorismo representa una de las amenazas más sofisticadas y potencialmente destructivas de la era digital, capaz de causar disrupciones masivas en infraestructuras críticas y generar pánico social a través de ataques coordinados contra sistemas informáticos.

La inclusión implícita del ciberterrorismo en el marco normativo ecuatoriano demuestra una comprensión avanzada de cómo las tecnologías pueden ser instrumentalizadas para fines terroristas. Esta modalidad delictiva se caracteriza por su capacidad de trascender fronteras geográficas y afectar simultáneamente múltiples jurisdicciones

El estudio de las disposiciones del Código Orgánico Integral Penal relacionadas con conductas cometidas a través de medios informáticos permite advertir que el derecho penal ecuatoriano ha incorporado una regulación amplia y diferenciada frente a los riesgos propios del entorno digital. Las normas analizadas

abarcan ámbitos diversos: la protección reforzada de niñas, niños y adolescentes, la tutela de la privacidad e intimidad, la defensa del patrimonio frente a fraudes electrónicos, la seguridad de los dispositivos móviles y la salvaguarda de la identidad en línea.

El resultado general muestra que el legislador ha optado por un modelo que no solo sanciona el daño ya consumado, sino que en varios casos anticipa la intervención penal para prevenir afectaciones mayores, esta característica es especialmente visible en los delitos contra la integridad sexual digital y en aquellos vinculados con la manipulación tecnológica, donde la respuesta jurídica busca frenar cadenas delictivas completas y no únicamente hechos aislados.

En términos globales, se puede mencionar que el ordenamiento penal ecuatoriano dispone de herramientas normativas suficientes para enfrentar la criminalidad informática contemporánea, no obstante, la efectividad real de este marco depende de su correcta aplicación, de la capacitación especializada de los operadores de justicia y de la actualización constante frente a la evolución tecnológica que se vive en la actualidad, así, el sistema jurídico no solo cumple una función sancionadora, sino también preventiva y protectora de derechos fundamentales en el ciberespacio.

CAPÍTULO III

METODOLOGÍA

La investigación desarrollada se enmarca en un diseño de tipo descriptivo–analítico. Es descriptiva en la medida en que identifica y caracteriza las modalidades de ciberdelitos que afectan al Ecuador, analizando sus particularidades y evolución en el periodo comprendido entre 2020 y 2025; y es analítica porque examina el marco jurídico-penal vigente, detectando vacíos normativos, desafíos procesales y posibles reformas orientadas a fortalecer la capacidad del Estado frente a la criminalidad digital.

El estudio adopta un enfoque cualitativo–cuantitativo de carácter mixto. El componente cualitativo permite abordar el análisis normativo, doctrinario y jurisprudencial sobre la tipificación, persecución y sanción de los ciberdelitos, mientras que el componente cuantitativo se fundamenta en el análisis documental de fuentes estadísticas secundarias. Este último implica el examen sistemático de datos oficiales ya existentes obtenidos de la Fiscalía General del Estado, el Ministerio del Interior y otras fuentes institucionales, sin que se hayan realizado encuestas o recolección de datos primarios. Esta aproximación metodológica permite analizar la incidencia de los ciberdelitos en el país a partir de la información estadística disponible en los registros oficiales.

En cuanto a su alcance, la investigación es exploratoria, descriptiva y propositiva. Es exploratoria porque examina fenómenos emergentes, como el uso de deepfakes, ransomware y criptomonedas para la comisión de ilícitos; descriptiva porque expone las distintas formas de ciberdelincuencia y su regulación en la legislación ecuatoriana; y propositiva porque formula recomendaciones normativas e institucionales basadas en estándares internacionales, como el Convenio de Budapest, adaptadas a las particularidades del contexto nacional.

Para la obtención y el tratamiento de la información se emplean diversos métodos. El método inductivo–deductivo permite partir de casos y estadísticas específicas para llegar a conclusiones generales y, a su vez, contrastar dichas conclusiones con la normativa y doctrina vigentes. El método analítico–sintético se utiliza para descomponer los elementos normativos, doctrinarios y procesales, integrándolos posteriormente en propuestas coherentes. Asimismo, el método comparativo facilita la confrontación entre la legislación ecuatoriana y los estándares internacionales en materia de ciberdelitos, mientras que el método documental respalda el análisis a través de la revisión exhaustiva de bibliografía especializada, normativa nacional e internacional y jurisprudencia relevante.

Las técnicas aplicadas incluyen la revisión documental de leyes, reformas, tratados internacionales, artículos académicos, informes institucionales y sentencias judiciales; el análisis estadístico de datos sobre denuncias y tendencias de ciberdelitos.

El muestreo aplicado es no probabilístico, de tipo intencional, seleccionándose como unidades de análisis las disposiciones normativas más relevantes como artículos del Código Orgánico Integral Penal, los registros estadísticos de denuncias por ciberdelitos entre 2020 y 2025 provenientes de fuentes oficiales, y la información aportada por expertos en materia jurídica y técnica vinculada a la ciberseguridad.

CAPÍTULO IV

RESULTADOS

Análisis de la Incidencia de Ciberdelitos en Ecuador

Los datos documentados por la Fiscalía General del Estado (2021) revelan un incremento significativo en los ciberdelitos registrados en Ecuador desde la implementación del Código Orgánico Integral Penal (COIP) en 2014. Según el Sistema Integrado de Actuaciones Fiscales (SIAF), se han registrado cifras alarmantes de denuncias en modalidades específicas: 829 casos de contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, 10.393 casos de apropiación fraudulenta

por medios electrónicos, 387 casos de transferencia electrónica de activo patrimonial, y 829 casos de acceso no consentido a sistemas informáticos desde 2014 (Salazar, 2021, p. 11).

Modalidades Delictivas Predominantes

La investigación de Posada Maya (2021) identifica que "transferencias forzadas, estafas y suplantación de identidad son los principales ciberdelitos que se cometen en Ecuador" según la Policía Nacional.

Según datos oficiales de la Fiscalía General del Estado, en el Ecuador entre enero del 2022 y mayo de 2025 se registraron 20,602 denuncias relacionadas a ciberdelitos.

Tipo penal	2022	2023	2024	01ene al 31may25	Total NDDS
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	355	485	943	400	2.183
Apropiación fraudulenta por medios electrónicos	3.137	3.449	3.698	1.549	11.833
Ataque a la integridad de sistemas informáticos	200	175	254	58	687
Estafa	1.063	1.339	1.483	682	4.567
Falsificación informática	24	68	116	64	272
Intercambio, comercialización o compra de información de equipos terminales móviles	1	1			2
Interceptación ilegal de datos	79	61	69	27	236
Reemplazo de identificación de terminales móviles		1			1

Reprogramación o modificación de información de equipos terminales móviles	8	3	4	1	16
Revelación ilegal de base de datos	63	29	45	26	163
Supresión, alteración o suposición de la identidad y estado civil	27	15	13	3	58
Transferencia electrónica de activo patrimonial	117	166	171	130	584
Total NDDS	5.074	5.792	6.796	2.940	20.602

Fuente: Fiscalia General del Estado

El análisis de la criminalidad vinculada al uso de tecnologías de la información exige distinguir entre delitos informáticos propiamente dichos y delitos comunes cometidos por medios informáticos, ya que ambos fenómenos responden a lógicas dogmáticas y de política criminal diferentes. Con base en información oficial de la Fiscalía General del Estado, entre enero de 2022 y el 31 de mayo de 2025 se registraron 20.602 denuncias relacionadas con conductas de esta naturaleza, lo que evidencia un incremento sostenido de la conflictividad penal en entornos digitales.

Desde una perspectiva estrictamente jurídico-penal, los delitos informáticos propiamente dichos son aquellos en los que el sistema informático, la información digital o la seguridad de las comunicaciones constituyen el bien jurídico directamente protegido. En el ordenamiento ecuatoriano, esta categoría se encuentra principalmente en los tipos penales incorporados en los artículos 234.1, 234.2, 234.3 y 234.4 del Código Orgánico Integral Penal, que tipifican el acceso no consentido a sistemas informáticos, el ataque a la integridad de sistemas, la interceptación ilegal de datos y la falsificación informática, a estos se suman otras figuras afines, como la revelación ilegal de bases de datos y ciertas conductas relacionadas con la manipulación de equipos terminales móviles, estas infracciones constituyen los nuevos tipos penales autónomos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información.

En contraste, los delitos cometidos por medios informáticos son ilícitos tradicionales en los que la tecnología opera únicamente como instrumento de ejecución, dentro de la base analizada destacan la apropiación fraudulenta por medios electrónicos, la estafa, la transferencia electrónica de activo patrimonial y la suplantación de identidad, estas cifras muestran que la apropiación fraudulenta por medios electrónicos

concentra la mayor cantidad de denuncias, seguida por la estafa, lo que confirma que el entorno digital está siendo utilizado predominantemente para la comisión de delitos patrimoniales más que para ataques directos a la seguridad informática.

Desde una aproximación criminológica, determinados grupos poblacionales presentan mayores niveles de exposición al riesgo. Datos de la Policía Nacional citados por Primicias (2024) señalan que niños y jóvenes constituyen sectores especialmente vulnerables frente a los ciberdelitos; adicionalmente, el mismo reporte advierte que el analfabetismo digital incrementa significativamente la probabilidad de victimización. Este contexto social contribuye a explicar la expansión de las conductas delictivas en entornos virtuales.

En términos territoriales, la mayor concentración de denuncias se localiza en las provincias de Pichincha, Guayas y Manabí; Moreira Mera (2025) reporta que Pichincha registra 8.089 delitos informáticos, seguida de Guayas con 4.644 casos y Manabí con 1.174, lo que confirma la focalización geográfica del fenómeno en las zonas de mayor densidad poblacional y actividad económica, sin embargo, para valorar de manera adecuada la eficacia del sistema penal no basta con examinar el número de noticias del delito; resulta imprescindible establecer cuántas de estas causas culminan efectivamente en sentencia.

En este punto emerge una limitación estadística relevante ya que la revisión de las bases públicas de la Fiscalía, así como de la información disponible en el sistema de la Función Judicial y del Consejo de la Judicatura, permite constatar que el Estado ecuatoriano publica de forma sistemática datos sobre denuncias, pero no difunde de manera consolidada el número de sentencias por delitos informáticos desagregadas por tipo penal y por provincia, esta ausencia de información impide determinar con precisión la tasa de judicialización específica para las provincias de Pichincha, Guayas y Manabí.

El examen del Código Orgánico Integral Penal (2014) revela avances importantes en la tipificación de conductas vinculadas a la criminalidad informática. La incorporación de la sección relativa a los delitos contra la seguridad de los activos de los sistemas de información y comunicación representa un progreso relevante dentro de la arquitectura jurídico-penal ecuatoriana, no obstante, la evolución de las modalidades delictivas evidencia que la respuesta normativa aún enfrenta desafíos de actualización.

En esta línea, Posada Maya (2021) sostiene que las innovaciones asociadas al delito cibernético han puesto de manifiesto las limitaciones de las instituciones tradicionales de seguridad y persecución penal. Entre los principales vacíos se advierte la insuficiente regulación de fenómenos emergentes, como el secuestro de información mediante software malicioso, determinadas formas de criminalidad vinculadas a criptoactivos y el uso malicioso de tecnologías de manipulación audiovisual avanzada. Estas lagunas

normativas reflejan la velocidad con la que evoluciona la criminalidad digital frente al ritmo más lento de la producción legislativa.

El carácter transnacional de los ciberdelitos añade, además, dificultades jurisdiccionales específicas. Como observa Salazar (2021), cuando la actividad delictiva se origina en un país, transita por varios territorios y produce el daño en otro distinto, surge la compleja cuestión de la determinación del lugar de comisión del delito, esta problemática se traduce en mecanismos de cooperación internacional todavía insuficientes, demoras en la asistencia penal mutua y ausencia de protocolos especializados para la investigación de delitos transfronterizos.

Frente a este escenario, el Estado ecuatoriano ha desarrollado ciertas capacidades institucionales para enfrentar la criminalidad informática, entre ellas se destacan la creación de unidades especializadas de investigación, el trabajo coordinado entre la Fiscalía y la Policía Nacional y la implementación de programas de concienciación ciudadana orientados a la prevención, sin embargo, persisten limitaciones que inciden en la efectividad del sistema.

En primer lugar, se evidencia insuficiencia de personal técnico especializado, particularmente en el ámbito de la informática forense y la pericia en evidencia digital, así como la necesidad de fortalecer programas de formación continua para los operadores de justicia, en segundo término, se observan restricciones en los recursos tecnológicos disponibles, reflejadas en la carencia de laboratorios forenses digitales plenamente equipados, software especializado para análisis complejo y protocolos técnicos actualizados para la preservación de evidencia digital. Finalmente, la capacitación de jueces y fiscales en materia tecnológica continúa siendo un desafío relevante, lo que repercute en la comprensión técnica de los casos y en la calidad de la respuesta jurisdiccional.

En consecuencia, aunque el Ecuador ha avanzado de manera significativa en la tipificación de los delitos informáticos especialmente con la incorporación de los artículos 234.1 a 234.4 del COIP, la evidencia empírica sugiere que subsiste una brecha entre el desarrollo normativo y la capacidad operativa del sistema penal.

CONCLUSIONES

El análisis realizado en la presente investigación permite afirmar que los ciberdelitos se han convertido en uno de los retos más complejos para el sistema jurídico-penal ecuatoriano. La acelerada digitalización de la sociedad ha propiciado la aparición de nuevas conductas ilícitas que no siempre encajan adecuadamente en las categorías tradicionales del Derecho Penal, lo que evidencia la necesidad de respuestas normativas y operativas acordes con la realidad tecnológica actual.

Aunque el Código Orgánico Integral Penal contempla tipos penales vinculados a la criminalidad informática, su alcance resulta todavía limitado frente a la constante evolución de las tecnologías, ya quee persisten vacíos regulatorios y ciertas imprecisiones en la configuración de algunos delitos, especialmente en lo relativo a fenómenos emergentes como el ransomware y el uso indebido de criptoactivos, lo cual incide en la eficacia de la persecución penal y en la seguridad jurídica.

De igual forma, se constató que las dificultades en la investigación de los ciberdelitos no se explican únicamente por aspectos normativos. Existen debilidades en materia de capacitación técnica, disponibilidad de infraestructura especializada y manejo de la prueba digital, factores que inciden directamente en la capacidad del Estado para responder de manera oportuna y efectiva frente a estas conductas y que contribuyen a la persistencia de niveles importantes de impunidad.

La adhesión del Ecuador al Convenio de Budapest constituye un paso relevante para fortalecer la cooperación internacional y armonizar la legislación interna con estándares globales en materia de ciberdelincuencia, sin embargo, la eficacia de este instrumento depende de su implementación real a nivel interno, así como del desarrollo de capacidades institucionales que permitan aplicar sus disposiciones de manera práctica y sostenida.

Desde la perspectiva constitucional, la respuesta penal frente a los ciberdelitos debe mantenerse dentro de los límites propios de un Estado constitucional de derechos y justicia. La Corte Constitucional del Ecuador, en la Sentencia No. 34-19-IN/21, ha reiterado la importancia de que toda expansión del poder punitivo respete los principios de legalidad, proporcionalidad y protección de los derechos fundamentales, criterios que también deben observarse en el ámbito digital.

En conjunto, se evidencia que el enfrentamiento de la criminalidad informática en el Ecuador requiere un enfoque integral que combine actualización normativa, fortalecimiento institucional, cooperación internacional y estrategias preventivas, con el fin de garantizar una respuesta penal eficaz y respetuosa de las garantías constitucionales.

RECOMENDACIONES

Resulta necesario impulsar una actualización del marco jurídico penal que responda de manera más precisa a las formas contemporáneas de criminalidad digital, en particular, conviene revisar la tipificación de conductas relacionadas con la extorsión mediante software malicioso, la manipulación avanzada de contenidos digitales y el uso ilícito de monedas virtuales (criptomonedas), procurando su armonización con estándares internacionales y el desarrollo de lineamientos técnicos claros para la investigación forense digital.

También es importante fortalecer la estructura institucional encargada de la investigación de ciberdelitos. La especialización de las unidades competentes, la creación o consolidación de laboratorios forenses digitales certificados y una mejor articulación interinstitucional permitirían optimizar la obtención, preservación y análisis de la evidencia electrónica.

En materia de talento humano, se recomienda promover programas permanentes de capacitación técnica y jurídica dirigidos a fiscales, jueces, peritos y personal investigador. La vinculación con universidades y centros de investigación puede contribuir a la formación de profesionales especializados y a la actualización continua frente a los cambios tecnológicos.

Respecto de la cooperación internacional, conviene fortalecer los mecanismos de intercambio de información y asistencia judicial, mediante protocolos internos que agilicen las solicitudes transfronterizas y la participación activa del Ecuador en redes regionales especializadas en ciberdelincuencia.

Desde un enfoque preventivo, se sugiere impulsar políticas públicas orientadas a la educación en seguridad digital, con programas de alfabetización tecnológica que permitan a la ciudadanía identificar riesgos y adoptar medidas básicas de autoprotección, la colaboración entre el sector público y el privado puede potenciar estas iniciativas, especialmente en ámbitos sensibles como el financiero.

Finalmente, se recomienda avanzar hacia una regulación complementaria que incorpore mecanismos administrativos de supervisión y prevención frente a tecnologías emergentes, de modo que el ordenamiento jurídico no actúe únicamente de forma reactiva, sino que anticipe los riesgos asociados al uso indebido de herramientas digitales.

REFERENCIAS BIBLIOGRÁFICAS

Acurio del Pino, S. (2015). *Delitos informáticos: Generalidades*. Corporación de Estudios y Publicaciones.

Albán Gómez, E. (2020). Los delitos informáticos en el Código Orgánico Integral Penal: Análisis dogmático. *Revista Jurídica de la Universidad Católica de Santiago de Guayaquil, 37*(2), 167-189.

Alvarado, M. (2023). Evidencia digital y proceso penal: Desafíos en la investigación de ciberdelitos. *Revista Ecuatoriana de Derecho Penal*, 15(2), 45-67.

Asamblea Nacional del Ecuador (2008). *Constitución de la Republica del Ecuador*. Registro Oficial No. 449.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180 de 10 de febrero de 2014.

Cámara de Comercio de Quito. (2025, mayo). *Ecuador acelera su migración a la nube: ¿qué sectores lideran y cómo enfrentan las ciberamenazas?* Recuperado de

Clough, J. (2010). *Principles of cybercrime*. Cambridge University Press

Corte Constitucional de Colombia. (2011). Sentencia C-748/11.

Corte Constitucional del Ecuador. (2021). Sentencia No. 34-19-IN/21.

Davis, C., & Rodriguez, E. (2021). Legal frameworks for authorized penetration testing: A global perspective. *Cybersecurity Law Review*, 18(4), 78-95.

Fernández, C. (2024). Microsegmentación en redes bancarias: Implementación y desafíos. *Revista de Seguridad Informática*, 18(2), 89-105.

Fiscalía General del Estado. (2021). *Ciberdelitos: Una primera aproximación y proyección institucional*. En *Perfil Criminológico - Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*. Quito: FGE.

García, L., Morales, P., & Herrera, J. (2024). Integración de telemetría de seguridad en sistemas financieros. *Ciberseguridad Latinoamericana*, 12(1), 156-178.

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunication Union.

González, P., Martínez, L., & Rodríguez, A. (2022). Fraude electrónico en Ecuador: Análisis de modalidades y tendencias 2020-2022. *Revista de Criminología Digital*, 7(1), 89-112.

Guerrero, A. M. (2022). La prueba digital en el proceso penal ecuatoriano: Desafíos y perspectivas. *Revista Ecuatoriana de Derecho Procesal, 5*(1), 43-62.

Herrera, M., & Morales, J. (2023). Delitos contra la privacidad en el entorno digital: Análisis del caso ecuatoriano. *Derecho y Tecnología*, 18, 67-89.

Jiménez, C. (2021). El tratamiento de los ciberdelitos en el Código Orgánico Integral Penal ecuatoriano. *Revista Jurídica Online*, 14(2), 234-256.

Keyzer, P. (2013). *Internet and the law: Technology, society, and compromises*. University of New South Wales Press.

López, M., & Vásquez, R. (2024). Ingeniería social contextualizada en ataques financieros. *Revista Internacional de Cibercrimen*, 15(3), 134-152.

Ministerio del Interior del Ecuador. (2024). *Estadísticas de seguridad ciudadana 2020-2023*. Quito: MINDEF.

Mir Puig, S. (2015). *Derecho penal. Parte general* (10.ª ed.). Reppertor.

Miró, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Moreira Mera, E. (2025, 26 de junio). *Ciberdelitos en Ecuador aumentan: conoce los fraudes más comunes y dónde atacan más.* Expreso.

Moreno, A., & Vega, L. (2022). Medidas cautelares en el proceso penal digital. *Revista de Derecho Procesal Penal*, 19(1), 34-56.

Páez, J., & Acurio, S. (2010). *Derecho y nuevas tecnologías*. Corporación de Estudios y Publicaciones.

Paladines, J. (2021). La criminalización de conductas en el ciberespacio: Análisis crítico desde la dogmática penal contemporánea. *Revista Iuris Dictio, 27*, 119-138.

Pérez, R., & Luna, S. (2023). Cultura digital y vulnerabilidad ante ciberdelitos en Ecuador. *Estudios Sociales Digitales*, 9(1), 45-68.

Posada Maya, R. (2021). Una aproximación a las dificultades en la investigación y persecución de los cibercrímenes. En *Perfil Criminológico - Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*. Fiscalía General del Estado, pp. 17-33.

Primicias. (2024, marzo 12). Los ciberdelitos crecen en Ecuador y los niños son las víctimas más vulnerables. *Primicias*.

Ramírez, E. (2024). Convergencia regulatoria en ciberseguridad financiera latinoamericana. *Derecho y Tecnología*, 19(1), 145-168.

Ramírez, H. (2022). Cooperación judicial internacional en ciberdelitos: Obstáculos y oportunidades. *Revista de Derecho Internacional*, 25(2), 178-198.

Rodríguez, M. (2023). Cooperación internacional en materia de cibercrimen: Desafíos para América Latina. *Derecho Penal Internacional*, 41(3), 195-210.

Rodríguez, M., & Castillo, E. (2021). Ataques a sistemas informáticos en Ecuador: Tipología y respuesta penal. *Ciberseguridad y Derecho*, 4, 234-267.

Rodríguez, P., Silva, M., & Torres, L. (2023). Evolución de troyanos bancarios y técnicas de evasión. *Malware Research Quarterly*, 7(2), 78-96.

Roxin, C. (2016). *Derecho penal. Parte general. Tomo I*. Civitas.

Salazar, D. (2021). El rol de la Administración de Justicia y la cooperación internacional en la lucha contra la ciberdelincuencia. En Perfil Criminológico - Revista Científica de Ciencias Jurídicas, Criminología y Seguridad. Fiscalía General del Estado, pp. 8-15.

Salazar, T. (2022). Protocolos de investigación forense digital: Propuesta metodológica. *Revista Forense*, 13(4), 67-89.

Saphirtek. (2025, 27 de enero). *Ciberataques en Ecuador: alarmante aumento en 2024*.

Silva, A., & Torres, M. (2023). Zero Trust en infraestructura financiera: Implementación y consideraciones regulatorias. *Financial Technology Review*, 16(4), 189-210.

Torres, G., Rodríguez, M., & Salazar, J. (2018). Evolución del marco normativo de las telecomunicaciones en Ecuador (1990-2017). *Revista Espacios, 39*(7), 10-24.

Torres, V., & Mendoza, C. (2022). Vacíos normativos en la legislación ecuatoriana sobre ciberdelitos. *Revista Crítica de Derecho*, 18(3), 201-223.

Tribunal Supremo (España). (2015). Sentencia 300/2015.

Vargas, I. (2022). Impacto de la pandemia COVID-19 en los ciberdelitos: El caso ecuatoriano. *Revista de Seguridad Digital*, 11(2), 78-95.

Villacís, C., & Zambrano, P. (2019). Cifra negra en delitos informáticos: Análisis comparativo entre denuncias formales e incidentes reportados en Ecuador. *Revista Criminalidad, 61*(2), 193-217.