ASCE MAGAZINE ISSN: 3073–1178

Revista ASCE Magazine, Periodicidad: Trimestral, Volumen: 5, Número: 2, Año: 2026 páginas 2747-2765

Doi: https://doi.org/10.70577/asce.v5i2.904

Recibido: 2026-04-15

Aceptado: 2026-04-29

Publicado: 2026-06-09

La Debilidad Normativa en Delitos Informáticos en Ecuador: Un Análisis Crítico del Coip y Lopdp

The Regulatory Weakness in Cybercrime in Ecuador: A Critical Analysis of the COIP and LOPDP

Autor(s)

Carmen del Rocío Acosta Sila [1]
Abogada de los Tribunales y Juzgado de la República del Ecuador.
Maestría en Derecho Penal
cdacostas@ube.edu.ec
https://orcid.org/0009-0000-8353-2333
Universidad Bolivariana del Ecuador
Guayaquil – Ecuador

Dra. Gina de Lourdes Jácome Veliz [2]
Docente, conferencista y facilitadora de post grado y pre grado en universidad
gdjacomev@ube.edu.ec
https://orcid.org/0009-0007-2204-4708
Universidad Bolivariana del Ecuador
Guayas – Ecuador

Dra. Sandra Patricia Morejón Llanos [3]
spmorejonl@ube.edu.ec
https://orcid.org/0009-0009-7229-438X
Universidad Bolivariana del Ecuador
Guayas – Ecuador

Como Citar

Acosta Sila. C. R. &, Jácome Veliz. G. L. &, Morejón Llanos. S. P. (2026) La Debilidad Normativa en Delitos Informáticos en Ecuador: Un Análisis Crítico del Coip y Lopdp ASCE MAGAZINE 5(2) 2747-2765

Resumen

La acelerada expansión del entorno digital ha generado nuevas formas de criminalidad que ponen en evidencia la limitación del marco jurídico ecuatoriano frente al cibercrimen. En este contexto, el problema central que aborda la presente investigación radica en la fragmentación existente entre la regulación penal de los delitos informativos prevista en el Código Orgánico Integral Penal (COIP) y la regulación administrativa contenida en la Ley Orgánica de Protección de Datos Personales (LOPDP), así como en la ausencia de una política criminal digital integral que articule prevención, sanción y protección efectiva de los derechos digitales. el objetivo del artículo es analizar críticamente las debilidades normativas de esta desarticulación, identificando los vacíos legislativos que dificultan la persecución penal y reducen la eficacia de la tutela jurídica en el entorno digital. La investigación se desarrolló bajo un enfoque cualitativo, aplicando métodos empíricos, análisis documental y jurisprudencial y métodos teóricos-dogmáticos, históricos-lógicos y comparados, contrastando la normativa ecuatoriana con estándares internacionales como la Convención de Budapest y el Reglamento General de Protección de Datos (RGPD). Los resultados evidencian que, aunque el COIP tipifica conductas informáticas básicas, no incorpora de manera suficiente delitos emergentes, mientras que la LOPDP se limita a un régimen sancionador administrativo, sin conexión efectiva con el sistema penal. Se concluye que esta fragmentación normativa, sumada a la inexistencia de una política criminal digital coherente, debilita la respuesta estatal frente al cibercrimen y exige una reforma legislativa integral.

Palabras clave: Protección de datos; seguridad informática; derecho a la privacidad; tecnología de la información; política criminal.

Abstract

The accelerated expansion of the digital environment has generated new forms of criminality that reveal the limitations of the Ecuadorian legal framework in addressing cybercrime. In this context, the central problem examined in this study lies in the fragmentation between the criminal regulation of cyber offenses established in the Comprehensive Organic Criminal Code (COIP) and the administrative regulation set forth in the Organic Law on Personal Data Protection (LOPDP), as well as in the absence of a comprehensive digital criminal policy capable of integrating prevention, punishment, and effective protection of digital rights. The aim of this article is to critically analyze the normative weaknesses resulting from this disarticulation, identifying legislative gaps that hinder criminal prosecution and undermine legal protection in the digital sphere. The research adopts a qualitative approach, applying empirical methods, including documentary and jurisprudential analysis, as theoretical methods dogmatic, historical-logical, and comparative methods contrasting Ecuadorian legislation with international standards such as the Budapest Convention and the General Data Protection Regulation (GDPR). The findings indicate that while the COIP criminalizes basic cyber-related conduct, it fails to adequately address emerging offenses, whereas the LOPDP remains confined to an administrative sanctioning framework without effective linkage to criminal law. It is concluded that this regulatory fragmentation, combined with the lack of an integrated digital criminal policy, weakens the State's response to cybercrime and highlights the need for comprehensive legislative reform.

Keywords: Data protection; cyber security; right to privacy; information technology; criminal policy.

Introducción

La transformación digital y el crecimiento acelerado del ciberespacio han generado nuevas formas de criminalidad que desafían los marcos jurídicos tradicionales. En Ecuador, los delitos informáticos se encuentran regulados en el Código Orgánico Integral Penal (COIP), específicamente en la sección tercera, artículos 229 al 234, en los cuales se tipifican conductas como el acceso no autorizado a sistema informático, la interferencia de sistema la interceptación de datos y el uso indebido de información

Paralelamente, la Ley Orgánica de Protección de Datos Personales (LOPDP) constituye un cuerpo normativo transversal orientado a regular el tratamiento y la protección de los datos personales, estableciendo principios, derechos, obligaciones y medidas de seguridad frente a posibles vulneraciones.

No obstante, pese a la relevancia de ambas normativas, se evidencia una desarticulación estructural entre el ámbito penal y el administrativo. Mientras el COIP presenta una regulación parcial y limitada frente a la complejidad de la ciberdelicuencia, la LOPDP se enfoca en un régimen preventivo y sancionador de carácter administrativo, sin establecer mecanismos de conexión efectiva con el sistema penal.

Esta situación genera vacíos normativos que dificultan la persecución penal de conductas emergentes, como el ransomware, el phishing sofisticado, la suplantación de identidad mediante inteligencia artificial y la manipulación de contenidos digitales, debilitando la protección de derechos fundamentales como la privacidad, la seguridad de la información y la autodeterminación informática.

En este contexto, el objetivo del presente artículo es analizar críticamente la debilidad normativa de la desarticulación entre COIP y la LOPDP, identificando los principales vacíos legislativos y proponiendo lineamientos para una política criminal digital integral acorde con los estándares internacionales en materia de ciberseguridad y protección de datos.

Material y métodos

La presente investigación se desarrolló bajo un enfoque cualitativo de tipo documental y dogmático, orientado al análisis crítico del marco jurídico ecuatoriano en materia de ciberdelincuencia. En el plano empírico, se recurrió al análisis documental jurisprudencial de normativa, doctrina y casos relevantes, con el propósito de identificar vacíos normativos y limitaciones en la persecución penal de los delitos informáticos.

En el plano teórico, se aplicaron métodos dogmatico-juridico, analítico histórico-lógico y comparado. El método analítico permitió descomponer las disposiciones del COIP y la LOPDP para examinar sus alcances y limitaciones, mientras que el método histórico-lógico facilitó la comprensión de la evolución normativa en materia de protección de datos y ciberdelicuencia.

Finalmente, el método comparado permitió contrastar la legislación ecuatoriana con estándares internacionales, particularmente con el convenio de Budapest sobre ciberdelincuencia y el reglamento general de protección de datos (RGPD), con el fin de identificar buenas prácticas y posibles líneas de reforma normativa.

Resultados

Evaluación del tratamiento legal de los delitos informático en el COIP y la LOPDP.

Según Villavicencio (2014), el fenómeno de los delitos informáticos surge en el marco de la evolución de las tecnologías de la información y comunicación (TIC), particularmente con la expansión de internet a finales del siglo XX. El autor advierte que no todo uso de computadoras en un acto ilícito constituye un ciberdelito, sino que este debe guardar relación directa con la afectación a la integridad, disponibilidad o confidencialidad de los sistemas y la información.

De acuerdo con Ponce (2024), los delitos informáticos comprenden actividades ilícitas cometidas mediante el uso de medios electrónicos o informáticos, en las que se ven afectados bienes jurídicos como la integridad de los sistemas y la privacidad de los usuarios. El autor señala que la legislación actual no tipifica de manera clara todos los delitos informáticos, dejando fuera conductas emergentes como el ciberacoso o el secuestro digital, y que las sanciones previstas no siempre son

suficientes para disuadir a los delincuentes. Además, resalta la desconexión entre la protección administrativa de los datos personales y la persecución penal, lo que genera vacíos legales y dificulta la aplicación efectiva de la ley. Para Ponce, estas limitaciones evidencian la necesidad de reformas integrales que articulen la protección de la información con la persecución penal, así como una mayor cooperación institucional y educación ciudadana para fortalecer la seguridad digital en Ecuador.

En Ecuador, el Código Orgánico Integral Penal (2021), incorporo tipos penales vinculados con seguridad informática, los artículos 229 al 234, los cuales buscan tutelar bienes jurídicos relacionados con la seguridad digital y la información. Destacan el acceso no consentido a sistema informáticos (art. 229), la interferencia en sistemas (art. 230), la intercepción de datos (art. 231) y el ataque a la integridad de sistemas (art. 232), figuras que constituyen el núcleo de la protección penal frente a conductas que comprometen la confidencialidad, integridad y disponibilidad de la información. Asimismo, se tipifica la producción y difusión de software malicioso (art. 233) y la falsificación informática (art. 234), delitos que atienden a fenómenos de manipulación y alteración de datos con fines fraudulentos. Estos tipos penales evidencian un intento del legislador por actualizar el marco jurídico a la realidad digital, reconociendo que la criminalidad informática afecta tanto a individuos como a infraestructuras críticas.

Sin embargo, pese a estos avances, el COIP no desarrolla un régimen sistemático y articulado de delitos informáticos, lo que genera vacíos normativos y dificultades en la persecución penal. La dispersión normativa impide una adecuada clasificación de estas conductas, limita la adaptación frente a nuevas tipologías criminales (como el phishing o el ransomware) y plantea riesgos de inseguridad jurídica. De ahí que, aunque los artículos mencionados son relevantes, su aplicación práctica requiere ser complementada con marcos normativos especializados, como la Ley Orgánica de Protección de Datos Personales (2021), que aporta principios de tutela de la información personal y mecanismos preventivos que el COIP, desde su perspectiva sancionadora, no cubre en su totalidad.

Paralelamente, la protección de datos personales ha adquirido relevancia como derecho fundamental. Para Cuello (1986), Alan Westin en 1967 vinculó la privacidad con el control de la información personal, mientras que Solove (2008), desarrolló una taxonomía sobre las formas de afectación a la privacidad en entornos digitales. En Ecuador, este reconocimiento se materializó

con la Ley Orgánica de Protección de Datos Personales (2021) inspirada en estándares internacionales como el Reglamento General de Protección de Datos (RGPD) europeo.

La selección de estos conceptos se justifica porque permiten comprender la doble dimensión de la investigación: los desafíos dogmáticos y legislativos para definir y sancionar los delitos informáticos y la necesidad de garantizar la protección de datos personales como bien jurídico autónomo en un entorno digital vulnerable.

Figura 1. Delitos informáticos tipificados en el COIP (Artículos 229 al 234).

Artículo	Delito	Bien jurídico protegido	Conducta sancionada	Límites o alcances del tipo penal
Art. 229 Revelación ilegal de base de datos	**Privacidad, intimidad y secreto**	La revelación intencional de datos contenidos en ficheros o bases de datos	Revelar información registrada en sistemas electrónicos, sin autorización, en beneficio propio o de terceros. Si lo comete un servidor público o empleado bancario, la pena se agrava.	Enfocado en la revelación de datos; no aborda otras formas de acceso no autorizado.
Art. 230 Interceptación ilegal de datos	**Confidencialidad de las comunicaciones**	La interceptación, desviación, grabación o copia de datos o transmisiones sin orden judicial	Incluye técnicas como phishing mediante sitios fraudulentos, clonación de tarjetas y fabricación de dispositivos para interceptar datos.	Aunque abarrotado, algunos métodos emergentes, como interceptaciones vía IoT, podrían quedar fuera.
Art. 231 Transferencia electrónica de activo patrimonial	**Patrimonio**	Apropiación o transferencia no consentida de valores digitales o patrimoniales	Manipular software para obtener transferencias o facilitar datos bancarios con ese propósito.	Se centra en transferencias patrimoniales; quizás no capta fraudes sin movimiento de fondos.
Art. 232 Ataque a la integridad de sistemas informáticos	**Integridad y disponibilidad**	Destruir, alterar, bloquear o interferir sistemas o datos; incluye creación y distribución de malware	Penaliza daños y alteraciones en sistemas; agrava si se daña infraestructura pública o de seguridad.	Bien redactado, pero las penas podrían no reflejar completamente el daño ocasionado por ataques sofisticados a gran escala.
Art. 233 Delitos contra la información pública reservada legalmente	**Seguridad del Estado**	Protección de información clasificada legalmente	Destruir o inutilizar información reservada o gestionarla sin autorización; pena máxima si compromete la seguridad del Estado.	Restricto al ámbito público; la filtración de datos clasificados desde el sector privado o tecnológico podría quedar fuera.
Art. 234 Acceso no consentido a sistemas informáticos	**Acceso legítimo y explotación de sistemas**	Acceder o mantenerse en sistemas sin autorización para explotar accesos, re direccionar o usar servicios sin pago	Penaliza acceso no autorizado, modificación de portales, desvío de tráfico, uso indebido de servicios.	Amplio, pero tecnologías nuevas como ataques por IA o deepfakes que simulan acceso legítimo podrían no estar contempladas.

Fuente: Elaboración Propia.

Análisis de los artículos 229 al 234 del COIP evidencia un esfuerzo legislativo por tipificar diversas conductas vinculadas a la criminalidad informática, protegiendo bienes jurídicos como la privacidad, la confidencialidad, la integridad de los sistemas, el patrimonio y la seguridad del Estado. Sin embargo, aunque los tipos penales muestran un avance técnico, incluyendo figuras como la interceptación mediante phishing o la manipulación de sistemas para transferencias patrimoniales, persisten vacíos importantes. La normativa se concentra en aspectos tradicionales de la informática, sin abarcar fenómenos emergentes como el ransomware, la sextorsion, el ciberacoso o la explotación ilícita de criptomonedas. Además, los tipos carecen de parámetros claros para graduar el daño, lo que genera riesgos de proporcionalidad sancionatoria. En definitiva, aunque el COIP representa un avance frente a la realidad digital, su alcance limitado y su falta de actualización frente a las nuevas dinámicas de los delitos informáticos comprometen la eficacia de la protección penal en Ecuador (Código Orgánico Integral Penal, 2021).

Riesgos tecnológicos actuales y límites del modelo penal vigente

La acelerada evolución tecnológica ha generado nuevas modalidades de criminalidad digital que desbordan los esquemas tradicionales de tipificación penal. En este contexto, uno de los principales riegos actuales radica en la desconexión entre la dinámica del desarrollo tecnológico y la rigidez del modelo de tipos penales previsto en el código orgánico integral penal (COIP), el cual no ha sido diseñado bajo una lógica de adaptabilidad tecnológica. Esta situación provoca que el legislador penal se vea obligado a impulsar reformas constantes para incorporar nuevas conductas delictivas, generando un marco normativo reactivo, fragmentado y, en ocasiones, tardío frente a la realidad del cibercrimen.

La ausencia de tipos penales tecnológicos dinámicos, capaces de abarcar conductas digitales complejo sin depender de descripciones cerradas o tecnología específicas, incrementa los riesgos de impunidad y de inseguridad jurídica. En particular, el COIP no cubre de manera óptima debido a su ambigüedad normativa conductas emergentes como el ransomware avanzado caracterizado por la encriptación masiva de sistema y la extorsión digital transnacional; el phishing sofisticado, que utiliza técnicas de ingeniería social altamente personalizadas y entorno digitales simulados; la suplantación de identidad mediante inteligencia artificial, que permite replicar voz, imagen o patrones de comportamiento; ni la utilización de deepfakes con fines de fraude, extorsión,

manipulación informativa o afectación a la reputación personal e institucional (Taco Sánchez y Villacis Mogrovejo, 2025).

Estas conductas, si bien pueden intentar subsumirse de manera forzada en tipos penales tradicionales como el acceso no autorizado, la falsificación informática o el fraude, no encuentran una cobertura penal clara, sistemática ni proporcional. Ello no solo debilita la persecución penal efectiva, sino que rompe la conexión esperada entre el COIP y la Ley Orgánica de Protección de Datos Personales (LOPDP), pues mientras esta última establece obligaciones preventivas frente a riesgos tecnológicos avanzados, el derecho penal carece de herramienta normativa suficiente para sancionar de manera coherente las vulneraciones graves derivadas del uso ilícito de tecnologías emergentes

En consecuencia, la falta de un enfoque de política criminal digital integral, en tipos penales flexibles y tecnológicamente adaptables, impide una articulación efectiva entre la protección administrativa de los datos personales y la respuesta penal frente a los delitos informáticos, perpetuando vacíos normativos que favorecen la impunidad y debilitan la tutela de los derechos digitales en Ecuador.

Figura 2. Disposiciones relevantes de la LOPDP frente a la vulneración de datos personales.

Artículo	Disposición	Bien jurídico protegido	Conducta / Obligación	Límites o alcances
Art. 37 Seguridad de datos personales	Establece la obligación de implementar medidas de seguridad proporcionales al tipo y volumen de datos.	Confidencialidad, integridad y disponibilidad de los datos personales.	Aplicar cifrado, desidentificación, controles de acceso, auditorías y planes de continuidad.	No prevé sanciones penales por incumplimiento; se restringe al ámbito administrativo.
Art. 41 Determinación de medidas de seguridad aplicables	Obliga a realizar un análisis de riesgos y adoptar medidas preventivas.	Seguridad preventiva de la información y derechos de los titulares.	Establecer medidas técnicas, organizativas y jurídicas para reducir riesgos.	No vincula estas medidas con procesos penales; se limita a la prevención administrativa.
Art. 43 Notificación de vulneración de seguridad	Obliga al responsable a notificar vulneraciones a la Autoridad de Protección de Datos y a la ARCOTEL en un máximo de 5 días.	Derecho a la información y a la protección frente a incidentes de seguridad.	El encargado debe notificar al responsable en 2 días; este, a su vez, a la Autoridad.	El incumplimiento no implica sanciones penales; únicamente administrativas.
Art. 46 Notificación de vulneración de seguridad al titular	Ordena informar al titular de los datos en un plazo de 3 días cuando exista riesgo a sus derechos fundamentales.	Autodeterminación informativa, privacidad y confianza del titular.	Comunicar de manera clara y oportuna la vulneración y las medidas adoptadas.	No establece sanciones penales por la omisión; las excepciones reducen la efectividad de la protección.
Art. 76 Funciones, atribuciones y facultades	Define a la Autoridad de Protección de Datos como órgano de control con potestad sancionadora.	Derecho fundamental a la protección de datos personales.	Realizar auditorías, imponer sanciones administrativas, crear el Registro Nacional.	Carece de facultades penales, lo que impide articular la protección administrativa con el COIP.

Fuente: Elaboración propia.

El cuadro evidencia que, aunque la Ley Orgánica de Protección de Datos Personales en Ecuador establece obligaciones claras sobre seguridad, confidencialidad y notificación de vulneraciones, su alcance sancionador resulta limitado frente a los delitos informáticos. Se privilegia un enfoque preventivo y administrativo, dejando fuera sanciones penales contundentes, lo que genera un vacío frente a la creciente sofisticación del cibercrimen. El hecho de que la mayoría de incumplimientos solo deriven en sanciones administrativas refleja una debilidad normativa que no disuade conductas ilícitas graves. Asimismo, se otorga a la Autoridad de Protección de Datos un rol regulador y sancionador, pero sin herramientas penales efectivas que articulen con el COIP. En consecuencia, la ley resulta más garantista en lo declarativo que en lo coercitivo, debilitando la tutela real de

derechos como la privacidad y la seguridad digital. Esto evidencia la necesidad de una armonización normativa que integre sanciones penales específicas y eficaces para los delitos informáticos (Ley Orgánica de Protección de Datos Personales, 2021).

Relación e independencia entre protección administrativa (LOPDP) y sanción penal (COIP).

Los autores García y Arciniegas (2023), examinan la tensión normativa entre el COIP y la LOPDP frente a los retos de las nuevas tecnologías. Su postura parte de reconocer que el COIP ha quedado rezagado frente al auge de los ciberdelitos, limitándose a un catálogo reducido de infracciones, mientras que la LOPDP representa un avance administrativo en la tutela de datos personales. Sin embargo, resaltan que ambas normativas funcionan de manera complementaria pero desarticulada. Por otra parte, demuestran que la debilidad normativa ecuatoriana no está solo en la ausencia de tipos penales desactualizados, sino también en la falta de articulación entre la protección administrativa de datos y la sanción penal de delitos informáticos. Su propuesta implícita es que se deben generar reformas integrales que incluyan tanto la prevención administrativa (LOPDP) como la represión penal (COIP), con el fin de cerrar la brecha de impunidad frente al cibercrimen.

Según Randi (2022), el autor parte de un diagnóstico crítico que en Ecuador existe una brecha entre la protección administrativa de la LOPDP y la sanción penal del COIP. Mientras la LOPDP introduce principios modernos de privacidad como la responsabilidad proactiva y el consentimiento informado, su alcance se limita al ámbito administrativo. Por su parte, el COIP tipifica ciertos delitos informáticos (acceso no autorizado, violación de la intimidad, pornografía infantil, etc.), no logra abarcar la complejidad de los delitos informáticos actuales, como el phishing, el fraude electrónico, la clonación de tarjetas o la manipulación de datos en entornos digitales. Esto provoca que muchas conductas ilícitas queden sin sanción penal efectiva.

Identificación de vacíos normativos y limitaciones en la regulación actual frente a los delitos informáticos.

Según el estudio realizo por Espinosa y Fuentes (2025), los autores mencionan que el sistema penal ecuatoriano enfrenta vacíos normativos significativos frente a los delitos informáticos, ya que, aunque el COIP tipifica conductas como acceso no autorizado a sistemas, suplantación de identidad y ciberacoso, carece de precisión ante modalidades complejas como ransomware, fraude con criptoactivos y secuestro digital, lo que genera ambigüedades y altos niveles de impunidad.

Además, la fragmentación normativa entre el COIP, la Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico limita la articulación efectiva de la protección de datos con la persecución penal, mientras la escasa especialización de operadores judiciales y la falta de recursos técnicos dificultan la recolección de pruebas digitales y la cooperación interinstitucional, evidenciando la necesidad urgente de actualizar y armonizar la legislación para fortalecer la prevención y sanción de los ciberdelitos en Ecuador.

Para Herrera y Balseca (2025), evidencian que la Ley de Protección de Datos en Ecuador presenta vacíos estructurales que limitan la seguridad frente a delitos informáticos. Carece de criterios claros para clasificar datos según su criticidad, lo que impide priorizar vulneraciones graves, mientras la supervisión institucional es fragmentada y dependiente de acciones aisladas. Esta debilidad se refleja en ciberataques a bancos, telecomunicaciones y municipalidades, donde las respuestas son inmediatas pero sin sanciones efectivas ni protocolos estandarizados. Los autores concluyen que la ausencia de una estrategia integral que articule regulación, capacitación, supervisión y coordinación interinstitucional perpetúa brechas legales y favorece la impunidad, por lo que urge una reforma profunda para garantizar protección de datos y seguridad digital en el país.

De acuerdo con Veloz (2025), señala que la legislación ecuatoriana sobre delitos informáticos es insuficiente, obsoleta y fragmentada, lo que compromete la seguridad digital y genera inseguridad jurídica. La falta de regulación específica dificulta la recolección de pruebas digitales, limita la eficacia judicial y aumenta la impunidad frente a delitos como phishing, ransomware y robo de identidad. Además, la ausencia de cooperación internacional y adaptación a nuevas tecnologías deja al país vulnerable ante ciberdelincuentes transnacionales y riesgos emergentes, afectando la confianza ciudadana. La autora concluye que se requiere un marco legal integral que combine sanción, prevención y educación en ciberseguridad, alineado con estándares internacionales y la realidad tecnológica de Ecuador.

Propuestas de reformas legales que articulen la protección de datos con la persecución penal en el entorno digital.

La necesidad de fortalecer el marco jurídico ecuatoriano frente a los delitos informáticos exige reformas que integren la protección de datos personales con la persecución penal, superando la actual desconexión entre la LOPDP y el COIP. Una reforma integral debe contemplar no solo la actualización de los tipos penales relacionados al uso inadecuado de la información digital, sino

también la creación de mecanismos de coordinación institucional, responsabilidad con los estándares internacionales de ciberseguridad. En este contexto, resulta indispensable analizar los modelos comparados y las experiencias internacionales que sirvan de referencia para diseñar un sistema normativo más coherente, eficaz y acorde con la realidad tecnológica del país.

Análisis comparado con estándares internacionales sobre ciberdelitos y datos personales.

La experiencia comparada demuestra que la regularización integral es indispensable para enfrentar los delitos informáticos. La Convención de Budapest sobre Ciberdelincuencia (2001), establece parámetros claros sobre conductas como el acceso ilícito (art. 2), la interceptación ilegal de datos (art. 3), la falsificación informática (art. 7), el fraude informático (art. 8) y la pornografía infantil (art. 9), además de fijar mecanismos de cooperación judicial internacional para la obtención y el intercambio de pruebas digitales. Por su parte, el Reglamento General de Protección de Datos de la Unión Europea (2016), refuerza el vínculo entre privacidad y sanciones efectivas frente al uso indebido de la información personal, estableciendo multas que pueden llegar a los 20 millones de euros o el 4 % de la facturación global anual. El RGPD otorga a los individuos más control sobre sus datos y unifica las normas de protección de datos en toda la UE.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa establece estándares claros orientados a la prevención y represión del cibercrimen, incluyendo la obligación de los Estados de adoptar marcos normativos que promuevan la responsabilidad de las personas jurídicas, la gestión de riesgos tecnológicos, la adopción de medidas de seguridad adecuadas y la cooperación internacional efectiva frente a delitos informáticos complejos. Sin embargo, en el contexto ecuatoriano, la evolución normativa en esta materia ha sido lenta y fragmentada, sin una política criminal digital sistemática que articule de manera coherente la legislación penal, los mecanismos del sistema penal tecnológico y el fortalecimiento de capacidades institucionales especializadas. Esta brecha estructural limita la integración efectiva de estándares internacionales, debilita la cooperación transnacional frente a delitos informáticos y evidencia la ausencia de un modelo moderno de responsabilidad penal y preventiva de las personas jurídicas acorde con la dinámica del riesgo tecnológico contemporáneo (Consejo de Europa, 2001).

El marco jurídico ecuatoriano en materia de ciberdelitos revela deficiencias jurídicas que dificultan la persecución de conductas como el fraude electrónico, el acceso ilícito, ransomware y manipulación de datos, lo que limita la efectividad del COIP frente a la dinámica delictiva digital.

Para Cabezas y Franco (2023), los autores señalan que la normativa carece de mecanismos integrales de ciberseguridad y no se ajusta de alineación con estándares internacionales, lo que debilita la protección de los derechos digitales y la cooperación judicial. En este sentido, la falta de incorporación sistemática de estos estándares internacionales en el ordenamiento jurídico ecuatoriano evidencia la necesidad de repensar el diseño de la política criminal digital, superando enfoques reactivos y fragmentados.

Finalmente, se presencia que la falta de armonización con estándares internacionales, especialmente los previstos en la Convención de Budapest y el RGPD, mantiene al país en una posición de rezago frente a la cooperación judicial y la defensa de los derechos digitales.

Integración entre LOPDP y COIP: hacia una normativa penal complementaria.

La actual disociación entre las sanciones administrativas de la LOPDP y los tipos penales del COIP debilita la respuesta estatal. Se propone:

- Incorporar en el COIP figuras delictivas vinculadas directamente con la vulneración de datos personales, especialmente la comercialización ilícita de datos y el uso indebido de información sensible.
- Modificar la LOPDP para que contemple remisiones expresas al COIP, permitiendo que las infracciones graves en materia de datos personales generen consecuencias penales.
- Crear un régimen de responsabilidad penal de las personas jurídicas en casos de violación masiva de datos, similar al modelo europeo, con sanciones que incluyan multas proporcionales al volumen de facturación, inhabilitaciones y medidas de reparación a las víctimas.

Estrategias para fortalecer la ciberseguridad y la política criminal digital en Ecuador

La eficacia normativa debe complementarse con políticas públicas y medidas institucionales:

- Establecer fiscalías especializadas en ciberdelincuencia, con peritos técnicos en recolección y preservación de pruebas digitales.
- Incorporar protocolos estandarizados para la cadena de custodia de evidencias electrónicas, a fin de garantizar su validez procesal.

- Implementar programas de capacitación continua a jueces, fiscales y policías en materia de ciberdelitos y protección de datos.
- Diseñar una estrategia nacional de ciberseguridad que articule prevención, educación ciudadana y cooperación público-privada.
- Promover la educación digital y el empoderamiento ciudadano como medidas preventivas para reducir la vulnerabilidad frente a ataques informáticos.

Discusión

El análisis de las normativas examinadas evidencia que las principales falencias en materia de ciberdelincuencia no se limitan a la ausencia o insuficiencia de tipos penales específicos, sino que revelan una falta de coherencia y articulación entre los distintos cuerpos normativos llamados a proteger los derechos de las personas frente a los delitos de ciberseguridad. En particular, mientras el Código Orgánico Integral Penal mantiene una estructura rígida y ambigua para abordar conductas digitales complejas, la Ley Orgánica de Protección de Datos Personales introduce obligaciones preventivas y estándares de diligencia que no encuentran un correlato penal claro ni sistemático, generando una protección fragmentada e incompleta tanto para personas naturales como para personas jurídicas.

Esta incongruencia normativa debilita la tutela efectiva de derechos fundamentales como la privacidad, la seguridad de la información y la autodeterminación informativa, pues las infracciones graves derivadas de ataques cibernéticos pueden ser objeto de sanciones administrativas sin que exista una respuesta penal proporcional y coherente frente a conductas especialmente lesivas. A ello se suma la ausencia de un modelo consolidado de responsabilidad y prevención aplicable a las personas jurídicas, lo que impide exigir de manera efectiva deberes de diligencia, gestión de riesgos tecnológicos y control interno frente a amenazas cibernéticas avanzadas.

Desde una perspectiva procesal, la insuficiencia normativa se agrava en el ámbito probatorio. La persecución penal de los delitos de ciberseguridad enfrenta serias limitaciones relacionadas con la obtención, preservación y valoración de la evidencia digital, particularmente en lo relativo a la cadena de custodia digital, la volatilidad de los datos, el almacenamiento de información en

servidores ubicados en el extranjero y la dependencia de mecanismos de cooperación internacional. La falta de protocolos técnicos obligatorios y estandarizados para el manejo de evidencia digital compromete la validez probatoria de los elementos recabados y afecta directamente la eficacia del proceso penal.

En este contexto, la ausencia de una política criminal digital sistemática impide una integración adecuada de estándares internacionales orientados al fortalecimiento de la cooperación transnacional, la especialización institucional y la protección procesal de los derechos de las partes. Ello evidencia que el problema no radica únicamente en la tipificación de nuevas conductas, sino en la carencia de una estructura normativa, procesal y técnica coherente que permita responder de manera efectiva y garantista a los desafíos contemporáneos de la ciberdelincuencia.

En consecuencia, el problema no es únicamente normativo, sino estructural, ya que refleja la ausencia de una política criminal digital coherente que articule prevención, sanción y protección de derechos en el entorno digital.

Conclusiones

La presente investigación ha permitido evidenciar que el marco jurídico ecuatoriano en materia de ciberdelincuencia se caracteriza por una fragmentación normativa estructural entre el Código Orgánico Integral Penal y la Ley Orgánica de Protección de Datos Personales, lo cual debilita la capacidad del Estado para responder de manera eficaz frente a los desafíos del entorno digital. Si bien el COIP incorpora tipos penales orientados a la protección de bien del COIP incorpora tipos penales orientados a la protección de bienes jurídico como la confidencialidad, integridad y disponibilidad de los sistemas informáticos, su regulación resulta parcial, regida y desactualizada frente a la evolución de las nuevas formas de criminalidad tecnológica.

Por su parte, la ley orgánica de protección de datos personales constituye un avance significativo en la garantía del derecho fundamental a la privacidad y a la autodeterminación informativa; sin embargo, su enfoque eminentemente administrativo y preventivo, carente de articulación con el sistema penal, limita su eficacia frente a vulneraciones graves derivadas del uso ilícito de

tecnologías emergentes. Esta desconexión impide una respuesta integral del ordenamiento jurídico, generando espacios de impunidad y debilitando la tutela efectiva de los derechos digitales.

Asimismo, se ha identificado que el sistema penal ecuatoriano presenta vacíos normativos relevantes, especialmente en relación con delitos emergentes como el ransomware, el phishing sofisticado, la suplantación de identidad mediante inteligencia artificial y la manipulación de contenidos digitales mediante tecnología artificial y la manipulación de contenidos digitales mediante tecnología como los deepfakes. La ausencia de tipos penales flexibles y tecnológicamente adaptables, así como la falta de protocolos especializados para la obtención y valoración de la prueba digital, comprometen seriamente la eficacia de la persecución penal en este ámbito.

Desde una perspectiva comparada, se constata que el Ecuador mantiene un rezago frente a estándares internacionales como la Convención de Budapest sobre Ciberdelicuencia y el Reglamento General de Protección de Datos, los cuales promueven modelos integrales que articulan la prevención, la sanción penal, la responsabilidad de las personas jurídicas y la cooperación internacional. La falta de incorporación sistemática de estos estándares limita la capacidad del país para enfrentar fenómenos delictivos de carácter transnacional y tecnológico.

En este contexto, se concluye que la problemática no radica únicamente en la necesidad de incorporar nuevos tipos penales, sino en la urgencia de diseñar una política criminal digital integral, que permita armonizar la protección administrativa de los datos personales, con la persecución penal de los delitos informáticos. Dicha política debe sustentarse en un enfoque multidimensional que incluya la actualización legislativa, la especialización institucional, la adopción de estándares internacionales, el fortalecimiento de la ciberseguridad y la educación digital de la ciudadanía.

En definitiva, la superación de la actual fragmentación normativa exige una reforma estructural del sistema jurídico ecuatoriano, orientada a construir un modelo coherente, dinámico y garantista, capaz de responder de manera efectiva a los desafíos del ciberespacio y de asegurar una protección real y efectiva de los derechos fundamentales en la era digital.

Referencias Bibliográficas

Cabezas Mena, D., & Lucas Franco, G. (2023). *Análisis Comparativo de la Ley Orgánica de Datos Personales del Ecuador con la Legislación española desde un enfoque de ciberseguridad y delitos informáticos.* [Tesis de grado]. Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/handle/123456789/25114

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia (ETS No. 185).* https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Córdova, L. O. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. *Reincisol, 3*(5), 1447-1469. doi:https://doi.org/10.59282/reincisol.V3(5)1447-1469

Cuello, C. (1986). *La Privacidad Individual y el Impacto en ella de la Tecnologia de Computadora*. Ciencia y Sociedad, 9. https://dialnet.unirioja.es/descarga/articulo/7483767.pdf

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

Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Regisro Oficial. https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

Espinosa Carvajal, G., y Paredes Fuentes, F. E. (2025). Los ciberdelitos y la protección de datos personales en el sistema penal ecuatoriano. *Revista de Investigación en Ciencias Jurídicas, 8*(29), 559-572. https://doi.org/10.33996/revistalex.v9i28.302

García Brito, P. J., y Arciniegas Castro , C. (2023). Las nuevas tecnologías frente al Código Orgánico Integral Penal. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 4*(4), 116-127. doi:https://doi.org/10.56712/latam.v4i4.1202

Herrera Llamba, F. A., y Balseca Manzano, J. M. (2025). Ley de Protección de Datos en Ecuador: implicaciones de ciberseguridad. *593 Digital Publisher CEIT, 10*(3), 619-635. doi:https://doi.org/10.33386/593dp.2025.3.2668

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio, 1*(58), 119-123. doi:https://doi.org/10.36097/rsan.v1i58.2667

Pozo Caicedo, L., y Rodriguez Ruiz, M. (2025). Regulación y procesamiento de los ciberdelitos en Ecuador. *593 Digital Publisher CEIT, 10*(1-1), 193-204. doi:doi.org/10.33386/593dp.2025.1-1.3025

Proaño, M. R. (2022). *El alcance de la responsabilidad jurídica ante la violación de la protección de datos personales en Ecuador.* [Tesis de grado]. Universidad Central del Ecuador. http://www.dspace.uce.edu.ec/handle/25000/29070

Sarmiento Chamba, J., y Maldonado Ruiz, L. (2024). Delitos informáticos y ciberataques en Ecuador. *Journal Scientific MQR Investigar, 8*(3), 1753-1781. https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

Solove, D. J. (2008). *Understanding privacy.* Harvard University Press. https://ssrn.com/abstract=1127888

Taco Sánchez, L. M., y Villacis Mogrovejo, F. D. (2025). Delitos Digitales generados mediante inteligencia artificial en Ecuador. *Revista científica Sociedad & Tecnología, 8*(S2), 607-622. https://doi.org/10.51247/st.v8iS2.68

Unión Europea (2016). *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Veloz, T. L., y Veliz Naranjo, V. (2025). *Delitos informáticos: un análisis jurídico integral de las amenazas en el entorno digital.* [Tesis de grado]. Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/handle/123456789/30252

Villavicencio, F. T. (2014). Delitos Informáticos. *IUS ET VERITAS, 24*(49), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

Expreso mi más sincero agradecimiento a Dios, por ser la fortaleza en cada etapa de este proceso académico. A mi familia, por su apoyo incondicional y por comprender las ausencias que implicó esta investigación. A mi tutora Dra. Gina Jacome, por su guía académica, paciencia y valiosos aportes que enriquecieron este trabajo. A la Universidad Bolivariana del Ecuador, en especial al programa de Maestría en Derecho Penal, por brindar el espacio para el debate y la construcción del conocimiento jurídico. Finalmente, a todos quienes con sus ideas, críticas y aliento contribuyeron a la culminación de este artículo.

Nota:

El artículo no es producto de una publicación anterior.