Tesla Revista Científica, ISSN: 2796-9320
Vol. 5 Núm. 1 (2025), e488
https://doi.org/10.55204/trc.v5i1.e488

Área: Derecho, Informática
Artículo de Revisión

Delitos digitales y protección jurídica en Ecuador: una revisión crítica del derecho informático como garante de los derechos digitales.
Digital Crimes and Legal Protection in Ecuador: A Critical Review of Computer Law as a Guarantor of Digital Rights.

Karina Alejandra Haro Tufiño [1][0009-0004-6670-5684], Juan Carlos Santillán-Lima [2][0000-0001-5812-7766], María José Alcívar Quijano [3][0000-0002-7974-017X], Héctor Eduardo Rangel Urdaneta [4][0009-0004-9354-1726]

[1,3,4] Pontificia Universidad Católica del Ecuador. Sede Manabí. Ecuador
[2]Puerto Madero Editorial Académica
[2]Escuela Superior Politécnica de Chimborazo. Facultad de Informática y Electrónica. Riobamba. Ecuador

[1]kaharot@pucesm.edu.ec, [2]carlos.santillan01@espoch.edu.ec, [3]mjalcivarq@pucesm.edu.ec, [4]herangel@pucesm.edu.ec

CITA EN APA:
Haro Tufiño, K. A., Santillán-Lima, J. C., Alcívar Quijano, M. J., & Rangel Urdaneta, H. E. (2025). Delitos digitales y protección jurídica en Ecuador: una revisión crítica del derecho informático como garante de los derechos digitales. *Tesla Revista Científica*, *5*(1). https://doi.org/10.55204/trc.v5i1.e488

Recibido: 2025-03-22
Revisado: 2025-04-01 al 2025-04-21
Corregido: 2025-05-08
Aceptado: 2025-06-12
Publicado: 2025-06-25

TESLA
Revista Científica
ISSN: 2796-9320

Los contenidos de este artículo están bajo una licencia de Creative Commons Attribution 4.0 International (CC BY 4.0)
Los autores conservan los derechos morales y patrimoniales de sus obras.
The contents of this article are under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. The authors retain the moral and patrimonial rights of their works.

Resumen. Este artículo analiza la interacción entre el derecho informático y los sistemas de información en el contexto ecuatoriano, enfatizando su relevancia ante el crecimiento de los delitos digitales. A través de una metodología de revisión documental bibliográfica, basada en literatura científica publicada entre 2010 y 2024 en bases como Scopus, Scielo y PubMed, se identificaron marcos normativos, desafíos institucionales y buenas prácticas en torno a la protección de datos, la criminalidad informática y la ciberseguridad. Los resultados muestran una fuerte convergencia entre el ámbito jurídico y tecnológico en aspectos como la propiedad intelectual digital, el fraude informático y la protección de derechos fundamentales en entornos digitales. Aunque Ecuador ha avanzado en la formulación de leyes y políticas públicas, persisten debilidades estructurales relacionadas con la tipificación legal, la capacitación técnica del personal judicial y la ausencia de una estrategia nacional robusta en ciberseguridad. Se concluye que la consolidación del derecho informático en Ecuador requiere un enfoque integral, dinámico y orientado a la garantía de los derechos digitales como extensión de los derechos humanos.
Palabras Clave: Derecho informático, Ciberseguridad, Delitos digitales, Protección de datos, Legislación ecuatoriana, Derechos digitales.
Abstract: This article analyzes the interaction between computer law and information systems in the Ecuadorian context, emphasizing its relevance in light of the rise of digital crimes. Through a documentary and bibliographic review methodology, based on scientific literature published between 2010 and 2024 in databases such as Scopus, Scielo, and PubMed, regulatory frameworks, institutional challenges, and best practices were identified concerning data protection, cybercrime, and cybersecurity. The results reveal a strong convergence between the legal and technological domains in areas such as digital intellectual property, computer fraud, and the protection of fundamental rights in digital environments. Although Ecuador has made progress in enacting laws and public policies, structural weaknesses persist regarding legal definitions, the technical training of judicial personnel, and the absence of a robust national cybersecurity strategy. It is concluded that the consolidation of computer law in Ecuador requires a comprehensive, dynamic approach focused on guaranteeing digital rights as an extension of human rights.
Keywords: Computer law, Cybersecurity, Digital crimes, Data protection, Ecuadorian legislation, Digital rights.

Introducción

La informática en relación con la sociedad requiere de un sin número de técnicas para tratar la información que se recepta y poder diferenciarlas de cada una de ellas de tal forma que la información que proporciona cada una de las personas en sitios tecnológicos como en aplicaciones móviles son tratados

según se allá creado para su determinada finalidad en cuanto a la relación que posee esta con la sociedad, toda información que tratamos e interactuamos en la informática como tal se regirá mediante técnicas y estrategias para que sea tratada según su contenido.

Según Adrián, (2019) "La informática es una ciencia de la computación que se encarga del tratamiento y estudio racional, de la información. Es decir, esta ciencia se encarga de distinguir a un conjunto de conocimientos prácticos y teóricos relacionados con la ciencia y la tecnología que, al relacionarse, hacen posible el tratamiento automático y racional de la información a través de computadoras."

En ese mismo orden de ideas, la informática desempeña funciones esenciales para la sociedad, especialmente en lo relativo a sus avances tecnológicos, considerando las diversas formas en que puede operar y ser gestionada. Esto implica un uso constante de la información y su tratamiento mediante herramientas informáticas, lo cual genera preocupación en torno a su regulación legal. En consecuencia, el uso de la informática a través de computadoras o dispositivos móviles se encuentra sujeto a normativas jurídicas que buscan garantizar su adecuado funcionamiento y el cumplimiento de los fines para los cuales fueron diseñados los programas y aplicaciones móviles.

En coherencia con lo anterior, el uso de la informática en la sociedad resulta de vital importancia, ya que constituye una herramienta que optimiza el tiempo en la realización de actividades cotidianas, tanto en dispositivos móviles como en ordenadores. Sin embargo, este uso está condicionado por el vertiginoso avance tecnológico, que plantea nuevos desafíos para el derecho informático. En este sentido, se vuelve imprescindible la regulación del uso de la información mediante la creación de normas, jurisprudencia, políticas públicas y otras herramientas jurídicas que permitan su control y utilización responsable, conforme a lo establecido por el Estado ecuatoriano (Andrade Arias, 2024).

El avance tecnológico presentado a finales del siglo XX ha desarrollado el uso de aplicaciones móviles en la sociedad en la cual cumple con diferentes funciones dependiendo para la cual fue creada surgen las primeras aplicaciones de los dispositivos móviles, desde sus inicios han sido mejorados y creados para cumplir con las necesidades que hoy atraviesa la sociedad, tomando relevancia el derecho informático como fuente de regulación legal.

(Valdés, 2008) manifiesta que la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho. Surgida propiamente en 1959 en Estados Unidos, esta disciplina ha experimentado transformaciones acordes con la evolución general de la informática.

Como se planteó en el párrafo anterior, el rápido progreso de las tecnologías de la información ha colocado al derecho informático (DI) y a los sistemas de información en el centro de la revolución digital. La digitalización y la convergencia tecnológica están transformando profundamente la sociedad, lo que hace que la intersección entre tecnología y derecho sea más relevante que nunca. Este fenómeno se explica

por las interacciones cotidianas y la completa digitalización e integración de nuevas tecnologías, lo cual marca un hito significativo en la manera en que se gestiona la información y los datos(Perasso, 2016)

Según (Iracelay, 2019)en la Revista Iberoamericana de Derecho Informático manifiesta que en este escenario, el derecho informático emerge como un campo fascinante y desafiante. Esta fusión de la tecnología y el derecho plantea desafíos legales y éticos constantes, exigiendo la participación activa de juristas o informáticos para entender la regulación de las tecnologías emergentes.

La literatura señala que la Informática Jurídica (IJ) es una disciplina que aborda la convergencia entre el derecho y la informática con el propósito de mejorar la eficiencia y accesibilidad de los procesos legales mediante el uso de herramientas informáticas. Comprende diversas áreas, como la informática documental, que facilita la gestión y búsqueda de documentos legales, y la informática de gestión, que se enfoca en administrar despachos legales y departamentos jurídicos. Busca aplicar la informática en la recuperación y análisis de información legal para la toma de decisiones jurídicas (Farías et al., 2023; Gutierrez Albarracin & Tibiriça, 2017; Moia, 2022)

En el Ecuador, el DI trasciende su función ejecutiva para proporcionar instrucción jurídica-tecnológica. Este estudio se centra en la relación entre el derecho informático y los sistemas de información en Ecuador. En este sentido se puede afirmar que los derechos digitales son una extensión de los derechos humanos tradicionales que se adaptan al entorno digital. En la generalidad se busca proteger las distintas libertades, la privacidad y la igualdad de las personas en el entorno virtual (Ius Novum, s.f.)..

La investigación sobre Derecho informático: marco legal en Ecuador, se ha motivado a conocer algunos aspectos que deben ser considerados para enfrentar los desafíos acaecidos en la apuesta por la ciencia con vista a la construcción de una cultura científica y tecnológica

En ese sentido el objetivo de esta revisión es caracterizar Derecho informático: marco legal en ecuador mediante una revisión de la literatura científica, para lo cual se han establecido dos objetivos específicos. El primero trata de conocer derecho informático. En segundo lugar, se pretende identificar en el marco legal con vista construcción de una cultura científica y tecnológica y de Derechos Humanos.

Material y Métodos

El artículo se realizó bajo una metodología de tipo documental bibliográfica, bajo la modalidad de revisión de textos científicos, entre artículos, publicaciones profesionales y tesis entre otros publicados en los últimos 5 años en las diferentes fuentes académicas como Pubmed, Scielo, Scopus entre otros que permitieron la recolección de la información bibliográfica, dándose a conocer las diferentes opiniones de los autores sobre Derecho informático: marco legal en ecuador que usaron para la investigación y dentro de la hermenéutica se explicó las diferencias y semejanzas de diferentes autores con rasgos similares en sus temas de estudio.

Técnicas empleadas

La búsqueda y localización de las literaturas fue exhaustiva, y de nivel profesional, por la amplia indagación que tenía similitud al tema de revisión, una vez localizada las publicaciones se analizó cada una de las partes, y los temas con mayor impacto se clasificaron para realizar una evaluación directa y más profunda a cada publicación, para luego extraer la información más relevante y realizar las comparaciones pertinentes.

Criterios de exclusión: No se tomaron en cuenta publicaciones opuestas al contenido del presente estudio o carentes de lógica. El presente artículo no debate conceptos, los analiza para alcanzar los objetivos propuestos, se excluyeron además publicaciones carentes de fundamentación científica y bases de datos referenciadas que se hayan obtenido por productos no investigativos.

Criterios de inclusión: Se tomaron en cuenta trabajos que contenían palabras referentes al título del presente trabajo de revisión, publicaciones que además de coincidir con los términos de investigación se encuentren en la línea de tiempo establecida. En la búsqueda de información se consideraron los términos, restringiendo la búsqueda según los resultados esperados y resultados previos en libros, revistas digitales y documentos en formato PDF. En la tabla 1 se pueden observar con mayor detalle los aspectos considerados para la selección de artículos utilizada en la presente investigación.

Tabla 1. Metodología de la Investigación

Elemento	Desarrollo
Tipo de estudio	Revisión documental bibliográfica bajo la modalidad de revisión de textos científicos.
Idioma	Español
Periodo	2010-2024
Fuentes revisadas	Revisión exhaustiva de artículos, tesis, publicaciones profesionales y científicas que tengan relación con el tema.
Términos	Derecho informático, sistemas informáticos, legislación, delito informático.
Registro	Análisis de la información revisada y búsqueda de resultados disponibles.
Recursos	Google Académico, Scielo, Scopus, PubMed, tesis de maestría y doctorado, libros.
Técnicas de recolección	Recolección de información mediante análisis documental y herramientas académicas.
Técnicas de análisis	Análisis hermenéutico-comparativo entre autores para identificar similitudes y diferencias conceptuales.
Criterios de inclusión	Trabajos que contengan términos del título y estén dentro del periodo 2010-2024, con base científica verificable.
Criterios de exclusión	Publicaciones sin respaldo científico, sin lógica argumentativa o contrarias al enfoque del estudio.

Elaborado por: El Autor

RESULTADOS

A continuación, se presenta un análisis previo cita de los documentos de carácter institucional y teóricos básicos a nivel nacional relacionados el Derecho informático: marco legal en Ecuador.

Para esquematizar los resultados, se plantea responder a las siguientes preguntas:

¿Qué tipos de investigación se han desarrollado en el tema planteado? y ¿Cuál es el marco legal del derecho informático en Ecuador?

Sobre la primera pregunta, en la tabla 2 se observa el tipo de estudio de cada investigación a las que se realizó la revisión bibliográfica, en el cual se demuestra que 3 estudios fueron de metodología cualitativa, 3 mixto y 6 artículos de revisión bibliográfica, danto un total de 30 estudios revisados.

Tabla 2. Tipo del Estudio

Tipo de estudio	Número de estudios
Cualitativo	3
Revisión Bibliográfica	6
Mixto	3
Total	12

Elaborado por: El Autor

En la tabla 3 se observan los estudios relacionados con el tema y revisados, sus autores, el tipo de metodología empleada y la población muestra a la cual se le efectuó la investigación

Tabla 3:

Tipo de estudios relacionados

Investigación	**Autores y año**	**Tipo de estudio**	**Resultados**
Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador.	Andrade Arias, F. J. (2024).	Revisión bibliográfica	Los resultados de esta investigación demuestran que los propietarios de los datos desconocen por completo el tratamiento inadecuado por parte de terceros y administradores a la hora de adquirir datos sensibles y su uso indebido en la sociedad actual. Se determina que no existen sanciones leves por el mal uso de los datos y su tratamiento inequívoco, que se estima existen en los parámetros de seguridad de las aplicaciones mencionadas
Implementación de sistemas de facturación electrónica en el marco del derecho informático: Desafíos y oportunidades para el desarrollo de sitios web en Ecuador.	Farías, J. J. C., Romero, V. J. S., Lumbano, C. A. S., & Millingalle, J. V. C. (2023).	Cualitativo	Los resultados obtenidos permiten que la implementación de la facturación electrónica es un proceso complejo que debe ser abordado de manera integral, considerando tanto los aspectos legales como los tecnológicos. La colaboración entre expertos en ambas áreas es fundamental para garantizar el éxito de la implementación de la facturación electrónica en empresas de Ecuador.
Marco civil de internet en Brasil y referentes en la región Américas.	Gutiérrez Albarracín, C. A., & Tibiriça, B	Cualitativo	Los resultados demuestran que el desarrollo del marco civil de internet (MCI) en Brasil - único país del continente americano con una constitución política de internet-; así como las políticas que, al respecto, se han implementado en la Región Américas
Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio.	Gómez Agudelo, D. S., Acevedo Valencia, J. M., & Aguirre Espinosa, J. E. (2021).	Mixto	En los resultados se evidencia que la facilidad para modificar mensajes de Whatsapp, aun sin los mayores conocimientos técnicos, por medio de aplicaciones gratuitas, genera la necesidad de revisar la autenticidad de los mensajes, para evitar desconocer el principio del debido proceso
Casos frecuentes, penalización y prevención de los delitos	Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q.,	Cualitativo	Los resultados, se generaron respuestas a las preguntas específicas de investigación (PIs1, PIs2, PIs3, PIs4 y PIs5), teniendo éxito en la

informáticos en el Ecuador: una breve revisión sistemática	Loor, J. J. M., Estupiñan-Troya, G., & Vizuete, J. D. R. (2022).		revisión sistemática. En conclusión, se sugiere al gobierno e instituciones públicas y privadas promover capacitaciones donde se socialicen los riesgos y tipos de delitos informáticos, normatividad que regule estos actos delictivos en relación con la tecnología y asesoría para protegerse y estar a la vanguardia de los ciberdelincuentes.
Reconciling remote sensing technologies with personal data and privacy protection in the European Union: Recent developments in Greek legislation and application perspectives in environmental law.	Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Maria, E. A. (2021).	Mixto	Como resultado del l estudio se presentan, a modo de oportuno «estudio de caso», la evolución reciente de la legislación griega y sus perspectivas de aplicación en el Derecho medioambiental.
Blockchain for Credibility in Educational Development: Key Technology, Application Potential, and Performance Evaluation.	Wang, Y., Cong, X., Zi, L., & Xiang, Q. (2023).	Revisión Bibliográfica	Analizamos los retos y las tendencias de investigación de la cadena de bloques en la credibilidad educativa y proporcionamos ideas útiles para futuras investigaciones.
Panorama del derecho informático en América Latina y el Caribe	Gamba, J. (2010).	Revisión Bibliográfica	Se hace una revisión y análisis de la literatura, se abordarán las principales y más relevantes temáticas en materia de Derecho Electrónico, que son: firmas y comercio electrónico, gobierno electrónico y transparencia, delitos informáticos y finalmente la e-justicia o aplicación de las TIC a los sistemas judiciales.
El delito de hacking	Almenar Pineda, F. (2017	Mixto	Los resultados constituyen un análisis de la necesaria reforma operada por la LO 5/2010 en el artículo 197 del Código Penal español, en concreto en su apartado 3, donde se han introducido las conductas de acceso ilícito a sistemas informáticos o hacking, y que tras la entrada en vigor de la LO 1/2015 se han ubicado en su artículo 197 bis 1
Análisis conceptual del delito informático en Ecuador.	Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021).	Referencias Bibliográfica	Los resultados obtenidos evidencian, destacan las normativas y tipificidades plasmadas en la Constitución de la República del Ecuador en cuanto al derecho y protección del delito informática.
Delito Informático. Procedimiento Penal en Ecuador	Zambrano, K. I. D., & Ordoñez, L. M. M. (2016).	Revisión bibliográfica	Se hace una revisión y análisis de la literatura destaca las normativas y tipificidades plasmadas en la Constitución de la República del Ecuador en cuanto al derecho y protección del delito informático.
El Marco Legal de los Delitos Cibernéticos en Ecuador.	Córdova, L. A. O. (2024).	Revision bibliográficas	La implementación efectiva de estas disposiciones requiere una capacitación adecuada de las fuerzas del orden y del sistema judicial. En 2021, se promulgó la Ley de Protección de Datos Personales que establece un

			marco legal integral para la protección de los datos personales.

La revisión bibliográfica de estos artículos, publicaciones permitieron encaminar la investigación cumpliendo con los objetivos estipulados y dando a conocer todo lo relacionado con derecho informático en el marco de Ecuador entre otros aspectos significativo que son de utilidad para el lector de la comunidad científica.

Discusión

La relación entre los sistemas informáticos (SI) y la legislación es esencial en la era moderna, donde la tecnología informática juega un papel fundamental en todas las esferas de la vida. Los SI desempeñan un rol crucial en la producción y distribución de contenido digital, como software, música, películas y libros electrónicos. Gestionar legalmente estos proyectos según las legislaciones y regímenes jurídicos de cada Estado es crucial para evitar consecuencias legales e integridad en su desarrollo. La regulación de la protección de datos personales propuesta por Becerril y Ortigoza fortalece la legislación y transforma el DI Las implicaciones legales en SI se centran en la seguridad de la información, la protección de datos y el acceso a la información pública. Prevenir y erradicar malas prácticas en la administración con el uso de tecnología es fundamental para garantizar este derecho esencial y evitar problemas legales(Gómez Agudelo et al., 2021; Macías-Lara et al., 2022)

Diversos organismos como CEPAL han advertido que en América Latina se ha optado por reformar los códigos penales para incorporar delitos informáticos en lugar de desarrollar leyes específicas y actualizadas. Esta práctica ha generado inseguridad jurídica y mayor riesgo de impunidad en la persecución penal de estos delitos (Gamba, 2010).

En Ecuador, la legislación establece normativas para proteger la privacidad y seguridad de los datos, como el Reglamento General de Protección de Datos, y aborda la seguridad de los SI y la protección contra amenazas cibernéticas. Esto se refleja en leyes que sancionan el acceso no autorizado a sistemas informáticos, la difusión de malware y la realización de ataques informáticos también, la legislación de propiedad intelectual salvaguarda los derechos de los creadores y establece directrices para el uso legítimo de dicho contenido; además, regula las transacciones comerciales llevadas a cabo a través de estos sistemas, como compras, contratos electrónicos y servicios financieros en línea, asegurando la validez legal de estas y protegiendo a los consumidores asimismo, existen leyes que definen y sancionan delitos informáticos, como fraude, robo de identidad, ciber acoso y piratería informática (Maniadaki et al., 2021)

Yang et al., (2023) en su estudio declara que al DI se le atribuyen diversos términos como Derecho Telemático o Derecho del Ciberespacio. En definitiva, su objetivo es establecer normativas que regulen la creación, desarrollo y uso de la informática, así como los problemas legales asociados. Es así que, otras leyes recientes, como la Ley de comercio electrónico, mensajes de datos y firmas electrónicas junto con las reformas al Código Orgánico Integral Penal que abordan los delitos Informáticos, han introducido nuevas

herramientas legales, por lo que es crucial que los futuros abogados las conozcan y estudien para utilizarlas adecuadamente (Wang et al., 2023)

Es importante destacar que la materia informática y derecho presentan dos tipos de relaciones:

- ✓ Si se toma como enfoque el aspecto meramente instrumental, se está haciendo referencia a la informática jurídica, que es la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el Derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del Derecho. En otras palabras, se trata de analizar el aspecto instrumental que surge de la aplicación de la informática en el Derecho.
- ✓ Por otro lado, si se considera a la informática como objeto del Derecho, o sea como conjunto de procedimientos que la ley tiene que regular, se hace alusión al Derecho de la Informática o simplemente Derecho Informático. En este caso se habla entonces del conjunto de normas, aplicaciones, procesos y relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática en diversos aspectos de las relaciones inherentes a las actividades realizadas por los distintos agentes que conforman la sociedad.(Gamba, 2010)

Delito informático en Ecuador

El vertiginoso desarrollo tecnológico, la interdependencia económica, la desmedida informatización de la sociedad y el omnímodo poder de la Informática, han demandado de la moderna Ciencia Penal, la comprensión de las conductas criminales en las que se ve inmersa la informática. El incremento de la ciberdelincuencia tiene su fundamentación en varios factores: por una parte, el aumento de tecnología disponible, tanto para el delincuente como las víctimas, y por otra el crecimiento sostenido del mercado negro de la información

En todo el mundo el ciber delito, al igual que otras figuras penales, ha sido objeto de análisis por parte de juristas y expertos en seguridad informática; lo que permitió que muchas legislaciones del continente americano tipifiquen conductas ciber delincuentes, tomando en consideración lo que se ha analizado doctrinalmente y tipificado en otros continentes(Almenar Pineda, 2017)

Las actividades informáticas delictivas están en crecimiento a nivel global, en América Latina, con una proyección cada vez mayor. En el Ecuador en el año 2009 se empieza a hablar de delitos informáticos registrándose hasta el 2013 un total de 3,143 casos, esto a pesar de que se conoce que el 80% de los delitos informáticos no son reportados, en cuanto al índice delictivo. Ecuador ocupa el tercer lugar después de México con el 92 % y Bolivia con el 85 %, lo que a criterio de la ONU se produce como consecuencia de la falta de una cultura de denuncia Según una publicación de fecha 30 de enero del 2015 del diario El Comercio (2015), Ecuador ocupa el octavo lugar entre los países de la región que más ataques informáticos registró en el 2014. Brasil y Perú lideran la lista con un 32% y 28% respectivamente.(Saltos Salgado et al., 2021)

Se consideran dos conceptualizaciones de Delito Informático:

- ✓ El concepto típico, corresponde a aquellos delitos informáticos que comprenden conductas típicas, antijurídicas y culpables, mediante las que se hace uso de las computadoras como instrumento o fin.
- ✓ El concepto atípico define a los delitos informáticos, como las actitudes ilícitas en donde se usa a las computadoras como medios o fin para delinquir.

El Tratado sobre Delito Informático se le define como un instrumento de carácter internacional que abarca los delitos cometidos mediante el uso del Internet y las redes informáticas, comprende los siguientes delitos:

- Violación por derechos de autor.
- Fraude informático.
- Pornografía infantil.
- Delitos de odio.
- Violaciones de seguridad de red.
- Incautación de datos informáticos.
- Inadecuado uso de dispositivos.
- Delitos relacionados con derechos conexos.
- Interferencia de sistemas.

Internacionalmente existen diferentes designaciones para la terminología delitos informáticos, tales como, delitos electrónicos, ciber crimen, ciber delitos, delitos relacionados con las computadoras, crímenes por computadora, entre otros. El término más usado por los autores en la doctrina del derecho penal informático es el de delito informático. Como se señala, es indispensable el uso de la computadora y del manejo del Internet, para la comisión de estas conductas delictivas.

En forma general, las principales características que revisten los Delitos informáticos son:

- Conductas criminógenas de cuello blanco.
- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

El Código Orgánico Integral Penal ecuatoriano ha transitado por diversas etapas donde le han realizado varias modificaciones parciales. Uno de esos cambios fue en materia de Delitos Informáticos, donde se adaptaron las figuras penales clásicas a fin de que sea posible su aplicación en los diferentes tipos de violaciones. Un gran avance fue La Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, promulgada en 1999, la que representó un gran avance en la búsqueda de un sistema jurídico que nos asegure confianza a los usuarios de la tecnología. En el 2002 se introdujo a esta ley cambios interesantes en el incompleto panorama de los delitos informáticos.

En esta misma línea de interpretación en Ecuador, específicamente la Ley No 67 (Asamblea Nacional .República del Ecuador, 2021) regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado “De las infracciones informáticas”, los artículos del 57 al 64 sancionan los siguientes delitos informáticos: 1) la violación al derecho a la intimidad en documentos con soporte electrónico (Art 58 y 64); 2) la violación o divulgación de información secreta contenida en documentos con soporte electrónico (Art. 58); 3) La obtención y utilización no autorizada de información (Art. 58); 4) la destrucción o supresión de documentos con soporte electrónico por parte de personas que tuvieren su resguardo a cargo (Art. 59); 5) la falsificación electrónica (Art. 60); 6)- los daños informáticos (Art. 61), 7) la apropiación ilícita (Art. 62) y, 8) la estafa utilizando medios electrónicos o telemáticos (Art. 63). Por otra parte, los delitos informáticos también están tipificados en el marco jurídico legal del Ecuador, en el Código Orgánico Integral Penal (COIP) del 2014.

No se puede sancionar un delito si éste no está debidamente tipificado en el marco legal; es decir, que toda conducta que atente contra la armonía y la tranquilidad del conglomerado social debe estar normalizada, ya que no es posible su sanción a través de analogías. Por esta razón, se precisa la creación de tipos penales sancionatorios de los nuevos delitos ilícitos producto del avance tecnológico como los que se desarrollan a través del internet estos son el ciberbulling, ciber ataques, subastas y ventas ilegales en internet, uso de redes robot o zombi, etc

En ese mismo orden de ideas la tipificación del delito informático en la ley penal responde a elementos tales como el sujeto o autor de la conducta ilícita o delictiva; el medio, el sistema informático; y el objeto, el bien que produce el beneficio económico o ilícito (Zambrano-Mendieta et al., 2016)

En el Ecuador en respuesta a la evolución de las amenazas cibernéticas, ha habido un esfuerzo continuo para actualizar y mejorar el marco legal ecuatoriano. Modificaciones recientes al COIP y nuevas propuestas legislativas reflejan un reconocimiento de la necesidad de mantener las leyes al día con las tecnologías emergentes. Entre estas propuestas se incluye la creación de una Agencia Nacional de

Ciberseguridad, que coordinaría los esfuerzos a nivel nacional. La participación en acuerdos y foros internacionales ha permitido a Ecuador acceder a recursos y capacitación, facilitando la cooperación en la investigación de delitos cibernéticos.(Córdova, 2024)

Las estrategias nacionales de ciberseguridad en Ecuador son fundamentales para articular una respuesta coordinada y efectiva a los desafíos del cibercrimen. Estas estrategias incluyen políticas para la protección de infraestructuras críticas, programas de concienciación y educación, y el desarrollo de capacidades técnicas en ciberseguridad. La evaluación constante de estas estrategias y la participación del sector privado son esenciales para su efectividad.(Campos, 2019)

A pesar de los avances, persisten lagunas legislativas que requieren atención, como:

- La necesidad de una ley específica que abarque todos los aspectos del cibercrimen.
- La rápida evolución tecnológica también plantea desafíos para la legislación y la aplicación de la ley.
- La adopción de nuevas tecnologías por parte de las fuerzas del orden es crucial para mejorar la capacidad de detección y persecución de delitos cibernéticos.
- La protección de datos personales es otro componente crítico de la ciberseguridad que necesita fortalecimiento continuo.
- La educación y concienciación pública son fundamentales para la prevención de delitos cibernéticos y la protección de los usuarios en el entorno digital.(Córdova, 2024)

Los retos para combatir el delito informático del Ecuador están intrínsecos a los establecidos por las Naciones Unidas lo que convierte al cibercrimen en un mal que aqueja a gran parte de la humanidad. Es importante que los países puedan aunar esfuerzos y superar estos retos para lograr disminuir las grandes pérdidas económicas, proteger a las personas, estados y empresas de los cibercriminales(Campos, 2019)

A nivel regional, Ecuador aún se encuentra en una fase formativa en el desarrollo de sus estrategias nacionales de ciberseguridad, lo que refleja un retraso respecto a países que ya cuentan con políticas consolidadas y mecanismos de respuesta coordinada, como Colombia, Uruguay o México. Esta brecha compromete la capacidad de defensa y resiliencia digital del país, según lo evidencian los informes del BID y la OEA (Aguilar Antonio, 2020).

A modo resumen se plantea, que en el caso del análisis jurídico tanto en el ámbito nacional como internacional para la temática del delito informático ha ocurrido una evolución histórica.

Se exponen algunos vínculos de la Ciberseguridad con la Planificación en el Ecuador.

- **Plan Específico de Seguridad Pública y Ciudadana 2019-2030**

Se establecen políticas articuladas y coordinadas de prevención y control respecto de las distintas expresiones del delito y en sus diferentes ámbitos, lo que lleva a prevenir, anticipar y combatir amenazas locales, nacionales e internacionales. La división entre seguridad pública y seguridad ciudadana permite un marco de acción diferenciado sobre la suscitación de delitos, por un lado, una competencia Estatal encaminada al resguardo del orden público y la protección interna, por otro lado, una seguridad ciudadana

enfocada en las acciones institucionales dedicadas a reducir los factores de vulnerabilidad hacia el cometimiento de delitos

- **Plan Específico de Inteligencia 2019 2030**

Este plan entiende como amenaza para el Estado ecuatoriano a todo fenómeno o condición en la que uno o más actores con capacidad y fines específicos generen un daño, pérdida o consecuencia negativa directa contra los ejes de protección de la seguridad integral del Estado, entendiendo a estos como ser humano, Estado y naturaleza. En este contexto, se establece como una de las amenazas para el Ecuador las acciones contra el Estado en el ciberespacio.

- **Política Ecuador Digital**

Instrumento cuyo objetivo es transformar y dirigir al país, hacia una economía basada en tecnologías digitales mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública, y la adopción digital en los sectores sociales y económicos, esta política se compone de 3 ejes: Ecuador Conectado, Ecuador Eficiente y Ciberseguro.

Ecuador Innovador y Competitivo. Cada uno incluye un conjunto de proyectos para incrementar los índices de accesibilidad a las tecnologías de la información y comunicación, el fortalecimiento de las capacidades de talento humano, la potenciación de los sectores de la economía y el impulso del emprendimiento e innovación; es así que el eje de acción Ecuador Eficiente y Ciberseguro garantiza la participación ciudadana, la democratización de los servicios públicos, la simplificación de trámites, la gestión de la seguridad de la información y la protección de datos personales.(Acuerdo-No.-006-2021-Politica-de-Ciberseguridad., 2021)

La implementación efectiva del marco legal ecuatoriano también depende de la capacitación técnica del personal judicial. CEPAL (2010) destaca que la ausencia de formación específica en ciberdelitos y análisis forense en fiscales, jueces y policías limita la correcta aplicación de la normativa vigente.

Las experiencias exitosas de Brasil, con el Marco Civil de Internet, y Colombia, con su Agenda de Conectividad, ofrecen ejemplos de cómo integrar la normativa digital con políticas públicas inclusivas. Ambos países han desarrollado marcos jurídicos que articulan protección de derechos, innovación tecnológica y fortalecimiento institucional (Gutierrez Albarracín & Tibiriça, 2017; CEPAL, 2010).

De la literatura revisada resultaron interesantes las siguientes publicaciones:

En el análisis conceptual del delito informático en Ecuador de los profesores (Saltos Salgado et al., 2021) pretende ofrecer una herramienta para comprender de mejor forma la problemática del delito informático desde del punto vista conceptual y jurídico, encontrando así evidencia empírica que existen factores como el avance propio de la tecnología de la información que conllevan al aumento de los delitos informáticos, y por tanto es de vital importancia un mejor análisis jurídico de su tipificación.

En el análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en ecuador de Andrade Arias, (2024) se evidencio que los titulares de su información desconocen por completo el tratamiento indebido que genera terceras personas y administradores ante la adquisición de

datos sensibles y su mala utilización en la sociedad actual determinado que no existen sanciones leves ante el mal uso de los datos y su tratamiento inequívoco sé que estima existen en los parámetros de seguridad de las aplicaciones mencionadas, la divulgación de esta información de carácter personal el adquirir dichos datos sensibles genera en terceras personas atracciones positivas como negativas para el tratamiento al que destine la persona que accedió a la información.

El derecho informático y la influencia en los sistemas de información: un análisis bibliográfico bajo la perspectiva jurídica y tecnológica en Ecuador de Moreira et al., (2024) buscan analizar la perspectiva jurídica y tecnológica del derecho informático y su influencia en los sistemas de información en el contexto ecuatoriano. Se señala la conexión significativa entre el derecho informático y los sistemas de información, destacando temas comunes como delitos informáticos, protección de datos y propiedad intelectual. Se identificaron vínculos respaldados por la legislación ecuatoriana en áreas como la protección de software y el comercio electrónico; sin embargo, se subraya la necesidad de una implementación efectiva de las leyes y una cooperación internacional más amplia para abordar desafíos como la delincuencia informática. El estudio puso de manifiesto las disparidades y conexiones entre el derecho informático y los sistemas de información en Ecuador. Se resalta la necesidad de adoptar un enfoque interdisciplinario para futuras investigaciones.

CONCLUSIONES

La interrelación entre el derecho informático y los sistemas de información se manifiesta en la convergencia de temáticas críticas como los delitos informáticos, la protección de datos personales, el fraude digital y la propiedad intelectual. Esta convergencia evidencia la necesidad de una colaboración interdisciplinaria entre el ámbito jurídico y el tecnológico, a fin de fortalecer los marcos normativos, garantizar la privacidad de los usuarios, y asegurar el cumplimiento legal en el entorno digital.

En el contexto ecuatoriano, si bien se han registrado avances en la regulación de los delitos cibernéticos, persisten desafíos estructurales que demandan un enfoque integral y proactivo. Este debe incluir la formación continua de operadores judiciales, el fortalecimiento de las capacidades institucionales, la cooperación internacional en materia de ciberseguridad y una actualización legislativa permanente, acorde con la evolución tecnológica y las nuevas formas de criminalidad digital

Los delitos informáticos constituyen una amenaza creciente a los derechos humanos fundamentales, como la privacidad, la libertad de expresión, el acceso a la información y la dignidad personal. En el entorno digital, el uso indebido de datos personales, la suplantación de identidad, el ciberacoso y otras formas de violencia digital pueden vulnerar gravemente estos derechos, en muchos casos sin una respuesta legal eficaz. En este sentido, el derecho informático no solo debe responder a los desafíos tecnológicos, sino también garantizar la protección de los derechos humanos en el ciberespacio. Los derechos digitales deben entenderse como una extensión de los derechos humanos tradicionales, adaptados a la realidad virtual, lo cual exige una regulación legal dinámica, educativa y basada en principios éticos.

Referencias Bibliográfica

Acuerdo-No.-006-2021-Politica-de-Ciberseguridad. (2021). Ministerio de Telecomunicaciones y de La

Sociedad de La Información (MINTEL).

Andrade Arias, F. J. (2024). Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador.

Aguilar Antonio, J. M. (2020). *La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas*. Revista de Estudios en Seguridad Internacional, 6(2), 17–43. https://doi.org/10.18847/1.12.2

Adrián, Y. (2019). *Concepto de Informatica*. Concepto Definicion. https://conceptodefinicion.de/informatica

Almenar Pineda, F. (2017). *El delito de hacking.*

Andrade Arias, F. J. (2024). *Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador.* (Tesis de Grado).Universidad Catolica de Cuenca.

Asamblea Nacional .República del Ecuador. (2021). *Ley de comercio electronico, firmas y mensajes de datos*.

Campos, N. J. O. (2019). Normativa legal sobre delitos informáticos en Ecuador. 21. *Revista Científica Hallazgos*, *4*(1), 100–111.

Córdova, L. A. O. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. *Reincisol*, *3*(5), 1447–1469.

Farías, J. J. C., Romero, V. J. S., Lumbano, C. A. S., & Millingalle, J. V. C. (2023). Implementación de sistemas de facturación electrónica en el marco del derecho informático: Desafíos y oportunidades para el desarrollo de sitios web en Ecuador. *Revista Científica FIPCAEC (Fomento de La Investigación y Publicación Científico-Técnica Multidisciplinaria).*

Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe. *CEPAL.Organización de Naciones Unidas, ONU- Comisión Económica Para América Latina.*

Gómez Agudelo, D. S., Acevedo Valencia, J. M., & Aguirre Espinosa, J. E. (2021). Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio. *Revista Chilena de Derecho y Tecnología*, *10*(2), 123–148.

Gutierrez Albarracin, C. A., & Tibiriça, B. (2017). Marco civil de internet en Brasil y referentes en la región Americas. *Revista VISIÓN ELECTRÓNICA: Algo Más Que Un Estado*.

Iracelay, J. (2019). Prólogo revista Fiadi segunda época. *Revista Iberoamericana de Derecho Informático (Segunda Época), 7*(7), 9–11.

Ius Novum. (s.f.). *La interacción de los derechos digitales y los derechos humanos*. https://iurenovum.com/la-interaccion-de-los-derechos-digitales-y-los-derechos-humanos

Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q., Loor J. J, M., & Estupiñan-Troya, G Vizuete, J. D. R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 231–243.

Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Maria, E. A. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the European Union: Recent developments in Greek legislation and application perspectives in environmental law. *Laws*, *10*(2), 33.

Moia, A. L. (2022). El salvataje en el concurso preventivo de las empresas de interés cultural. Una relectura de las normas y su aplicación. *Papeles. Revista Del Centro de Investigaciones de La Facultad de Ciencias Jurídicas y Sociales de La Universidad Nacional Del Litoral*, *13*(24), 17.

Moreira, I. A. M., Mendoza, M. N., & Parraga-Alava, J. (2024). El derecho informático y la influencia en los sistemas de información: un análisis bibliográfico bajo la perspectiva jurídica y tecnológica en Ecuador. *Revista Tecnológica-Espol*, *36*(1), 162–17.

Perasso, V. (2016). *Qué es la cuarta revolución industrial (y por qué debería preocuparnos).* BBC. https://www.bbc.com/mundo/noticias-37631834

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343–351.

Saltos Salgado, Marco Fernando, Robalino Villafuerte, José Luis, & Pazmiño Salazar, Lenin Darío. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343-351. Epub 02 de febrero de 2021. Recuperado en 12 de mayo de 2025, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343&lng=es&tlng=es.

Valdés, J. T. (2008). *Derecho informatico* (Cuarta edi). McGraw-Hill/Interamericana Editores, S.A.

Wang, Y., Cong, X., Zi, L., & Xiang, Q. (2023). Blockchain for Credibility in Educational Development: Key Technology, Application Potential, and Performance Evaluation. *Security and Communication Networks*, *1*.

Zambrano-Mendieta, J. E., Dueñas-Zambrano, K. I., & Macías-Ordoñez, L. M. (2016). Delito. Procedimiento Penal en Ecuador. *Revista Cientifica Dominio de Las Ciencias*, *2*, 204–215. http://dominiodelasciencias.com/ojs/index.php/es/index