Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nº. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

La responsabilidad penal derivada de los delitos de apropiación ilícita a través de medios electrónicos

Criminal liability arising from the offenses of unlawful appropriation through electronic media

Jonathan Estanislao Freire Altamirano[1] (jfreirea5@unemi.edu.ec) (https://orcid.org/ 0009-0004-9097-9765)

Marylin Viviana Villalobos Cisneros[2] (mvillalobsc2@unemi.edu.ec) (https://orcid.org/0009-0000-8831-4351)

José Luis Morales Herrera[3] (jmoralesh2@unemi.edu.ec) (https://orcid.org/0009-0008-5708-7000)

Leonel Steeven Nieves Licoa[4] (lnievesl@unemi.edu.ec) (https://orcid.org/0009-0003-5446-9509)

Enrique Colon Ferruzola Gomez[1] (eferruzolag@unemi.edu.ec) (https://orcid.org/0009-0003-5446-9509)

Resumen

Este estudio analiza la efectividad del marco legal ecuatoriano en la regulación y sanción de delitos de apropiación ilícita por medios electrónicos ante el aumento de ciberdelitos. El objetivo fue identificar fallas en el COIP y proponer mejoras legislativas. La metodología fue cualitativa, centrada en el análisis de normas y estudios comparativos sobre la regulación del cibercrimen, especialmente en países del Convenio de Budapest.

Los resultados muestran que el COIP no tiene sanciones disuasorias para delitos cibernéticos, lo que aumenta la impunidad. La falta de cooperación internacional limita a Ecuador en enfrentar

[1] Estudiante de la Universidad de Milagro, Ecuador
[2] Estudiante de la Universidad de Milagro, Ecuador
[3] Estudiante de la Universidad de Milagro, Ecuador
[4] Estudiante de la Universidad de Milagro, Ecuador
[5] Docente de la Universidad de Milagro, Ecuador

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

delitos transnacionales, un desafío que Costa Rica y Panamá han superado al unirse al Convenio de Budapest.

Estos hallazgos proponen reformas legislativas, incluyendo penas más severas, el Convenio de Budapest y unidades especializadas en ciberdelitos en Ecuador. Estas medidas mejorarían la capacidad del país para responder al cibercrimen, alineándose con estándares internacionales y protegiendo derechos patrimoniales y de privacidad en lo digital.

Abstract

This study analyzes the effectiveness of the Ecuadorian legal framework in regulating and punishing crimes of illicit appropriation by electronic means in the face of the increase in cybercrime. The objective was to identify flaws in the COIP and propose legislative improvements. The methodology was qualitative, focused on the analysis of norms and comparative studies on the regulation of cybercrime, especially in Budapest Convention countries.

The results show that the COIP does not have dissuasive sanctions for cybercrime, which increases impunity. The lack of international cooperation limits Ecuador in dealing with transnational crimes, a challenge that Costa Rica and Panama have overcome by joining the Budapest Convention.

These findings propose legislative reforms, including harsher penalties, the Budapest Convention and specialized cybercrime units in Ecuador. These measures would improve the country's ability to respond to cybercrime, aligning with international standards and protecting digital privacy and property rights.

Palabras clave: normativa penal, apropiación ilícita, delitos electrónicos, cibercrimen

Keywords: criminal regulations, unlawful appropriation, electronic crimes, cybercrime

Introducción

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

La tecnología ha cambiado la sociedad moderna, mejorando la comunicación, transacciones y gestión de la información. La digitalización ha originado delitos informáticos, que implican la apropiación ilegal de bienes y datos electrónicamente. Estas amenazas perjudican la privacidad, seguridad y economía de personas y organizaciones globalmente. Ecuador, como otros países de América Latina, debe adaptar su marco legal para enfrentar esta nueva criminalidad. Agregando a ello, El FBI registró 791,790 denuncias por delitos cibernéticos en 2020, lo que causó más de $4.200 millones en pérdidas. Comparado con el año 2019, las denuncias aumentaron un 69%. Este fenómeno ocurrió en casi todos los países, no solo en EE. UU (Velaña Quishpe, 2023). Resaltando la problemática a nivel global que se experimenta.

La necesidad de legislar contra delitos informáticos en Ecuador se hizo evidente con la Ley de Comercio Electrónico de 2002, el primer paso hacia un marco regulatorio (Ordóñez Córdova, 2024). La ley fue pionera en reconocer legalmente documentos y firmas electrónicas esenciales para la economía digital. Sin embargo, su efectividad en ciberseguridad fue limitada, dejando muchas amenazas sin regulación. Con el aumento de la dependencia digital, quedó claro que las normativas iniciales eran insuficientes para proteger contra delitos cibernéticos.

En 2014, Ecuador implementó el “Código Orgánico Integral Penal” (COIP), que incluyó por primera vez normas para delitos informáticos (Asamblea Nacional, 2014). El “COIP” clasifica delitos digitales como el acceso no autorizado a sistemas y la interceptación de datos que comprometen la seguridad y privacidad. Este código busca facilitar la persecución de actividades ilícitas en el ciberespacio. La efectividad de estas normativas depende de la capacitación de jueces, fiscales y policías en tecnologías digitales para enfrentar el cibercrimen.

Los retos en la regulación de delitos cibernéticos son globales. La adopción de tecnologías digitales en la región ha incrementado los delitos informáticos, como se observa en Tamaulipas, lo que resalta la necesidad de una política pública integral de ciberseguridad en México (Domínguez Arteaga y Vera Vázquez, 2020). Recientes estudios indican que el ciberfraude, el phishing y el robo de contraseñas son crecientes amenazas para el comercio electrónico. Los ciberdelincuentes utilizan técnicas avanzadas para robar información financiera, causando grandes pérdidas a empresas e individuos (Sempertegui Torres, 2022). Este tipo de crímenes

Sinergia Académica
ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

abunda en plataformas de comercio electrónico debido a la gran cantidad de datos personales y financieros. Estos delitos requieren que los países implementen leyes y medidas de ciberseguridad adecuadas a los riesgos actuales.

El análisis en Ecuador, según expertos como Sempertegui (2022), muestra que el "COIP" ha sentado bases para sancionar la apropiación fraudulenta electrónica, pero las lagunas legales y la aplicación desigual han causado impunidad (Sempertegui Torres, 2022). Sempertegui indica que el "phishing" carece de regulación adecuada en el sistema penal ecuatoriano. En comparación con otros países, Ecuador tiene limitaciones significativas en la persecución de delitos, lo que afecta la eficacia del sistema de justicia y vulnera a los ciudadanos.

En cuanto a, la "apropiación ilícita electrónica" es un delito común en el ámbito digital, difícil de atribuir a los culpables y de naturaleza transnacional (Paguay, 2020). Esto significa que los delitos pueden abarcar diversas jurisdicciones, por lo que la cooperación internacional es esencial. Ecuador ha mejorado al unirse a acuerdos internacionales de ciberseguridad y protección de datos, alineándose parcialmente con normas globales como el Convenio de Budapest (Becker y Viollier , 2020). La falta de armonización con normativas internacionales y un marco legal específico complican la prevención y sanción del cibercrimen.

La criminalidad informática es una preocupación principal en América Latina, especialmente tras el aumento en el uso de plataformas digitales post-COVID-19 (Zuñiga Paredes et al., 2021). Esto aumentó la exposición de los usuarios a ciberdelitos como fraude en línea, robo de identidad y manipulación de datos. Las investigaciones de Domínguez y Vera (2022) destacan que los "ciberdelitos" afectan tanto la seguridad de los datos como la economía. Los expertos indican que sanciones deben ir acompañadas de campañas educativas sobre riesgos y prácticas seguras en tecnología.

En Ecuador, estudios recientes destacan las complejidades que enfrentan las autoridades judiciales en la persecución de delitos de apropiación fraudulenta en línea. En donde Entre 2017 y 2021, los casos denunciados aumentaron un 29,11%. Incrementando de un 17.480 en 2017 a 22.569 en 2021, según la Fiscalía (Velaña Quishpe, 2023).

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

El estudio Aguirre Castillo (2022) en Ibarra muestra que es complicado establecer la responsabilidad penal de las personas jurídicas en delitos cibernéticos debido al anonimato y movilidad de los delincuentes. La investigación muestra que los escasos casos de la Fiscalía de Ibarra no han llegado a juicio por falta de pruebas y capacitación en ciberinvestigación (Aguirre Castillo, 2022). Asimismo, la autora sostiene que la falta de formación de los agentes judiciales perjudica la protección de derechos patrimoniales y deja impunes muchos delitos. Se destaca la necesidad de mejorar la capacitación de jueces, fiscales y personal de seguridad financiera para contrarrestar la sofisticación de los delincuentes cibernéticos.

En este sentido es pertinente mencionar el estudio de Velaña Quishpe (2023) ofrece una perspectiva profunda sobre la participación y responsabilidad penal en delitos de apropiación fraudulenta electrónica. Velaña (2023) analiza cómo las TIC han facilitado el surgimiento de nuevos tipos de crimen que amenazan bienes protegidos. Su trabajo analiza los niveles de participación en estos delitos, diferenciando entre autores y cómplices, y subraya la necesidad de un marco normativo adaptado a su naturaleza digital. El autor concluye que la legislación actual no garantiza adecuadamente la individualización de la responsabilidad penal en delitos informáticos (Velaña Quishpe, 2023). Este estudio destaca la necesidad de regular adecuadamente para identificar responsables en ciberdelincuencia y proteger el derecho a la propiedad.

En definitiva, los delitos informáticos en Ecuador evidencian que la tecnología ha superado la capacidad del sistema penal. Ecuador ha avanzado en cibercriminalidad, pero aún necesita un marco regulatorio integral para proteger a los ciudadanos en el entorno digital. Actualizar la legislación y fomentar la colaboración transnacional son claves para combatir la apropiación ilícita electrónica y delitos informáticos. Se requiere un enfoque integral que incluya actualización

legislativa, formación judicial y cooperación internacional para abordar la cibercriminalidad y proteger derechos en la era digital.

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

Ahora bien, comprendemos que la dependencia de tecnologías digitales ha creado desafíos legales y de seguridad sin precedentes. Los delitos informáticos, como la apropiación ilícita electrónica, son amenazas complejas que afectan la privacidad y los derechos de las personas. Este fenómeno requiere una respuesta legal que sancione a los delincuentes y prevenga conductas delictivas en un entorno digital complejo.

Esta investigación busca identificar la efectividad del marco legal ecuatoriano en la regulación de delitos de apropiación ilícita por medios electrónicos. El "COIP" y la "Ley de Protección de Datos Personales" abordan ciberdelitos, pero hay vacíos y desafíos en su aplicación. Analizar estas normas y su implementación es vital para entender sus limitaciones y proponer mejoras en la protección jurídica contra estos delitos.

El estudio aporta al derecho penal y la ciberseguridad al revisar la jurisprudencia y doctrinas, señalando avances y deficiencias en la justicia ecuatoriana. Este trabajo está dirigido a académicos, abogados y legisladores encargados de actualizar las leyes frente a nuevas amenazas digitales. Este análisis resalta la necesidad de una normativa ágil y robusta, alineada con estándares internacionales, para que Ecuador combata efectivamente el cibercrimen en una sociedad digitalizada.

Objetivo General

El objetivo de este trabajo es analizar y describir la efectividad del marco jurídico ecuatoriano en la regulación de los delitos de apropiación ilícita por medios electrónicos, identificando vacíos normativos y limitaciones en su aplicación. Este estudio busca ofrecer recomendaciones para mejorar la respuesta jurídica a delitos digitales, fortaleciendo la seguridad y los derechos patrimoniales.

Materiales y métodos

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

Se empleó un enfoque cualitativo para analizar las complejidades legales de la responsabilidad penal en delitos de apropiación ilícita por medios electrónicos. Este enfoque permitió un análisis profundo de los marcos normativos y las interpretaciones jurisprudenciales sobre la aplicación y efectividad de la legislación penal en el entorno digital.

El estudio es exploratorio y descriptivo. Se caracterizó la normativa vigente y principios doctrinales, y se observó su aplicación en casos de apropiación ilícita en medios electrónicos. Se llevó a cabo una revisión de la literatura y un análisis de leyes y casos relacionados.

La recolección de datos usó fuentes secundarias y se centró en dos métodos.

Por un lado, revisión documental: Se analizaron leyes nacionales e internacionales, doctrinas y estudios en derecho penal y ciberseguridad. Esta revisión ofrece el contexto legal y doctrinal para entender la evolución de la legislación penal sobre delitos electrónicos.

Por otro lado, el análisis comparativo internacional: Se examinaron las estrategias de países del "Convenio de Budapest" para entender mejor el marco ecuatoriano. Este análisis identificó áreas de mejora y recomendaciones para Ecuador.

Se utilizaron técnicas de análisis cualitativo, como el análisis de contenido, para identificar patrones en la aplicación de la ley penal en casos de apropiación ilícita digital. Se compararon los hallazgos de la revisión documental con el contexto internacional, identificando similitudes y diferencias en la normativa penal.

Resultados

La investigación aplicó un enfoque teórico del Derecho Penal y Ciberseguridad, analizando ciberdelitos y apropiación ilícita por medios electrónicos dentro de un marco normativo. Este enfoque permite identificar y tener un acercamiento con la efectividad de la legislación ecuatoriana ante las amenazas digitales. A continuación, se presentan los resultados de la investigación sobre la frecuencia, impacto y tipos de delitos informáticos, así como un análisis de las disposiciones actuales y recomendaciones.

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

1. Incremento de delitos cibernéticos en Ecuador.

Ecuador ha registrado 3,183 delitos informáticos entre 2020 y 2022 (Morejón Llanos, 2018). Las provincias más afectadas son Pichincha, Guayas, Imbabura, Manabí, Azuay y Carchi, con 682 casos en total (Chugá-Montenegro et al., 2024). Estas áreas activas económicamente son focos de ciberdelincuencia por el aumento del comercio en línea y los servicios bancarios digitales.

Tabla 1. Estadísticas de delitos cibernéticos en Ecuador y globalmente.

Año	Delitos cibernéticos reportados en Ecuador	Incremento porcentual (2017-2021)	Pérdidas económicas globales (FBI, 2020)	Incremento global en denuncias (2019-2020)
2017	17,480	-	-	-
2021	22,569	29.11%	$4,200 millones	69%

Datos de esta tabla provienen de la Fiscalía de Ecuador y el FBI.
Nota: No se encontraron datos sobre pérdidas económicas y el aumento global en Ecuador en 2017. Se identificó un aumento general en los delitos cibernéticos en años posteriores.

El aumento de delitos cibernéticos en estas provincias muestra la vulnerabilidad de ciudadanos y empresas ante amenazas digitales. Este fenómeno destaca la necesidad de un marco legal que proteja los derechos patrimoniales y refuerce la ciberseguridad. Estos datos indican la necesidad de actualizar el "COIP" y otras normativas para tratar los riesgos del crimen en el ciberespacio.

2. Tipología de Delitos Informáticos

Los delitos informáticos en Ecuador incluyen diversas modalidades que implican riesgos para el sistema de justicia. Los Delitos más reportados según (Morejón Llanos, 2018):

- Estafa en línea: Engaño para obtener información financiera o dinero. Las técnicas van del phishing, donde los delincuentes fingen ser entidades legítimas, a enlaces fraudulentos

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

que instalan "malware" en los dispositivos. La estafa en línea afecta económicamente a las víctimas y crea desconfianza en el comercio electrónico.

- Violación de la intimidad: acceso no autorizado a información privada, como correos y cuentas en redes sociales. Estos delitos violan la privacidad y pueden impactar psicológicamente a las víctimas (Pardo, 2024). La falta de conciencia ciudadana sobre la protección de datos favorece estos delitos.
- Acceso no autorizado a sistemas informáticos: Ingreso sin permiso del propietario. Esta práctica compromete la seguridad de la información y puede facilitar delitos como el robo de identidad o el espionaje industrial.
- Ataque a sistemas informáticos: Modifica o destruye datos críticos, dañando a individuos y organizaciones. Estos ataques buscan robar datos y sabotear operaciones.
- Fraude electrónico: Transferencia ilegal de bienes a través de sistemas electrónicos. Este delito compromete la seguridad financiera de las víctimas y es difícil de rastrear por el anonimato en el entorno digital.

Tabla 2. Delitos informáticos comunes y su impacto en Ecuador.

Tipo de delito	Descripción	Impacto
Estafa en línea.	Fraude para robar datos o dinero.	Pérdidas y desconfianza.
Violación de la intimidad.	Acceso indebido a información privada.	Afecta la privacidad y seguridad.
Acceso no autorizado a sistemas.	Acceso no autorizado a sistemas.	Vulnerabilidad de sistemas.
Ataque a la integridad de sistemas.	Alteración o eliminación de datos.	Daño a la integridad y operatividad de datos.
Apropiación fraudulenta por medios electrónicos.	Transferencia ilegal de bienes.	Pérdida de patrimonio y fraude financiero.

(Morejón Llanos, 2018)

3. Eficacia del COIP

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

El "COIP" de Ecuador tipifica varios delitos informáticos, como apropiación fraudulenta y acceso no autorizado. Los estudios indican que estas normas son insuficientes para los delitos digitales actuales (Sarmiento-Chamba y Maldonado-Ruiz, 2024). Por una parte, el art.- 190 del "COIP" impone penas de uno a tres años por apropiación fraudulenta. Sin embargo, estas penas son leves frente al daño financiero y emocional a las víctimas. Los expertos creen que estas sanciones no disuaden a los ciberdelincuentes, quienes operan casi impunes.

Mientras tanto, el "artículo 202" sanciona la violación de sistemas de seguridad y el uso indebido de datos personales con penas de seis meses a tres años de prisión y multas de $500 a $2,000. Se critica esta penalización por su falta de proporcionalidad al daño potencial. La escasa sanción de estos delitos puede aumentar la reincidencia, dañando la confianza pública en la justicia y la protección digital.

Tabla 3: Delitos Informáticos en Ecuador, Frecuencia, Impacto y Sanciones

Tipo de Delito Informático	**Frecuencia**	**Impacto Principal**	**Sanción Actual en el COIP**	**Recomendación de Reforma**
Estafa en línea	Alta	Pérdidas y desconfianza en e-commerce.	Prisión de 1 a 3 años (Art. 190)	Endurecer las penas por fraude grave.
Violación de la intimidad	Moderada	Impacto en la privacidad	(art. 178) - 1 a 3 años; Penas de 6 meses a 3 años y multas de $500 a $2,000. (art.-202)	Incluir medidas preventivas y endurecer penas por violación de datos sensibles.
Acceso no autorizado a sistemas informáticos	Alta	Vulnerabilidad de información	Penas de 3 a 5 años de prisión (Art. 234)	Personalizar sanciones según el daño.
Ataque a la	Moderada	Daño a la	Penas de 3 a 5	Aumentar penas

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

integridad de sistemas informáticos		integridad y operatividad de datos	años de prisión (Art. 232)	según el impacto en entidades.
Apropiación fraudulenta por medios electrónicos	Alta	Pérdida de patrimonio y fraude financiero	Penas de 1 a 3 años de prisión (art.190)	Reforzar normas contra transferencias ilegales de alto valor.

Comprendemos que, el cibercrimen, un desafío global de seguridad, afecta a todas las naciones. Países de diversas regiones han establecido normativas y colaboran internacionalmente contra estos delitos. El "Convenio de Budapest", el primer tratado internacional contra la ciberdelincuencia promueve la cooperación entre Estados en su investigación y persecución. Numerosos países, principalmente en Europa y América del Norte, han firmado y ratificado este tratado. En América Latina, solo cinco países están en el convenio, limitando la cooperación internacional.

Ciberseguridad en América Latina y el Caribe: Estado y Adopción del "Convenio de Budapest"

Los países de América Latina enfrentan grandes limitaciones para responder al cibercrimen. El Reporte de Ciberseguridad 2020 del "BID" y la "OEA" indica que solo 12 países de la región tienen estrategias nacionales de ciberseguridad (Ochoa Marcillo , 2021). Solo siete países tienen un plan para proteger su infraestructura crítica y menos de la mitad disponen de un grupo CERT o CSIRT para responder a ataques en tiempo real (OEA, 2020).

Ecuador no ha adoptado el "Convenio de Budapest", lo que restringe su cooperación en la lucha contra delitos transnacionales. La falta de adhesión a este convenio dificulta el enjuiciamiento de cibercriminales que operan desde el extranjero. La experiencia de Colombia y Argentina muestra

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

que la cooperación internacional ayuda a capturar ciberdelincuentes y a prevenir delitos a través del intercambio de información y prácticas de seguridad.

Comparación con EE. UU. y la UE

EE. UU. y la Unión Europea han adoptado medidas avanzadas de ciberseguridad y cooperan estrechamente. El IC3 del FBI en EE. UU. trabaja con agencias internacionales y locales para prevenir el cibercrimen (Martínez Padilla, 2015). La "Unión Europea" ha impuesto la Directiva NIS, que requiere a los Estados miembros adoptar medidas de ciberseguridad y colaborar en la investigación de incidentes cibernéticos. Ambas regiones tienen marcos regulatorios que sancionan delitos informáticos y exigen a empresas e instituciones públicas medidas de seguridad proactivas. La experiencia de estas regiones muestra la eficacia de políticas de ciberseguridad bien diseñadas y la cooperación internacional contra el cibercrimen.

Cooperación Transnacional y Comparación Internacional (Éxitos del Convenio de Budapest)

La adhesión al "Convenio de Budapest" ha mejorado la seguridad y cooperación contra el cibercrimen en varios países de América Latina y el Caribe. El Convenio unifica normas penales internacionales para mejorar la cooperación y la investigación de delitos cibernéticos entre países miembros (Guerrero, 2023). Costa Rica, República Dominicana y Panamá han mejorado su capacidad para responder a ciberdelitos y modernizar sus sistemas de justicia. Los estudios indican que el Convenio en Costa Rica ha facilitado reformas, incluyendo nuevos delitos informáticos y mejoras en ciberseguridad. Este país utilizó el Convenio para mejorar su ciberseguridad y crear infraestructura para responder a incidentes en tiempo real.

Impacto del Convenio en la "Cooperación Internacional"

El Convenio ha establecido un ecosistema internacional que facilita el intercambio de información y asistencia en cibercrimen entre naciones firmantes. Panamá usa la Red 24/7 para responder en tiempo real a ciberataques, mejorando su capacidad de manejar incidentes que impactan varias jurisdicciones (Guerrero, 2023). Este modelo de asistencia rápida y coordinación

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

entre gobiernos es crucial ante los ciberataques transfronterizos. Estas prácticas son viables para Ecuador, que busca mejorar su ciberseguridad y cumplir estándares internacionales.

Lecciones y Propuestas para Ecuador basadas en Estrategias Internacionales

La implementación del "Convenio de Budapest" en Latinoamérica demuestra que adoptar estándares internacionales es viable en economías emergentes, mejorando la efectividad en la lucha contra delitos y la protección de infraestructuras críticas (Novoa Toledo y Venegas Cruz, 2020). Ecuador podría aprender de Panamá y Costa Rica para crear unidades de ciberdelitos, establecer protocolos de conservación de evidencia digital y adoptar medidas de protección de datos alineadas con estándares internacionales.

Discusión

La investigación señala el aumento de delitos cibernéticos en Ecuador y analiza las limitaciones legales en comparación con experiencias internacionales. Se sintetizan y comparan los resultados con investigaciones de otros autores para evaluar la efectividad del marco legal ecuatoriano y sus desafíos:

1. Crecimiento de delitos cibernéticos y eficacia del COIP

Entre 2017 y 2021, Ecuador vio un aumento del 29.11% en denuncias de delitos cibernéticos. Este aumento demuestra la inadecuación de las sanciones del COIP, como indican (Velaña Quishpe, 2023) y (Sempertegui Torres, 2022), quienes destacan la ausencia de sanciones disuasorias para delitos como el phishing y el fraude en línea. Las penas de uno a tres años por apropiación fraudulenta no reflejan la gravedad del daño causado a las víctimas, limitando su efecto disuasorio.

Se sugiere que el COIP aumente las sanciones por delitos informáticos de gran impacto económico. La comparación con México y Estados Unidos sugiere que reformas legales en Ecuador podrían disminuir la impunidad y aumentar la confianza en la justicia.

2. Tipos de Delitos Cibernéticos y Vacíos Legales

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

La variedad de delitos cibernéticos en Ecuador revela que el marco normativo actual no aborda eficazmente cada infracción. La falta de diferenciación en la legislación, según (Morejón Llanos, 2018), dificulta la aplicación de sanciones. La ambigüedad en la definición de estos delitos permite a los culpables evadir la justicia o recibir penas menores.

Se recomienda definir con más precisión los delitos cibernéticos en el COIP para abordar esta deficiencia. Establecer agravantes y sanciones específicas fortalecería a jueces y fiscales en la imposición de penas justas. Esta especificidad legislativa es común en marcos avanzados como el de España, donde cada ciberdelito tiene regulación detallada para facilitar su persecución.

3. Beneficios del Convenio de Budapest a nivel internacional

Los hallazgos destacan la importancia de la cooperación internacional contra el cibercrimen, especialmente el Convenio de Budapest. Costa Rica y Panamá han mejorado su ciberseguridad y respuesta a incidentes transfronterizos al adoptar el Convenio. La falta de un marco de colaboración internacional en Ecuador dificulta la investigación y persecución de delitos cometidos desde el extranjero.

Se recomienda que Ecuador adhiera al Convenio de Budapest por esta limitación. Al unirse al Convenio, Ecuador podría acceder a redes internacionales como la Red 24/7, facilitando la coordinación en tiempo real contra delitos transnacionales. La integración facilitaría la adopción de estándares internacionales, alineando la legislación ecuatoriana con las mejores prácticas globales para una respuesta más eficaz al cibercrimen.

4. Mejoras y Desafíos de Implementación

A partir de los resultados y la comparación internacional, se proponen medidas para fortalecer el marco legal y operativo de Ecuador contra delitos informáticos, basadas en resultados y comparaciones internacionales. Entre ellos, la creación de unidades especializadas en ciberdelitos con personal capacitado aborda la falta de preparación del sistema judicial ecuatoriano para gestionar evidencia digital, como señala (Iñahuazo López, 2024). Estas unidades brindarán apoyo

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

especializado a jueces y fiscales en la recolección y preservación de pruebas digitales de manera segura.

También, la ejecución de campañas de concientización pública sobre riesgos y sanciones de delitos informáticos podrían reducir su incidencia, como se ha visto en España. En España, la educación digital es crucial para concienciar sobre los riesgos y consecuencias legales de las actividades en línea. La falta de conocimiento sobre derechos digitales en Ecuador conduce a que los ciudadanos realicen prácticas riesgosas o ilegales sin ser conscientes.

Estas recomendaciones destacan la necesidad de una estrategia integral que incluya reformas legislativas, capacitación y educación pública, basándose en las deficiencias identificadas en el estudio. Al implementar estas medidas, Ecuador fortalecería su marco legal contra el cibercrimen y se alinearía con estándares internacionales, protegiendo mejor a sus ciudadanos en el entorno digital.

Conclusiones

Este estudio analiza la efectividad del Código Orgánico Integral Penal (COIP) en Ecuador frente a los delitos cibernéticos de apropiación ilícita. El análisis revela que el aumento de la criminalidad digital en Ecuador supera la capacidad del sistema penal, mostrando vacíos legislativos y limitaciones en la investigación y sanción.

Los hallazgos indican que las penas y definiciones del COIP sobre delitos informáticos no se ajustan a la complejidad y el impacto económico de estos delitos. Las sanciones actuales no disuaden a los delincuentes, lo que aumenta la impunidad. La falta de especificidad en los delitos cibernéticos complica la asignación de responsabilidades y la aplicación de la ley, lo que exige reformas con agravantes y sanciones diferenciadas.

La comparación internacional muestra que el Convenio de Budapest podría ayudar a Ecuador a enfrentar mejor el cibercrimen. Los países del convenio han mejorado su cooperación y respuesta ante delitos transnacionales, facilitando investigaciones y juicios. La adopción de este convenio y

Jonathan Estanislao Freire Altamirano
Marylin Viviana Villalobos Cisneros
José Luis Morales Herrera
Leonel Steeven Nieves Licoa
Enrique Colon Ferruzola Gomez
Sinergia Académica
ISSN: 2765-8252
Volumen: 7
Nro. Especial 7
Año: 2024
Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

la creación de unidades especializadas en ciberdelitos fortalecerían la seguridad digital en Ecuador y protegerían mejor los derechos patrimoniales y de privacidad.

En definitiva, reformar el marco legal, especializar el sistema judicial y fomentar la cooperación internacional son claves para combatir los delitos cibernéticos en Ecuador. Estas medidas ayudarían a Ecuador a cumplir con estándares internacionales de ciberseguridad y proteger mejor a sus ciudadanos en un mundo digital.

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

Bibliografía

Aguirre Castillo, S. (2022). *El delito de Apropiación Fraudalenta por medios electrónicos y la responsibilidad de las personas jurídicas en el cantón Ibarra en el año 2021*. Universidad Regional Autónoma de los Andes.

Asamblea Nacional. (2014). *Código Orgánico Integral Penal, COIP*. Registro Oficial Suplemento.

Becker, S., & Viollier , P. (2020). La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. *Revista de derecho (Concepción), 88*(248), 75-112. https://doi.org/https://dx.doi.org/10.29393/rd248-13icsb20013

Chugá-Montenegro, J., Romero-Gutiérrez, M., Villarreal-Lugmaña, E., & Santander-Moreno, J. (2024). Delitos informáticos de apropiación fraudulenta por medios y transferencia electrónicos de activo patrimonial. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, 9*(1), 220-229. https://doi.org/https://doi.org/10.35381/racji.v9i1.3528

Domínguez Arteaga, R., & Vera Vázquez, R. (2020). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. *Podium*(41), 21–40. https://doi.org/doi:10.31095/podium.2022.41.2

Guerrero, C. (2023). *Convenio de Budapest sobre la ciberdelicuencia: Análisis sobre la adhesión y el proceso de implementación en Costa Rica, Guatemala, Panamá y la república Domenicana.* IPANDETEC.

Iñahuazo López, A. (2024). *Estudio jurídico y doctrinario sobre el ciber delito denominado phishing y la falta de normativa legal que regule los delitos informáticos [Tesis de Grado, Universidad Nacional de Loja]*. Repositorio UNL.

Martínez Padilla, M. (2015). *La responsabilidad bancaria frente a los delitos informáticos [Tesis de Maestría, Universidad Andina Simón Bolívar]*. Repositorio UASB.

Morejón Llanos, P. (2018). *Infracciones Informáticas en el Ecuador.* Universidad Espíritu Santo – Ecuador.

Novoa Toledo, I., & Venegas Cruz, L. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional.* Universidad de Chile.

Ochoa Marcillo , A. (2021). *Desafíos globales del cibercrimen: Caso Ecuador período 2014 – 2019 [Tesis de Maestría, Universidad Andina Simón Bolívar]*. Repositorio UASB.

Sinergia Académica ISSN: 2765-8252

Volumen: 7
Nro. Especial 7
Año: 2024

Recepción:18-08-2024 / Revisión:25-08-2024 / Aprobación:12-11-2024 / Publicación: 27-11-2024

OEA. (2020). *Ciberseguridad Riesgos, avances y el camino a seguir en América Latina y el Caribe.* Banco Interamericano de Desarrollo.

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

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet [Tesis de Grado, Universidad Nacional de Chimborazo]*. Repositorio UNACH.

Pardo, M. (2024). El tratamiento de las defraudaciones de fluido eléctrico en el Código Penal español. *Artículos doctrinales, 45*, 1-26. https://doi.org/https://doi.org/10.15304/epc.45.9482

Sarmiento-Chamba, J., & Maldonado-Ruiz, L. (2024). Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador. *Journal Scientific MQRInvestigar*, *8*(3), 1753-1781. https://doi.org/https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

Sempertegui Torres, M. (2022). *Delito de Apropiación Fraudulente por medios electrónicos bajo la modalidad de Phising dentro del marco jurídico ecuatoriano [Tesis de Grado, Universidad del Azuay]*. Repositorio UAZUAY.

Velaña Quishpe, C. (2023). *Los niveles de participación y la atribución de responsabilidad penal en el delito de apropiación fraudalenta por medios electrónicos [Tesis de Grado, Universidad Técnica del Norte]*. Repositorio UTN.

Zuñiga Paredes, A., Jalón Arias, E., Andrade Olmedo, M., & Giler Chango, J. (2021). Análisis de seguridad informática en entornos virtuales de la universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de Covid-19. *Revista Universidad y Sociedad, 13*(3), 454-459.