UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

Título

"La regulación jurídica del ciberdelito del carding a través del derecho comparado"

Trabajo de Titulación para optar al título de Abogado de los Tribunales y Juzgados de la República del Ecuador

Autores:
Cristhian Alexander Robalino Pailiacho
Ronald Joshua Malo Amancha

Tutor:
Dr. Bécquer Carvajal Flor.

Riobamba, Ecuador. 2024

DECLARATORIA DE AUTORÍA

Yo, **CRISTHIAN ALEXANDER ROBALINO PAILIACHO**, con cédula de ciudadanía **060476406-8** y **RONALD JOSHUA MALO AMANCHA**, con cedula de ciudadanía **060477064-4,** autores del trabajo de investigación titulado**: "LA REGULACIÓN JURÍDICA DEL CIBERDELITO DEL CARDING A TRAVÉS DEL DERECHO COMPARADO"**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, a los 09 días del mes de mayo de 2024.

Cristhian Alexander Robalino Pailiacho

C.I. 060476406-8

Ronald Joshua Malo Amancha

C.I. 060477064-4

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quién suscribe**, BÉCQUER CARVAJAL FLOR** catedrático adscrito a la Facultad de Ciencias Políticas y Administrativas por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado **"LA REGULACIÓN JURÍDICA DEL CIBERDELITO DEL CARDING A TRAVÉS DEL DERECHO COMPARADO"** bajo la autoría de Cristhian Alexander Robalino Pailiacho y Ronald Joshua Malo Amancha; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 06 días del mes de marzo de 2024.

Dr. Bécquer Carvajal Flor

C.I: 150043221-4

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"LA REGULACIÓN JURÍDICA DEL CIBERDELITO DEL CARDING A TRAVÉS DEL DERECHO COMPARADO",** presentado por Cristhian Alexander Robalino Pailiacho con cédula de ciudadanía número 060476406-8 y Ronald Joshua Malo Amancha con cédula de ciudadanía número 060477064-4, bajo la tutoría de Dr. Bécquer Carvajal Flor; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

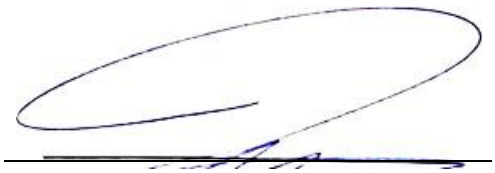
De conformidad a la normativa aplicable firmamos, en Riobamba, a los 20 días del mes de mayo de 2024.

Mg. Wendy Romero Noboa

PRESIDENTA DEL TRIBUNAL DE GRADO

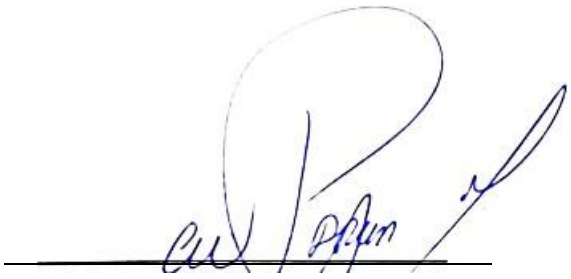
Dra. Rosita Campuzano Llaguno

MIEMBRO DEL TRIBUNAL DE GRADO



Dr. Walter Parra Molina

MIEMBRO DEL TRIBUNAL DE GRADO



NOTA FINAL: 10

CERTIFICADO ANTIPLAGIO

Que, **Cristhian Alexander Robalino Pailiacho**, portador de la cédula de ciudadanía **060476406-8** y **Ronald Joshua Malo Amancha**, portador de la cédula de ciudadanía **060477064-4**, estudiantes de la Carrera de **Derecho** de la Facultad de Ciencias Políticas y Administrativas; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"La regulación jurídica del ciberdelito del carding a través del derecho comparado"**, cumple con el 4%, de acuerdo al reporte del sistema Anti-plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente, autorizo continuar con el proceso.

Riobamba, 24 de abril de 2024.

Dr. Bécquer Caryajal Flor
TUTOR(A)

DEDICATORIA

El presente trabajo investigativo lo dedico a Dios, por haberme brindado la salud y permitirme alcanzar este momento tan significativo en mi vida. A mis padres Rosario y Jorge, por ser los pilares de mi vida y por sus sabios consejos que me han guiado mi vida y camino académico. A mis hermanos Isa y Jorsh por siempre haber creído en mí y apoyarme en cada paso de mi vida para lograr superar los desafíos. A mis perros, que han sido como mis hijos siempre los llevare conmigo. A mis mentores, las personas con las que eh tenido la grata oportunidad de trabajar y crecer académicamente. Finalmente, dedico esto a mí mismo y a todas las personas espectaculares que he conocido y me han inspirado, motivado y apoyado. Hoy es un objetivo más cumplido, pero, la meta a alcanzar es alta.

Con gratitud y amor,

Cristhian Alexander Robalino Pailiacho.

Dedico este trabajo a mis padres, por su amor incondicional, apoyo constante y sacrificios incansables que hicieron posible este logro. A mi familia, por su comprensión, paciencia y aliento en cada etapa de este viaje académico. A mis amigos y seres queridos, por su inspiración, motivación y momentos de distracción que mantuvieron mi espíritu en alto. A mis profesores y mentores, por su sabiduría, guía y pasión por el conocimiento que han sido una fuente inagotable de inspiración, gracias por ser parte de este camino hacia la realización de un sueño.

Ronald Joshua Malo Amancha.

AGRADECIMIENTO

Expresamos el más profundo agradecimiento a la Universidad Nacional de Chimborazo y a todas aquellas personas que hicieron posible la culminación de esta tesis, sin su apoyo, guía y aliento, este logro no habría sido posible.

En primer lugar, agradecemos a nuestro tutor de tesis, Dr. Bécquer Carvajal Flor, por su orientación experta, paciencia y dedicación, sabiduría académica y consejos valiosos fueron fundamentales para dar forma a este trabajo, constante apoyo y entusiasmo nos motivaron a superar obstáculos y seguir adelante.

También queremos expresar gratitud a nuestra familia, amigos y profesores por sus palabras de aliento y comprensión que durante los momentos de presión fueron invaluables.

Asimismo, deseamos agradecer a todas las personas que participaron en la recopilación de datos, su colaboración fue esencial para obtener información relevante y enriquecedora para este estudio.

Finalmente, a cada una de las personas que han dejado una huella indeleble en nuestra vida académica y personal, y les estaremos eternamente agradecido por el valioso papel que han desempeñado en este proceso.

¡Gracias a todos!

Cristhian Robalino y Ronald Malo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El proyecto de investigación analizó la regulación jurídica del ciberdelito del carding a través del Derecho Comparado, con un enfoque particular en la dimensión jurídica. La investigación se llevó a cabo en el cantón Riobamba y empleó un enfoque cualitativo que combinó métodos de comparación jurídica, dogmático, jurídico descriptivo y jurídico comparativo. Desde una perspectiva jurídica, se identificaron desafíos significativos en el tratamiento del ciberdelito de carding en Ecuador, destacándose la impunidad generada por la falta de claridad legal debido a la ineficacia de las leyes existentes y la escasez de una correcta tipificación en la ley penal. Asimismo, surge una preocupación legítima sobre la ausencia de tratados que fortalezcan la cooperación jurídica internacional. Además, la investigación reveló que países como Estados Unidos, Indonesia y Reino Unido abordan el carding mediante una normativa especializada. La metodología de investigación adoptada fue de carácter no experimental, con una muestra intencional compuesta por 13 jueces penales del cantón Riobamba, provincia de Chimborazo. Se aplicó una encuesta con un cuestionario de 10 preguntas utilizando Google Forms, dirigida a una población de jueces de unidad penal, tribunal de garantías penales y sala de lo penal en Riobamba. Los resultados de la encuesta reflejaron la falta de tipificación clara del carding en la legislación ecuatoriana, así como la precepción general de una regulación normativa insuficiente y poco ágil para abordar los ciberdelitos. Se resaltó la necesidad de crear políticas criminales digitales para establecer medidas preventivas y establecer sanciones; destacando sobre la importancia de abordar las deficiencias legislativas y fortalecer la capacidad normativa en la lucha contra el ciberdelito del carding en el contexto ecuatoriano.

Palabras clave: Cibercrimen, carding, derecho comparado, cooperación internacional.

ABSTRACT

The research project analyzed the legal regulation of the cybercrime of carding through comparative law, focusing on the legal dimension. The research was conducted in Canton of Riobamba and used a qualitative approach, combining comparative, dogmatic, descriptive, and comparative legal methods. From a legal perspective, significant challenges were identified in treating the cybercrime of carding in Ecuador, highlighting the impunity generated by the lack of legal clarity due to the ineffectiveness of existing laws and the lack of proper typification in criminal law. There is also a legitimate concern about the absence of agreements to strengthen international legal cooperation. In addition, the research revealed that countries such as the United States, Indonesia, and the United Kingdom address carding through specific legislation. The research methodology used was non-experimental, with a purposive sample of 13 judges of criminal cases from the canton of Riobamba in the province of Chimborazo. A 10-question questionnaire using Google Forms was applied to a population of judges of the Criminal Unit, Criminal Guarantee Court, and Criminal Court in Riobamba. The survey results reflected the need for a clear typification of carding in Ecuadorian legislation and the general perception of an insufficient and not very agile normative regulation to address cybercrimes. The need to create a digital crime policy to establish preventive measures and sanctions was highlighted, emphasizing the importance of addressing legislative deficiencies and strengthening regulatory capacity in the fight against the cybercrime of carding in the Ecuadorian context.

Keywords: Cybercrime, carding, comparative law, international cooperation.

Reviewed by:

Lic. Eduardo Barreno Freire. Msc.

ENGLISH PROFESSOR

C.C. 0604936211

CAPÍTULO I

1. INTRODUCCIÓN

La presente investigación examinó la regulación jurídica del ciberdelito del carding a través de un estudio comparativo del Derecho en distintas naciones. Se destacó cómo este fenómeno delictivo impacta a las sociedades estatales, generando una disyuntiva legal al abordar la normativa de este acto punible, la cual ha experimentado un aumento en diversos países alrededor del mundo. Esta transgresión digital trasciende las fronteras tanto a nivel nacional como internacional, Sambodo y Wahyinigsih (2021) aseguran que se han identificado obstáculos legales para tratar de manera efectiva este delito transnacional. Estas lagunas jurídicas afectan directamente a los usuarios que confían en las transacciones digitales, visto que las leyes existentes han demostrado ser insuficientes para su adecuado control, contribuyendo así a la impunidad de los casos.

Para Ali (2021), "el delito cibernético son todas las actividades delictuales que se efectúen utilizando sistemas informáticos o internet, puede incluir actividades como hackeo, robo de identidad, fraude y propagación de malware" (p. 2). Por tanto, el carding está estrechamente relacionado con los ciberdelitos de estafa y robo de información, como lo explica Sambodo y Wahyuningsih (2021) el carding es una práctica ilegal de usar información de las tarjetas de crédito robadas para consumar compras o transacciones no autorizadas, a través de diversos métodos de hackeo o pirateo en los que el titular de la tarjeta nunca provee su consentimiento.

El método de estudio se orientó en el análisis de la legislación de distintos países como son Ecuador, Estados Unidos, Indonesia y Reino Unido. Indagando normativa jurídica, los procedimientos penales y el juzgamiento del ciberdelito del carding. El objetivo fue establecer las bases estructurales para tipificar esta conducta antijurídica que transgrede el patrimonio de las personas y vulnera sus derechos constitucionales. El método de estudio del derecho comparado ayudó a que la investigación se enriquezca de la legislación internacional, con ello posterior al análisis individual, poder realizar conclusiones colectivas de los resultados obtenidos.

Este proyecto de investigación se propuso abordar la necesidad profesional de comprender la regulación jurídica del ciberdelito conocido como "carding", interés que se sustenta en la creciente influencia de la globalización tecnológica, que se ha implantado repentinamente en múltiples Estados, produciendo inconvenientes en la función legislativa de los mismos y enfocándose de manera principal en las transacciones que involucran el uso de tarjetas de crédito.

Para el análisis y estudio, se emplearon los métodos de comparación jurídica, dogmático, jurídico descriptivo y jurídico comparativo. Dado el carácter jurídico de la investigación, se adoptó un enfoque cualitativo. En función de los objetivos planteados, la investigación se catalogó como dogmática y jurídica descriptiva, con un diseño no

experimental. La población objeto de estudio estuvo conformada por 13 jueces penales del cantón Riobamba, provincia de Chimborazo.

Para la recolección de datos, se implementó una encuesta utilizando un cuestionario como instrumento. La información recabada fue analizada siguiendo la secuencia de preguntas de la encuesta. Para interpretar los resultados, se emplearon técnicas de inducción, análisis y síntesis, considerando la totalidad de los datos obtenidos. El objetivo principal fue verificar la hipótesis planteada y determinar los parámetros legales relevantes para la regulación del ciberdelito de carding dentro del Ecuador.

1.1. PLANTEAMIENTO DEL PROBLEMA

La globalización digital ha propiciado la difusión transfronteriza de datos en varias plataformas digitales, convirtiéndose en una práctica fundamental para las empresas y compañías, ya sean públicas o privadas en el desarrollo de sus actividades laborales diarias. Sin embargo, este avance tecnológico ha dado lugar, de manera inintencional, a la proliferación de nuevas formas delictivas, específicamente los ciberdelitos o delitos digitales. El carding como ciberdelito en sí forma parte del cibercrimen en las transacciones bancarias que utilizan el Internet para ser realizadas (Arifin et al., 2020), y encuentra su impulso principal en la filtración de datos, lo que a su vez ha generado métodos y técnicas innovadoras para llevar a cabo acciones delictuales en el ámbito digital. Por lo cual, la información recopilada y analizada sobre este delito determina el carácter transnacional del carding como delito que cruza fronteras nacionales y utiliza tecnología (Sambodo y Wahyuningsih, 2021).

Bajo esa premisa, Pérez et al. (2020) manifiesta que estos delitos son perpetrados por ciberdelincuentes tanto locales como internacionales y afectan a empresas y particulares por igual. En ese contexto, Peters y Hindocha (2020) concluyen que la dificultad para enjuiciar a los delincuentes en línea se debe a la complejidad de las redes de ciberdelincuencia y la necesidad de una mayor coordinación internacional. La existencia de victimización en el ciberespacio subraya la necesidad de abordar el ciberdelito de manera multidisciplinaria, esto implica la participación activa de diversas partes interesadas, tanto del sector público como del privado. Autores como Toro-Álvarez (2023) y Peters & Hindocha (2020) coinciden en la importancia de esta colaboración para fortalecer los esfuerzos de prevención y control del ciberdelito. (Toro-Álvarez, 2023).

Ahora bien, aunque varios países del mundo tienen una normativa -precaria- que tipifica y sanciona estos ciberdelitos, contrariamente, otras naciones carecen completamente de legislación positivada y de políticas criminales estatales que contribuyan a mitigar los efectos y consecuencias derivadas de este tipo de delitos. Así pues, la presencia de instrumentos internacionales se vuelve esencial para regular la convivencia social y sancionar las nuevas conductas típicas antijurídicas digitales. En el caso de Ecuador, Pérez et al. (2020) han concluido que los ciberdelitos en Ecuador han aumentado significativamente en la actualidad, siendo hoy por hoy de las principales amenazas para la seguridad digital en el país.

En base a lo expuesto, se evidencia la fragilidad estatal en Ecuador y en varios países a nivel mundial frente a la creciente amenaza de los ciberdelitos. Castro y Elizalde (2021) manifiestan que "han surgido nuevos delitos que con anterioridad no existían por tal razón el Estado debe adecuar su normativa (...)" (p. 14), este criterio se basa en la "cotidianeidad" con la que se cometen infracciones que implican diversas formas de estafas y robo de información a nivel tecnológico. Ante este aumento significativo y desproporcionado de la cibercriminalidad se ha creado un tipo penal específico, como es el carding que se dedica más a las transacciones, ya sean físicas u online (Muharam y Budianto, 2022).

El carding, ha experimentado un rápido crecimiento en la sociedad, focalizando principalmente sus acciones en las transacciones digitales, especialmente aquellas efectuadas con tarjetas de crédito. En el caso de Ecuador se implementan iniciativas y políticas públicas para fortalecer la seguridad digital en el país. Sin embargo, estas medidas son insuficientes (Juca-Maldonado & Medina-Peña, 2023). La escasa y deficiente regulación jurídica genera efectos perjudiciales para las víctimas directas de este ciberdelito, quienes en su mayoría son los consumidores o titulares de cuentas bancarias que enfrentan pérdidas financieras considerables al no poder demostrar de manera efectiva que no llevaron a cabo las transacciones fraudulentas, por esta razón, "los actores empresariales han considerado que los bancos no son seguros para asegurar los pagos en línea" (Arifin et al., 2020, p. 3).

1.1.1. Formulación del Problema

¿La carente regulación del carding en el Ecuador se ve reflejada a través de diversos enfoques legales adoptados por las legislaciones de Estados Unidos, Indonesia y Reino Unido para el tratamiento de este ciberdelito?

1.2. JUSTIFICACIÓN

La relevancia de esta investigación radica específicamente en ofrecer una perspectiva legal, sólidamente fundamentada en los estándares de Derecho Internacional Penal, particularmente en relación con el ciberdelito del carding y su tratamiento como infracción penal en las diferentes legislaciones analizadas.

Es esencial emprender una investigación jurídica centrada con un enfoque exhaustivo en el ciberdelito del carding. Este análisis debe llevarse a cabo mediante un estudio en Derecho Comparado, explorando las demás legislaciones que ya han desarrollado precedentes jurisprudenciales o normativa que contribuyan a no solo fortalecer una base jurídica sino a profundizar la comprensión de esta nueva infracción penal.

Resolver la impunidad es una de las razones para realizar el proyecto, considerando que la investigación adapta a la legislación a una evolución tecnológica, combatiendo así los desafíos que esta actividad delictiva ha generado con el pasar de los días, garantizando leyes que sean pertinentes y sobre todo efectivas en la era digital.

Desde una óptica legicentrista, es imperativo que el ordenamiento jurídico se adapte a las nuevas tecnologías, de manera que resulta fundamental la institución de un tipo penal específico y de la participación activa del país dentro de la cooperación jurídica internacional

especialmente en lo que corresponde a la asistencia judicial recíproca entre naciones para evitar la debilidad estatal.

En la actualidad las tasas de ciberdelitos en Ecuador y en los países del mundo han aumentado bruscamente y de manera incontrolable, por la inexistencia de un control estatal adecuado para mitigar los efectos jurídico-sociales de este tipo de delitos cibernéticos, fortaleciendo así los lazos transnacionales con otras naciones y otorgando recomendaciones para la creación de normas y tratados internacionales.

Por todo lo expuesto, mediante la divulgación de este trabajo de investigación los principales beneficiarios serán directamente los legisladores en el uso de sus atribuciones e indirectamente los abogados en el libre ejercicio de su profesión. Además del aporte en los usuarios que realizan este tipo de transacciones digitales, conociendo acerca del limbo jurídico que el carding provoca en su capital económico y reforzando la idea de que este delito necesita una regulación más severa.

Los beneficiados serán las compañías de seguridad digital empresarial, puesto que gracias a este análisis pueden comprender de mejor manera el delito que están sufriendo, contribuyendo a que refuercen su seguridad y aseguren proteger los intereses económicos propios y de los usuarios que depositaron la confianza en las transacciones comerciales.

1.3. OBJETIVOS

1.3.1. Objetivo General

Analizar a través de un enfoque de Derecho Comparado el ciberdelito del carding para determinar su regulación normativa en las diferentes legislaciones, abordar los desafíos jurídicos asociados y explorar la forma de consolidar la cooperación internacional.

1.3.2. Objetivos Específicos

- Realizar un estudio jurídico, comparado y crítico del ciberdelito del carding conforme a las bases jurídicas del tipo penal en las legislaciones de Ecuador, Estados Unidos, Indonesia y Reino Unido.
- Evaluar la relevancia jurídica del ciberdelito del carding en el ámbito digital, proporcionando una base sólida que garantice la eficacia normativa.
- Identificar las perspectivas legales específicas que enfrentan los sistemas judiciales al tratar el ciberdelito del carding.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ESTADO DEL ARTE

En relación con el tema "La regulación jurídica del ciberdelito del carding a través del derecho comparado", hasta el momento no se han realizado investigaciones idénticas; sin embargo, existen algunos estudios similares que han arrojado conclusiones relevantes. Entre los más destacados se encuentran:

Ali (2021) en la revista Internacional de Investigación Avanzada en Humanidades Público, dentro del articulo investigativo denominado *"Cyberspace and Organized Crime: The New Challenges of the 21st Century",* cuyo foco de investigación es la discusión de la vulnerabilidad en las sociedades occidentales respecto a los ataques cibernéticos, obtuvo como resultado:

> *The Internet provides an easily accessible means for individuals to conduct undetectable, high-impact cyber activities, leading to threats of cybercrime, cyber terrorism, and cyber warfare.*
>
> El internet proporciona un medio electrónico asequible para que todas las personas lleven a cabo actividades cibernéticas indetectables y de alto impacto, lo que lleva a amenazas de ciberdelincuencia, terrorismo cibernético y guerra cibernética (Ali, 2021).

Castro y Elizalde (2021), llevaron a cabo una investigación como parte de sus requisitos para obtener el título de Abogado/a en la Universidad de Guayaquil, Ecuador. El trabajo, titulado "Los ciberdelitos y su tipificación en el Código Orgánico Integral Penal", arrojó conclusiones significativas que contribuyen al entendimiento y abordaje de los ciberdelitos en el contexto legal ecuatoriano, como es:

> La materialización de los delitos cibernéticos depende de la tecnología, ya que es el conducto a través del cual se pueden manifestar estos delitos. Además, al ser delitos que ocurren en la clandestinidad requieren ser tratados por el Estado (Castro & Elizalde, 2021).

Sambodo y Wahyuningsih (2021), investigadores de la "Universidad Islámica Sultán Agung" escribieron un artículo investigativo titulado *"The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions",* analizando la aplicación del Derecho Penal contra el delito de *carding* en transacciones electrónicas, los resultados obtenidos de la investigación revelan:

> *Carding involves fraudulent practices in electronic transactions, with the potential to cause budgetary hurt to both people and trade substances. The application of criminal law in these cases is critical due to the transnational nature of such activities.*

> El carding implica prácticas fraudulentas en las transacciones electrónicas, con el potencial de causar perjuicios presupuestarios tanto a personas como a instituciones financieras. La aplicación del Derecho Penal en estos casos es fundamental debido a su carácter transnacional (Sambodo & Wahyuningsih, 2021).

Muharam y Bundianto (2022), en un artículo científico para la "Universidad Borobudur" de la ciudad de Jakarta, Indonesia, realizaron un trabajo investigativo titulado *"Carding Crime Analysis as A Form of Cyber Crime in Indonesia's Criminal Law"*, concluyen que:

> *Endeavors to address carding crimes are punitive or repressive. This effort is a legal policy in tackling cybercrime and to emphasize the number of crimes by using punishment or legislation, for the eradication of crimes that have occurred.*
>
> Los esfuerzos para hacer frente a los delitos de carding son punitivos o represivos. Este esfuerzo es una política legal en la lucha contra la mediante el uso de castigo o la legislación, para la erradicación de los delitos (Muharam & Budianto, 2022).

En su artículo científico titulado *"The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud"*, en la "Universidad Estatal de Semarang", Indonesia. Los autores Arifin, Hartini y Waspiah (2020), a través de un análisis exhaustivo concluyeron que:

> *Carding is a manifestation of various cybercrimes and a transnational crime involving credit card data theft. Carding as a cybercrime has been explicitly addressed and stipulated in the Budapest Convention on Cybercrime.*
>
> El carding es una manifestación de varios ciberdelitos y un delito transnacional que involucra la sustracción ilegal de datos de tarjetas de crédito. El carding ha sido explícitamente abordado y estipulado en el Convenio de Budapest sobre la Ciberdelincuencia (Arifin et al., 2020).

2.2. ASPECTOS TEÓRICOS

2.2.1. UNIDAD 1: INTRODUCCIÓN AL CIBERDELITO DEL CARDING

2.2.1.1. Reseña histórica de los ciberdelitos

Los inicios del internet se remontan a mediados del pasado siglo, concretamente a los años 1960 cuando ingenieros y científicos de los Estados Unidos desarrollaron una red llamada "*Advanced Research Project Agency"* (ARPA), para fortalecer las comunicaciones militares durante la Guerra Fría. En 1970, surgieron los proveedores de información online como *"Lexis"* y *"Dialog"*, marcando los inicios de las redes globales de comunicación de datos, esto abriría paso para el desarrollo de los primitivos servicios de *email* como *"CompuServe"* y *"Prodigy"* (Campbell-Kelly & Garcia-Swartz, 2005).

Durante las siguientes décadas, particularmente en los años 1980 y 1990, se desarrollaron hitos significativos en el ámbito tecnológico. Entre ellos destacan: el *"Transmission Control Protocol/Internet Protocol"* (protocolo TCP/IP), la institución de Microsoft, el avance de la *"Domain Name System"* (DNS), el descubrimiento de la *"World Wide Web"* (WWW), la fundación de páginas web como "*Yahoo!"*, "*Google"*, entre otras. Como se puede observar, el advenimiento del internet, de la computación y de las comunicaciones van simultáneamente, a la vez que, con ellas ha emergido la oportunidad de ejecutar los ciberdelitos (Giménez Solano, 2011).

El ciberdelito como fenómeno criminal, hizo su aparición por primera vez a mediados del siglo pasado, coincidiendo con el auge de las incipientes redes de internet y el desarrollo de las computadoras. La primera mención del uso de una computadora para cometer un crimen se hizo público en la década de 1960, cuando las computadoras eran grandes máquinas universales (Babanina et al., 2021).

El surgimiento de Internet y las conexiones inicialmente establecidas con computadoras específicas experimentó un notable desarrollo y popularización en la década de 1980. Durante este periodo, comenzaron a manifestarse las primeras evidencias de software malicioso (Tarhan, 2022). Desde una perspectiva histórica, estos delitos informáticos han sido perpetrados generalmente por individuos conocidos como "*hackers*", quienes son expertos en tecnologías de la información y poseen un conocimiento especializado en el funcionamiento de las computadoras.

Los delitos cibernéticos tuvieron una etapa de crecimiento durante la década de 1990 coincidiendo con la expansión del Internet, es decir, cuando comenzó la globalización digital. Este período se caracterizó por la accesibilidad creciente de las computadoras personales y el Internet, aunque es importante señalar que la expansión del internet a nivel mundial no fue uniforme (Babanina et al., 2021). No obstante, el uso generalizado de Internet propició un aumento significativo de los ciberataques, lo que generó el reconocimiento de la seguridad de las redes como una prioridad clave tanto para los gobiernos como para las industrias (Tarhan, 2022).

Desde el inicio del presente siglo hasta el presente, el impulso de las tecnologías de la información y su globalización mundial contribuyeron en el aumento de los ciberdelitos, pues, indirectamente tuvieron un impacto negativo en la sociedad dado que crearon nuevas

formas de delinquir adoptadas por los cibercriminales que comprometen los datos de las personas en el ciberespacio.

2.2.1.2. Aproximación, definición y alcance de los ciberdelitos

El término "ciberdelito", también conocido como "delito cibernético" o "delito informático" y en inglés como "*cybercrime*", fue internacionalmente adoptado en 2004 con la firma del Convenio de Budapest sobre la ciberdelincuencia. El Diccionario Oxford (2024) y el Diccionario de la Real Academia Española [RAE] (2024) definen al ciberdelito como "un delito que se ejecuta a través de la red", es decir, en esencia refieren principalmente a las actividades delictivas que hacen uso del internet y de las tecnologías de la información. Vale la pena aclarar que, doctrinariamente no existe una definición única de los ciberdelitos, por lo tanto, es importante destacar varias interpretaciones proporcionadas por distintos autores.

Para Bregant y Bregant II: "Los términos "delitos informáticos" y "ciberdelitos", que a menudo son sinónimos y usados indistintamente, se refieren a actos criminales realizados a través de internet " (Bregant & Bregant, 2014, p. 1). Para la Oficina de Responsabilidad del Gobierno de Estados Unidos: "El delito informático corresponde a las prácticas criminales que tienen como objetivo específico una computadora o red por daños o infiltración" (United States Government Accountability Office, 2007, p. 5).

El *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (2000) afirma que:

> El término "delitos informáticos" había sido desarrollado para abarcar tanto las formas completamente nuevas de delincuencia que estaban dirigidos a computadoras, redes y sus usuarios y las formas más tradicionales de delincuencia que ahora se estaban cometidos con el uso o asistencia de equipos informáticos. (United Nations, 2000, p. 26).

El *Comprehensive Study on Cybercrime de la United Nations Office on Drugs and Crime* [*UNODC*] (2013) asevera que en las diferentes legislaciones de los países se incluyen a los ciberdelitos como "el acceso no autorizado a un sistema informático, o la interferencia de un sistema cibernético o de datos" (UNODC, 2013, p. 12).

La Policía Nacional del Ecuador (2015) define a los ciberdelitos como:

> (…) toda actividad ilícita que: (a) Se ejecuta a través del uso de computadoras, sistemas informáticos u otros dispositivos de comunicación; o (b) Su objetivo es el robo de información, robo de contraseñas, fraude a cuentas bancarias, etc. (Policía Nacional del Ecuador, 2015, párr. 1).

El alcance de los ciberdelitos se vincula especialmente con las tecnologías de la información, abarcando las diversas actividades delictivas en el ciberespacio. Este alcance puede diferenciarse en tres formas principales: como una forma tradicional de actividad criminal, como un medio para la propagación y publicación de contenidos ilegales, y como una categoría de crimen exclusivo en redes electrónicas (Commission of the European Communities, 2007).

En la primera forma, se reflejan los ciberdelitos más comunes como: el fraude en línea, el robo de identidad, la estafa, la extorsión y el robo de información. En la segunda forma, se engloban los delitos vinculados a las graves violaciones que atentan contra los Derechos Humanos, tales como: el ciberterrorismo, el racismo, el ciberacoso, el tráfico ilícito de sustancias, la xenofobia, la pornografía infantil, la trata de personas, el tráfico de armas, el tráfico de órganos y el tráfico de animales.

En la última forma, se incluyen los delitos perpetrados contra personas naturales, sistemas de información estatales y organismos privados. Estos ataques se llevan a cabo mediante el uso de "*botnets*" (redes infectadas), para introducir software malicioso o "*malware*" e infectar equipos informáticos con el objetivo de cometer delitos sin que los usuarios estén al tanto o sin que puedan hacer algo al respecto (Commission of the European Communities, 2007). Un claro ejemplo de esta forma de delitos es: el "*phishing*", el "*carding*", el ciber espionaje y el "*hacking*".

2.2.1.3. Origen del ciberdelito del carding

El término carding tiene sus raíces en el idioma inglés, derivándose del sustantivo "*card"* que significa tarjeta, al que se le añade el sufijo "*-ing"*. El Diccionario Oxford (2024) define al primer término como "un pequeño trozo de plástico emitido por un banco o tienda, que se utiliza para comprar cosas u obtener dinero" (Oxford, 2024, párr. 7). Por otro lado, al aplicar las reglas gramaticales para traducir el sufijo "*-ing"* al español, se le otorga la terminación de un gerundio, resultando en -ado e -ido. De esta manera, el término carding puede ser literalmente traducido al idioma español como cardado o tarjetado.

Al ser considerado como un ciberdelito, el carding o cardado tiene su origen en el desarrollo y expansión de las tecnologías de la información a nivel mundial, específicamente en los años 1990. Esta particular práctica delictiva, surge como una amalgama de los delitos realizados por el crimen organizado como: estafa, lavado de dinero, robo de identidad y fraude (Arifin et al., 2020). No obstante, lo que distingue al carding y le confiere una trascendencia única es su ejecución a través de internet, utilizando como herramienta principal las tarjetas magnéticas, específicamente las tarjetas de crédito (Sambodo & Wahyuningsih, 2021).

Históricamente, este ciberdelito ha sido llevado a cabo por individuos que obtienen de manera ilícita información de tarjetas de crédito a través de Internet, para posteriormente utilizar estos datos para pedir cualquier producto o servicio en línea. (Arifin et al., 2020). Dicho de otro modo, el carding es un delito informático que se ha caracterizado por el uso ilegal de la información de las tarjetas de crédito y su número de seguridad, con el fin de adquirir ítems en línea. (Marbun & Setiyono, 2023).

2.2.1.4. Evolución del carding como ciberdelito

La propagación de las tecnologías analógicas conjuntamente con el advenimiento de las nuevas manifestaciones de la actividad delictiva digital presentan obstáculos sustanciales para las autoridades y la sociedad en general (Juca-Maldonado & Medina-Peña, 2023). Esto añadido a que, actualmente los ciberdelincuentes dentro de su *modus operandi* emplean

nuevas herramientas, técnicas y recursos para atacar a sus objetivos (Muharam & Budianto, 2022).

En las dos últimas décadas, las infraestructuras que facilitan la venta en línea de información de tarjetas de pago adquiridas ilícitamente han experimentado avances significativos (Van Hardeveld, 2018). Por tal motivo, el carding como ciberdelito ha experimentado una considerable evolución, manifestándose en dos métodos o modalidades diferentes, pero, intrínsecamente relacionadas en su resultado criminal. Estas son:

> 1) El defraude llevado a cabo mediante la obtención ilegal de información utilizando técnicas de ingeniería social, comúnmente el *phishing, skimming* y *cashing*; y, 2) El defraude tradicional que implica la sustracción o apropiación ilegítima de la información de las tarjetas de crédito mediante el uso de sistemas o programas de software malicioso o *malware* diseñados para hackear. (Arifin et al., 2020; Marbun & Setiyono, 2023; Sambodo & Wahyuningsih, 2021).

La primera forma se traduce a todos aquellas acciones criminales que emplean las tecnologías de la información en combinación de las técnicas de ingeniería social. En este enfoque, el delincuente se comunica con servicios de atención al cliente adoptando el papel de usuario para persuadir a los empleados mediante engaños a divulgar información que pueda otorgarle acceso al delincuente al sistema o viceversa (Bregant & Bregant, 2014). Entre las más destacadas se encuentran:

1. *Phishing*. - es el proceso que implica el engaño y la ingeniería social, tiene como objetivo obtener información confidencial de los clientes de una organización. (Meijerink, 2013). Existen varios tipos de *phishing* como: *smishing* (*phishing* por SMS), *vishing* (*phishing* por teléfono), *spear phishing* (*phishing* dirigido) y *whaling* (*spear phishing* netamente a ejecutivos y altos mandos).
2. *Skimming*. – involucra la adquisición de información de tarjeta de crédito y detalles adicionales mediante cámaras o bandas magnéticas dentro de la ranura de las tarjetas de los cajeros automáticos para realizar pagos no autorizados (Manaf, 2023).
3. *Cashing*. – técnica de ingeniería social para recaudar y cobrar dinero de cuentas financieras comprometidas. (Meijerink, 2013). Se divide en varios métodos como: *carding online* (robo de la información de la tarjeta de crédito*), in-store carding* (tarjetas de crédito falsas con datos reales) y *gift cards vending* (venta de tarjetas de regalo falsas).

La segunda forma implica tradicionalmente la extracción de la información de las tarjetas de crédito mediante programas de software malicioso. El *malware* es el conjunto de códigos y programas diseñados para infiltrarse en sistemas informáticos con el fin de causar daños o comprometer su integridad (Quevedo González, 2017). Algunas de las variantes más

conocidas y peligrosas de *malware* incluyen: virus, gusano, troyano, *adware*, *spyware*, *scripts*, *sniffers*, bombas lógicas, *botnets*, *exploit*, *droppers*, *rootkits*, *DDoS*, *spam* y *carding forums* (Ali, 2021; Meijerink, 2013; Quevedo González, 2017; Van Hardeveld, 2018).

2.2.1.5. Relevancia del carding en el contexto jurídico

En sus primeras etapas, el carding se entendía como parte del conjunto de delitos mencionados anteriormente. Sin embargo, con el tiempo al ya no ser sólo un problema técnico y legal, sino también un problema social, la solución efectiva fue abordar el fenómeno con un enfoque sistemático jurídico (Babanina et al., 2021).

Tipicidad del carding como delito

Para que el carding fuera tipificado como tipo penal, se debía identificar y demostrar los elementos objetivos del delito. Estos elementos incluyen: sujeto activo, sujeto pasivo, bien jurídico protegido, medios comisivos, nexo causal y resultado. (Arellano Cruz & Mendivil Cortez, 2020).

En este contexto, el sujeto activo o persona ejecutora del delito suele ser llamado "*carder*" o "*hacker*" (Muharam & Budianto, 2022). El término "*carder"* se refiere a una variante de hacker que se dedica a actividades de "*cracking*", con el fin de realizar transacciones fraudulentas con tarjetas creadas o adulteradas, empleando técnicas de ingeniería social y troyanos para obtener ilegalmente los números de tarjetas (Giménez Solano, 2011). Las actividades de *"cracking"* refieren a todos los actos de evitar o eliminar las medidas de protección de software, inhabilitando o evitando las restricciones en este caso de los sistemas financieros para realizar transacciones sin autorización (Chou, 2022).

Por otro lado, el sujeto pasivo o víctimas abarca tanto a las personas naturales (usuarios) como a instituciones gubernamentales y organismos privados (bancos) (Arifin et al., 2020). El bien jurídico protegido en este caso refiere al dinero que se encuentra en las cuentas bancarias (Muharam & Budianto, 2022). El medio comisivo es a través de la manipulación de las tecnologías de la información y comunicación (internet). El nexo causal se establece a través del método específico utilizado para la ejecución del delito y, el resultado se manifiesta en el uso ilegal de la información de las tarjetas para hacer transacciones y adquirir bienes o servicios (Marbun & Setiyono, 2023).

Elementos estructurales del ciberdelito

Como se ha observado, el carding es un ciberdelito que cumple con los estándares de tipicidad manifestados por la Teoría del Delito del Derecho Penal. Al respecto conviene agregar que, según la Organización de las Naciones Unidas (2020), en concordancia con Manaf (2023) existen varios elementos estructurales a tomar en consideración para la correcta tipificación de esta conducta tecnológica criminal en un Estado y son:

a. Delito tecnológico. De entre los tipos de delitos que utilizan totalmente la tecnología como medio de cometer un crimen, se encuentran los delitos del carding (Marbun & Setiyono, 2023).

b. Delito de carácter global. El carding como delito tiene un carácter global y transnacional que cruza fronteras nacionales y utiliza tecnología para ser realizado (Sambodo y Wahyuningsih, 2021).

c. Delito con mínimo contacto físico. Este crimen no necesita ningún tipo de contacto físico entre el victimario y la víctima para ser realizado. En el *modus operandi* del carding nunca existe contacto físico entre la víctima y el perpetrador, debido a que, el crimen ocurre en el mundo virtual, pero, tiene sus efectos en el mundo real (Manaf, 2023).

d. Identidad secreta del carder. Dentro de las particularidades de este ciberdelito se destaca el anonimato de los victimarios, ocultando su identidad de la detección por parte de las autoridades, asiendo así más difícil su enjuiciamiento (Juca-Maldonado & Medina-Peña, 2023).

e. Se ejerce sin violencia. El ciberdelincuente del carding no necesita robar la tarjeta de crédito, ni mucho menos amenazas físicas para crear miedo a la víctima, es suficiente saber los datos de la tarjeta (Manaf, 2023).

2.2.2. UNIDAD 2: REGULACIÓN JURÍDICA DEL CIBERDELITO DEL CARDING

2.2.2.1. Legislación relativa al carding

El ciberdelito del carding en el COIP

En el Ecuador, el ciberdelito del carding se encuentra dentro del tipo penal de estafa, mismo que, se destaca por ser un delito económico que involucra al engaño como principal factor y del cual se subdividen otras conductas nocivas. Bajo esta esencia, el tipo delictual se manifiesta cuando el sujeto activo, también llamado, estafador, emplea distintas artimañas u otros métodos fraudulentos en contra del sujeto pasivo, la persona estafada, induciendo al mismo a un acto voluntario que al momento de completarse tiene beneficios exclusivos para el infractor y deja afectado el patrimonio de la víctima (Morán Giler et al., 2022).

En el Código Orgánico Integral Penal (en adelante COIP) se encuentra tipificado el delito de estafa en el artículo 186. Cabe mencionar que, en este artículo se han implementado diversas modalidades para abarcar la mayor cantidad de conductas antijuridicas en el mismo tipo penal. Es por esta razón que, gran parte de las modalidades de fraude han sido revisadas de una manera muy superficial dejando varios casos en la impunidad (Farto Crespo, 2021).

Concretamente el numeral 1 y 2, del artículo ibidem, ajusta los presupuestos jurídicos del ciberdelito del carding, dado que, manifiesta:

1) La persona que defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2) Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. (Asamblea Nacional Constituyente, 2014).

De igual forma, relacionado con el tipo penal del carding, se encuentra el inciso 1 del artículo 190 del mismo cuerpo legal, que afirma:

1) La apropiación fraudulenta de un sistema informático para facilitar la apropiación de un bien ajeno, para la transferencia no consentida de bienes, valores o derechos, para beneficio suyo o de un tercero, manipulando el funcionamiento de redes electrónicas. (Asamblea Nacional Constituyente, 2014).

2.2.2.2. Convenciones y tratados relevantes

Normativa Internacional

La asistencia judicial mutua representa un pacto colaborativo entre Estados con el propósito de combatir las distintas infracciones penales en un plano de igualdad, reciprocidad y sobre todo para enfrentar y resolver conjuntamente cuestiones relacionadas

con la delincuencia transnacional. La esencia de este instrumento reside en la comprensión y reconocimiento de que los delitos actuales, especialmente aquellos vinculados a la ciberdelincuencia y la delincuencia organizada. Su finalidad se centra en facilitar el intercambio de información, pruebas y evidencias, para así, garantizar que los procesos judiciales se desarrollen conforme a estándares de legalidad y justicia, independientemente de la nacionalidad de las partes involucradas (Fiscalía General del Estado, 2013).

En el año 2004 entró en vigor el primer convenio sobre los delitos cibernéticos, el llamado Convenio de Budapest, mismo que, es un documento vinculante en materia penal que establece diferentes herramientas legales con el objetivo de perseguir y tipificar aquellas actividades ilícitas en contra de sistemas, medios informáticos o mediante el uso de estos. Éste se origina de una necesidad de reglas comunes entre sus miembros, para mejorar la cooperación internacional y así hacer frente a la ciberdelincuencia manteniente una misma línea normativa entre sus miembros (Convenio Sobre La Ciberdelincuencia, 2001).

Este tratado considera el ciberdelito como una criminalización de comportamientos que abordan habitualmente el acceso ilegal y la interferencia de los datos que se encuentran en los sistemas informáticos con propósitos ilícitos. Entre estos delitos se incluyen el acceso a computadores sin autorización, envió o recepción de información de datos personales de ajenos, así como la falsificación de documentos para beneficios de terceros (Mejía Lobo et al., 2023).

El Convenio Internacional sobre la Ciberdelincuencia tiene como finalidad la protección de víctimas de la ciberdelincuencia, enfatizando que, para esto es necesaria la implementación de estrategias efectivas al momento de investigar la identidad de quien o quienes están detrás de estas actividades ilícitas, en virtud de que, el *modus operandi* de estos infractores está basado en el anonimato. Por ello, es fundamental mejorar el acceso a la evidencia digital y la información disponible al momento del ataque, especialmente en casos de acción inmediata como delitos transfronterizos o amenazas económicas cibernéticas (Spiezia, 2022).

El convenio aborda los desafíos surgidos de las tecnologías modernas en la disputa contra la delincuencia cibernética. Subraya además la complejidad transnacional de tales delitos, donde los actos ilícitos, datos, víctimas y delincuentes pueden estar ubicados en distintas jurisdicciones. Al ser el primer instrumento internacional vinculante en este ámbito busca instituir una política penal común con el propósito de salvaguardar a la sociedad contra la ciberdelincuencia, combatiendo así los problemas de integridad y disponibilidad de sistemas, redes y datos informáticos (Wicki-Birchler, 2020).

En países como Indonesia con la suscripción del Convenio de Budapest se mejoró notablemente la seguridad digital, aunque este país ya contaba con regulaciones para los delitos cibernéticos, no eran suficientes para hacer frente a los ciberdelincuentes trasnacionales y su constante evolución, con la firma de este tratado se empleó el principio *"Aut Dedere Aut Judicare"*, expresión en latín que significa entregar o juzgar, la cual, es utilizada dentro del Derecho Internacional. Establece la obligación a los Estados de

extraditar a individuos acusados de delitos graves; en caso de no llevar a cabo la extradición, deben ejercer su jurisdicción para juzgar las situaciones e infracciones que la comunidad internacional considera particularmente serias (Fahamsyah et al., 2022).

La ratificación del Convenio de Budapest destaca la colaboración internacional entre naciones para la detención y sanción de los perpetradores, debido a que este instrumento otorga una base jurídica para la implementación de este principio. Los países que lo firmen pueden establecer un marco que facilite la asistencia mutua en la investigación y enjuiciamiento de la ciberdelincuencia, superando las fronteras y garantizando la seguridad jurídica al cubrir los vacíos legales que dejan las normas locales como el Código Penal.

La constante evolución de la tecnología y el mercado digital ha impulsado también el avance del Convenio de Budapest con el Protocolo II, el cual pretende fortalecer las estructuras de cooperación jurídica internacional en la lucha contra los ciberdelitos, ampliando así su margen hacia la relación directa con los prestadores de servicios digitales y con esto llevar una base de datos de quien es el autor de todo lo que se maneja dentro de la red de acuerdo con el servicio de internet que posean, con el objetivo que las posibles víctimas de estos delitos encuentren un poco de tranquilidad a la hora que las autoridades correspondientes atiendan su caso. Enfatizando la existencia de la cooperación de parte de todos los implicados para alcanzar el estándar de justicia y reforzar una rendición de cuentas hacia los perpetradores (Spiezia, 2022).

Lastimosamente a lo largo del tiempo nuestro país ha sido uno de los pocos países que no se ha suscrito el convenio de Budapest en ninguna de sus fases ni protocolos actualizados. Las autoridades competentes durante sus mandatos se enfocaron más a otro tipo de necesidades sociales, dejando de lado algo tan significativo como la ciberdelincuencia que ha tomado fuerza, pues, aunque el país haya firmado acuerdos internacionales en los últimos años, son escasos los que tengan relación con la jurisdicción penal y peor aún algo con los ciberdelitos.

En el Ecuador a partir del año 2021 hasta la actualidad, se han aprobado quince tratados e instrumentos internacionales esto en referencia a la información proporcionada por el portal de la Asamblea Nacional Constituyente, de los cuales, resalta. El tratado de Asistencia legal mutua en temas penales entre la República del Ecuador y la República Popular de China que en su parte pertinente manifiesta: Tener como objetivo el combatir en conjunto la prevención, investigación, persecución y enjuiciamiento de delitos, manteniendo los principios de independencia, igualdad jurídica, convivencia pacífica y cooperación internacional (Asamblea Nacional de la República del Ecuador, 2022).

En relación con los catorce tratos restantes, el mismo portal se evidencia áreas de interés, como el Derecho comercial, marítimo, acuerdos de extradición y asentamientos transfronterizos con países aledaños como Colombia, Perú y demás países europeos. Es evidente que ninguno de los convenios internacionales es de naturaleza penal, lo que destaca la necesidad de una reforma integral en la ideología que actualmente se lleva para tratar la ciberdelincuencia como fenómeno delictivo del Derecho Penal.

Dentro de la colaboración internacional que tiene el Ecuador con las demás naciones se encuentra el Instructivo de Cooperación Penal Internacional suscrito por la Fiscalía General del Estado, en el cual, se da a conocer los instrumentos bilaterales y multilaterales, además de memorándums de entendimiento para la administración de justicia en materia penal. Entre los instrumentos más relevantes tenemos:

1. Instrumentos Bilaterales
    - Tratado de cooperación en materia penal con Suiza (1999).
    - Convenio sobre asistencia judicial en materia penal entre Ecuador y la República de Paraguay (2001).
    - Convenio sobre asistencia jurídica entre el Ecuador y los Estados Unidos Mexicanos (2005).
2. Instrumentos Multilaterales
    - Convención Interamericana sobre asistencia mutua en materia penal, Nassau (1992).
    - Convención de las Naciones Unidas contra la delincuencia organizada transnacional, Palermo (2000).
    - Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas, Viena (1988).
    - Convención Interamericana contra la corrupción (1997).
3. Memorándums de entendimiento
    - Memorándum de entendimiento en materia de cooperación entre la fiscalía general de la República del Ecuador y la Fiscalía General de la nación de Colombia (2012).
    - Convenio interinstitucional de asistencia mutua en materia penal entre la Fiscalía General de la República del Ecuador y la Fiscalía General de la República de China (2011).

Los antes mencionados instrumentos internacionales son los más importantes que ha firmado el Ecuador en los últimos años. Si bien son todos de naturaleza penal, cabe aclarar que ninguno se refiere exclusivamente al tratamiento de los ciberdelitos y mucho menos al delito del carding o similares (Fiscalía General del Estado, 2013).

2.2.2.3. Impacto jurídico económico del carding

El ciberdelito del carding consiste en que los perpetradores emplean el uso de herramientas y recursos electrónicos, los cuales son originados por las mismas empresas de comercio digital y, son mal utilizadas por los delincuentes para llevar a cabo sus tácticas

criminales, con el objetivo de acceder a los sistemas informáticos y sustraer información confidencial de los usuarios.

En Ecuador, según la Unidad de Ciberdelitos de la Policía Nacional, se reportaron las siguientes cifras desde el año 2017 hasta junio del año 2023: en el año 2017, la cifra de 709 delitos cibernéticos; en el año 2018, la cifra de 738 delitos cibernéticos; en el año 2019, la cifra de 935 delitos cibernéticos; en el año 2020, la cifra de 682 delitos cibernéticos; en el año 2021, la cifra de 1851 delitos cibernéticos; en el año 2022, la cifra de 1340 delitos cibernéticos; y, en el año 2023, 573 delitos cibernéticos. Como se puede observar desde la pandemia COVID-19 que fue cuando obligatoriamente las empresas tuvieron que digitalizarse, es decir, desde el año 2020 al presente, la cifra de delitos informáticos es de 4.446, de los cuales, la mayoría de los casos no fueron investigados quedando en la impunidad (Angulo, 2023).

En el sector financiero, la evolución digital y la proliferación de las transacciones electrónicas han generado preocupación a nivel global, debido a la escaza regulación del comercio digital ocasionando con esto conflictos socioeconómicos para afrontar las posibles estafas y delitos derivados que surjan debido a este nuevo formato de negocios en la red. Los vacíos legales vulneran directamente los derechos de los implicados sea de forma individual o colectiva. De manera singular como un cliente de las empresas que ofrecen este servicio comercial y es víctima del robo de información personal y la pérdida de sus recursos económicos. O, de manera colectiva a las compañías que ofrecen el servicio, ocasionado daño a la honra y buen nombre de las empresas. En nuestro país, los sectores más perjudicados por la cibercriminalidad incluyen el bancario, el estatal y el minorista (*retail*) (Angulo, 2023).

Los datos recientes de una investigación realizada por Paysafe revelan que un alto porcentaje de ecuatorianos (73%) prefiere utilizar métodos de pago que no requieran compartir sus datos financieros. Sin embargo, a pesar de esta preferencia, el 72% de los encuestados considera que el riesgo de fraude es inevitable al realizar compras por internet. Estas discrepancias señalan la necesidad de fortalecer la cooperación internacional entre los Estados para abordar eficazmente estas preocupaciones. Se destaca la importancia de implementar leyes y regulaciones específicas para combatir el fraude en línea y garantizar que estas conductas no queden impunes (Juca-Maldonado & Medina-Peña, 2023).

2.2.2.4. Desafíos en la armonización jurídica

La armonización jurídica entre los Estados es crucial para abordar de manera efectiva los ciberdelitos y ejercer adecuadamente el poder punitivo. En ese contexto, la jurisdicción se plantea como un desafío y refleja el poder originario y propio del Estado para administrar justicia, que se materializa a través de organismos designados por el gobierno para ejercer dicha administración. La capacidad del Estado para lograr sus objetivos se traduce en poder, siendo la administración de justicia uno de sus propósitos fundamentales. Para lograr esto, las naciones establecen órganos especializados, con individuos debidamente capacitados, que desempeñaran la función de legisladores (Zambrano Pasquel, 2023).

La Jurisdicción responde a ciertos principios esenciales, entre los que destacan el principio de territorialidad. Este principio, derivado de una ficción legal, permite la aplicación de la ley al perpetrador del delito tanto en el lugar donde se comete la infracción como en el lugar donde se efectúa la detención (Zambrano Pasquel, 2023, p. 28). Además, se encuentra el principio de personalidad, que establece que la jurisdicción es personal, ya que, el sistema penal sigue a la persona esté donde esté (Zambrano Pasquel, 2023, p. 29).

De forma internacional la jurisdicción, tiende a ser una cooperación entre Estados, derivando un compromiso armonioso por tipificar y ejercer la jurisdicción penal sobre crímenes universales que salgan del alcance primario, esto incluye la facultad de investigar y procesar dichos crímenes, ya sean cometidos por personas físicas o jurídicas, dentro o fuera del territorio nacional. Posibilita la coordinación con otros países para tramitar el caso y su enjuiciamiento, sujeto a los vínculos de conexión establecidos en convenios internacionales y de forma subsidiaria los tribunales nacionales (Esteve Molto, 2020).

Para que exista una verdadera armonización jurídica se debe tomar en cuenta los estándares establecidos por las más altas cortes de justicia a nivel internacional para el caso de juzgamiento de los delitos perpetrados por delincuentes transnacionales como la ciberdelincuencia, teniendo en cuenta eso, se debe verificar la jurisdicción aplicable a los casos concretos como puede ser la nacional o la internacional.

Criterios de jurisdicción

En el Ecuador, la jurisdicción consiste en la potestad estatal de juzgar y ejecutor lo dictaminado. En el caso de jurisdicción nacional, se emplea de acuerdo con el ámbito espacial de aplicación estipulado en el Art. 14 del Código Orgánico Integral Penal, mismo que, en su numeral 1 manifiesta que: 1) Se aplicarán las normas penales del código a toda infracción cometida dentro de este territorio (Asamblea Nacional Constituyente, 2014). Esto en concordancia con el ámbito de la potestad jurisdiccional, establecido en el Art. 400 del código antes descrito, mismo que revela que, están sujetos a la jurisdicción penal del Ecuador: 1) Las y los ecuatorianos o las y los extranjeros que cometen una infracción en el territorio nacional (…) (Asamblea Nacional Constituyente, 2014).

En relación con la jurisdicción extraterritorial, de acuerdo con el Art. 14, numeral 2 del código ibidem, las normas de este código se aplicarán en las infracciones cometidas fuera del territorio, en los casos:

a) Cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción.
b) Cuando la infracción penal es cometida en el extranjero, contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se la cometió.
c) Cuando la infracción penal es cometida por las o los servidores públicos mientras desempeñan sus funciones o gestiones oficiales.

d) Cuando la infracción penal afecta bienes jurídicos protegidos por el Derecho Internacional, a través de instrumentos internacionales ratificados por el Ecuador, siempre que no se haya iniciado su juzgamiento en otra jurisdicción.
e) Cuando las infracciones constituyen graves violaciones a los Derechos Humanos, de acuerdo con las reglas procesales establecidas en este Código. (Asamblea Nacional Constituyente, 2014)

Al mismo tiempo, el ámbito de la potestad jurisdiccional establecido en el Art. 400 del código supra, están sujetos a la jurisdicción penal del Ecuador:

4) Las y los ecuatorianos o las o los extranjeros que cometen infracciones contra el Derecho Internacional o los derechos previstos en convenios o tratados internacionales vigentes, siempre que no hayan sido juzgados en otro Estado. (Asamblea Nacional Constituyente, 2014)

Además, conforme las reglas de competencia prescritas en el Art. 404 del COIP, se determina la competencia del juzgador en casos extraterritoriales: 6) Cuando la infracción se comete en territorio extranjero, la persona procesada será juzgada por la o el juzgador de la circunscripción territorial en la que es aprehendida o detenida o por la o el juzgador de la capital de la República del Ecuador (Asamblea Nacional Constituyente, 2014).

Jurisdicción extraterritorial

En delitos internacionales y transnacionales, el Ecuador, de acuerdo con los instrumentos internacionales a los que se encuentra suscrito y ratificado, concede jurisdicción extraterritorial exclusivamente a la Corte Penal Internacional. Esta corte se ocupa principalmente de investigar y perseguir a las personas que hayan cometido los delitos internacionales más graves (Santos Villareal, 2010). Así pues, la Corte Penal Internacional no está particularmente enfocada en perseguir ciberdelitos, lo que limita su capacidad para abordar las violaciones de derechos cometidas por delincuentes cibernéticos. Su enfoque principal recae en otros tipos de crímenes internacionales, lo que significa que los ciberdelitos podrían no recibir la atención necesaria en este ámbito.

La efectividad en el juzgamiento de los delincuentes de ciberdelitos es crucial para garantizar que no queden impunes, para ello, es esencial contar con normativas sólidas, ya sea a nivel nacional o internacional, que aborden adecuadamente este fenómeno criminal. Asimismo, se debe tener en cuenta los presupuestos jurídicos de la jurisdicción pertinente, asegurando que se cumplan los requisitos para considerar la conducta como típica, culpable, antijurídica y punible. La coordinación y cooperación internacional son fundamentales para abordar los ciberdelitos, ya que suelen trascender las fronteras nacionales.

2.2.3. UNIDAD 3: PERSPECTIVAS LEGALES INTERNACIONALES EN LA REGULACIÓN DEL CARDING

2.2.3.1. Mejoras en la cooperación internacional

La asistencia entre organismos internacionales y nacionales en la resolución de delitos transnacionales significa un reto jurídico importante en la actualidad. Pues, la colaboración internacional, interinstitucional y multidisciplinaria a veces llega a ser un concepto difuso que puede dar lugar a la falta de entendimiento mutuo, de lenguaje y de objetivos dentro de procedimientos penales (Geiran, 2022).

En el caso de los ciberdelitos, la estrecha cooperación sistemática internacional de los Estados es esencial para abordar los desafíos asociados a las manifestaciones delictivas transnacionales. Así pues, para Sambodo y Wahyuningsih (2021) "la comunidad internacional debe estar al tanto de la necesidad de cooperacion entre paises y la industria para combatir el cibercrimen". Es decir, las organizaciones intergubernamentales, interestatales, internacionales, interregionales y regionales deben desempeñar un papel crucial en la coordinación de las fuerzas del orden público para combatir la ciberdelincuencia (Evdokimov & Hobonkova, 2022).

En este contexto, aunque se busque una coordinación internacional entre Estados, es imperativo evitar el error de inobservar las normas y la jurisdicción propias de cada país. Sin embargo, tampoco sería prudente que un país, enfrentando delitos transnacionales, busque juzgar a los criminales de manera aislada sin la colaboración de otros Estados. Esto se fundamenta en el hecho que la mayoría de ciberdelitos cruzan la barrera nacional a través de diferentes naciones y entre varias jurisdicciones (Bregant & Bregant, 2014).

Con esas consideraciones, ¿La prevención, investigación y resolución de crímenes transnacionales, al igual que la persecución de los delincuentes de los crímenes de naturaleza internacional no puede ser llevada a cabo unilateralmente por un Estado sin la asistencia de otros Estados? La respuesta es un rotundo sí (Nahorniuk-Danyliuk et al., 2022).

Bajo esa premisa, el país debe coordinar esfuerzos con organizaciones internacionales como la Organización de las Naciones Unidas (ONU) y, las organizaciones internacionales de aplicación de la ley como la Organización Internacional de Policía Criminal (Interpol) (Evdokimov & Hobonkova, 2022). Además, aplicar instrumentos bilaterales, instrumentos multilaterales y, memorándums de entendimiento de cooperación en los que Ecuador se encuentra suscrito como país miembro y que fueron analizados supra.

Es pertinente que el Ecuador adopte una posición activa, especialmente en instancias como los Congresos sobre la Prevención del Delito y Justicia Penal que se han realizado desde 1955 por la ONU, puesto que, son lugares indispensables que buscan establecer métodos para luchar contra la delincuencia y la ciberdelincuencia. Es así que, el país debe participar tanto en los comités, las mesas de diálogos y las comisiones de expertos, como, en las votaciones de las resoluciones, dado que, esto influye en la creación de marcos legales que facilitan la coordinación internacional en la indagación y persecución de delitos.

En esa línea, el Ecuador debe reconocer la necesidad de una posible reforma al COIP en el ámbito de ciberdelitos, delimitando específicamente al delito del carding como tipo penal único alejado de otras infracciones. Además, debe crear mecanismos eficaces y eficientes encaminados en establecer políticas públicas, en este caso, políticas criminales digitales para colaborar a cerrar la brecha jurídica sobre la cual recae la impunidad de los delitos de carding. Igualmente, debe procurar suscribirse instrumentos internacionales contra los ciberdelitos como el Convenio de Budapest. También, explorar la posibilidad de realizar las reformas constitucionales pertinentes para permitir la extradición de delincuentes transnacionales.

Se debe promover la estandarización de procesos internacionales de asistencia judicial para contribuir a superar las barreras jurisdiccionales tal y como manifiesta el Manual de Asistencia Judicial Recíproca y Extradición de la UNODC. Asimismo, según el *14th United Nations Congress on Crime Prevention and Criminal Justice Congress* (2020) con el fin de facilitar una cooperación más fluida en la lucha contra los ciberdelitos es necesario utilizar herramientas e innovaciones tecnológicas, como:

El portal de gestión de conocimientos titulado *Sharing Electronic Resources and Laws on Crime* (SHERLOC)

El portal cuyo nombre en español es "Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia", fue fundado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y tiene como objetivo facilitar la divulgación de información relativa a la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus tres Protocolos (UNODC, 2024).

Este portal alberga una base de datos bibliográfica de legislación y jurisprudencia sobre diversos tipos penales, una base de datos de estrategias con planes de acción para los diferentes delitos, una base de datos de tratados para ratificar la Convención contra la Delincuencia Organizada Transnacional y sus diferentes protocolos, un directorio de todas las autoridades centrales y nacionales (DANC) designadas para la cooperación internacional y un módulo seguro (REV MOD) para examinar la aplicación de la convención ibidem en ciertos casos. Siendo, un recurso elemental para el intercambio de conocimientos y la colaboración internacional entre países miembros.

El portal SHERLOC juega un rol importante en la prevención de ciberdelitos como el carding, al permitir:

- Establecer bases de datos de incidentes, legislación aplicable, jurisprudencia y los modus operandi accesibles a las instituciones financieras públicas o privadas para mejorar sus sistemas de monitoreo y detección temprana de carding.
- Incentivar la centralización de las investigaciones sobre los métodos de carding para que organismos estatales (policiales), bancos y empresas sigan las últimas tendencias y actualicen sus defensas.

- Proveer foros para que investigadores en ciberseguridad colaboren e intercambien información con agentes financieros y fuerzas del orden sobre tácticas y herramientas utilizadas por los cibercriminales con el fin de mejorar la cooperación internacional.
- Compartir información y estrategias sobre cómo prevenir el robo de datos de tarjetas y la realización de transacciones fraudulentas. En este caso ayuda a que las instituciones públicas y privadas den estricta observancia a las técnicas y campañas utilizadas para obtener datos de tarjetas de crédito.

2.2.3.2. Adaptación de la legislación nacional a las tecnologías emergentes

La noción sobre que el Derecho debe perseguir constantemente los cambios de la sociedad y debe ajustarse continuamente a las realidades en evolución, refleja una perspectiva dinámica y evolutiva del Derecho con la sociedad. Esta afirmación reconoce la necesidad de que los Estados desarrollen nuevos marcos jurídicos actualizados que se adapten a las exigencias de la sociedad en constante evolución para abordar los retos y dinámicas contemporáneas.

La situación en Ecuador respecto a los ciberdelitos destaca la necesidad de adaptar la legislación nacional para abordar las tecnologías emergentes y ampliar la cobertura legal en contra de los ciberdelincuentes. Desde su entrada en vigor en agosto de 2014, las reformas al COIP reflejan cuan importante resulta mantener una normativa jurídica actualizada que tipifique y sancione de manera efectiva las conductas antijurídicas en el ámbito digital. El constante progreso de los delitos digitales conjuntamente con su ejecución a través de medios electrónicos requiere una permanente actualización jurídica, para evitar daños severos en la sociedad (Gómez Fonseca, 2023).

La posibilidad de reformar el COIP busca fortalecer el poder punitivo del Estado al tipificar la conducta penal en un artículo único, separado de lo estipulado en otros tipos penales como estafa y apropiación fraudulenta. El propósito es extender el alcance de esta conducta antijurídica al abordar diversos elementos relacionados con las infracciones cibernéticas. No se trata de establecer delitos de forma arbitraria o reformar la legislación penal para perjudicar a otros; más bien, se debe proporcionar herramientas eficaces a los operadores de justicia, para estos nuevos retos en la era digital (Gómez Fonseca, 2023).

En la era actual donde la tecnología predomina en el mundo, es crucial adherirse a las recomendaciones de la ONU sobre la digitalización de los procesos judiciales. Vale la pena decir que, en Ecuador, como en muchos países del mundo, se siguen llevando los registros en papel y las búsquedas y envío de documentos de forma física. Sin tomar en cuenta que, la tecnología permite utilizar plataformas electrónicas para gestionar las solicitudes judiciales que se envían y reciben o recopilar datos estadísticos sobre casos (United Nations, 2020).

En esa línea, la globalización digital ha experimentado cambios significativos con la incorporación de la inteligencia artificial (IA), que ha dado lugar al desarrollo de tecnologías predictivas en la gestión de la justicia penal. La escasa familiaridad con esta nueva herramienta informativa ha generado desconfianza en el sistema legal, argumentando la

necesidad de una mayor exploración antes de considerar su aplicación en procesos legales (Spesivov, 2023). Dicha introducción de la IA se debe llevar a cabo de manera gradual, creando así un equilibrio en la aplicación de estos instrumentos investigativos y el raciocinio humano.

La implementación de estas tecnologías en la administración de justicia local no debería obstaculizar el acceso de los ciudadanos a la justicia. Por el contrario, se espera que agilice el proceso penal tanto para los administradores de justicia como para los ciudadanos. Esta inteligencia artificial tiene la capacidad de analizar sistemas de datos cuantiosos para así distinguir los patrones de comportamiento, facilitando la detección de información y la evidencia relevante que podría haber pasado desapercibida para los seres humanos.

Para atribuir personalidad jurídica a los sistemas de IA, es imperativo fortalecer la responsabilidad penal en delitos vinculados con el uso de servicios digitales. La explosiva expansión de la inteligencia artificial ha incrementado los delitos de alta tecnología asociados con estas herramientas. Este panorama plantea interrogantes que deben abordarse mediante la implementación de regulaciones específicas enfocadas en los delitos relacionados con dicho instrumento electrónico, asegurando así una cobertura integral y una aplicación efectiva.

Para lograr esto, es esencial la colaboración internacional para establecer normas y marcos universales que aborden los delitos digitales y armonicen la responsabilidad penal en todas las jurisdicciones, modificando las normativas del Derecho Penal. La colaboración con expertos en IA resulta primordial para obtener información detallada sobre los beneficios y posibles riesgos e implicaciones de esta herramienta, asociados con los delitos originados a partir de ellas (Kamalova, 2020).

CAPÍTULO III

3. METODOLOGÍA

3.1. Unidad de análisis

La presente investigación se ubicó en el cantón Riobamba, provincia de Chimborazo, lugar donde se analizó el impacto del ciberdelito del carding.

3.2. Métodos

Para abordar el estudio del problema, por su naturaleza, se emplearon los siguientes métodos:

- **Método de comparación jurídica:** Este método permitió examinar las semejanzas y discrepancias del tema de investigación en diferentes sistemas legales, principalmente en otros países, con el fin de enriquecer el análisis y obtener una comprensión más profunda del tema de investigación.
- **Método dogmático:** Este método ha permitido dilucidar correctamente todos los aspectos del Derecho, como normas, doctrina y jurisprudencia, a través de un proceso sistemático jurídico utilizando el pensamiento crítico, la reflexión y la construcción de soluciones como herramientas principales.
- **Método jurídico descriptivo**: Este método faculta al investigador decidir la forma de derivar lógicamente las características y la naturaleza del objeto de estudio a partir de técnicas como la observación, recolección de información, análisis y comparación de datos y conclusiones.
- **Método jurídico comparativo:** Este método cualitativo relacionó lo teórico con lo empírico, basándose en lo estadístico y las particularidades específicas de la naturaleza del problema, es completamente recomendado para estudios en ciencias sociales y políticas.

3.3. Enfoque de investigación

Por las características de la presente investigación, se empleó un enfoque cualitativo.

3.4. Tipo de investigación

- **Investigación dogmática**: Se centró en el estudio lógico de la estructura del Derecho positivo, analizando normas jurídicas, jurisprudencia, doctrinas y precedentes para determinar la validez del ordenamiento jurídico en un contexto específico.
- **Investigación jurídica descriptiva:** Tuvo como objetivo describir las cualidades y características del problema, fenómeno o hecho jurídico investigado, proporcionando una visión detallada y precisa de la situación analizada.

3.5. Diseño de investigación

Dado la complejidad de la investigación, los objetivos alcanzados, los métodos utilizados para abordar el problema jurídico y por el tipo de investigación llevada a cabo, el diseño adoptado es de naturaleza netamente no experimental.

3.6. Población y muestra

3.6.1. Población

La población se estableció en los jueces penales con sede en el cantón Riobamba, provincia de Chimborazo.

3.6.2. Muestra

El diseño de la muestra se basó en un enfoque intencional no probabilístico, utilizando los siguientes criterios de inclusión:

- Jueces de Unidad Judicial Penal.
- Jueces del Tribunal de Garantías Penales.
- Jueces de Sala Penal.

Por tanto, la muestra se definió en un número de 13.

3.7. Técnicas e instrumentos de investigación

Técnicas

- Encuesta

Instrumentos

- Cuestionario consolidado en 10 preguntas relacionadas con "La regulación del carding a través del derecho comparado" a los jueces penales con sede en el catón Riobamba, provincia de Chimborazo a través de Google Forms.

3.8. Técnicas para el tratamiento de información

1. Elaboración del instrumento de investigación y aplicación del instrumento de investigación.
2. Tabulación de los datos proporcionados.
3. Procesamiento de los datos suministrados.
4. Interpretación y posterior análisis de los resultados.
5. Discusión de los resultados.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Análisis jurídico, comparado y crítico del ciberdelito del carding conforme a las bases jurídicas del tipo penal

Tabla 1. Análisis comparado del ciberdelito del carding.

	Ecuador	***Estados Unidos***	***Indonesia***	***Reino Unido***
Definición y caracterización del carding	Ecuador cuenta como norma sancionatoria al Código Orgánico Integral Penal, en el cual, no existe un artículo específico que defina y caracterice concretamente al carding. Sin embargo, esta infracción digital se encuentra determinada dentro de dos tipos penales como: Art. 186.- Estafa "cuando exista un defraude en la tarjeta de crédito"; y, Art. 190.- Apropiación fraudulenta "cuando se utilice sistemas informáticos para apropiarse de bienes" (Asamblea Nacional Constituyente, 2014)	En Estados Unidos la ley federal contra el fraude con el uso de tarjetas de crédito, específicamente en la sección 1029, clasifica el carding como: "la utilización no autorizada de información de tarjetas de crédito para llevar a cabo transacciones fraudulentas, tales como compras, transferencias de fondos u otras operaciones financieras, sin el consentimiento del titular de la tarjeta" (Office of the Law Revision Counsel of the House of Representatives, 2006). Este país al haber sido el punto de partida de la globalización digital ha dado lugar, a la tipificación de los ciberdelitos en su legislación penal a principios de la década de los 2000.	El carding implica el uso ilícito de tarjetas de crédito, ya sea robadas o falsificadas, con el propósito de cometer fraude en línea. Los perpetradores buscan adquirir productos ilegalmente o retirar fondos de cuentas bancarias pertenecientes a terceros, esto se encuentra tipificado en la Regulación Gubernamental N° 71 de 2019 de Operaciones de Transacciones y Sistemas Electrónicos (Sekretariat Negara, 2019)	Reino Unido cuenta como norma penal la Ley de Uso Indebido de Computadoras de 1990 que penaliza el acceso no autorizado a datos y distingue la existencia de la intención de cometer o la de facilitar la comisión de otros delitos para sancionar (Parliament of the United Kingdom, 1990). Además, existe la Ley de Fraude de 2006 que tipifica y penaliza la obtención de ganancias por fraude (Fraud Act, 2006).
Pena	El carding está previsto dentro de los tipos penales de estafa y apropiación fraudulenta: en el primer caso, la pena privativa de libertad será de hasta 7 años; mientras que, en el segundo caso la pena privativa de libertad será de 1 a 3 años.	En la sección de Delitos Informáticos y Propiedad Intelectual del Departamento de Justicia de EE.UU., se penaliza el carding con multas que varían a partir de mil dólares, dependiendo de la gravedad del delito. En casos de condenas	Las sanciones administrativas las impone el ministro según la normativa legal y reglamentaria pertinente. La imposición de las sanciones administrativas se realizará coordinadamente con el responsable del Ministerio o	El carding se encuentra previsto dentro la Ley de Uso Indebido de Computadoras de 1990 que penaliza el acceso no autorizado a datos de una persona, en esta caso, tarjeta de crédito con la intención de cometer o facilitar la comisión de otros

	Ecuador	*Estados Unidos*	*Indonesia*	*Reino Unido*
		reincidentes, se imponen penas privativas de libertad que oscilan entre 10 y 15 años (Office of the Law Revision Counsel of the House of Representatives, 2006)	Institución correspondiente. La imposición de sanciones administrativas no exime de responsabilidad penal ni civil (Sekretariat Negara, 2019)	delitos. La pena será de 12 meses a máximo 5 años o una multa de acuerdo con el procedimiento. Pero, si en el caso de que el acto no autorizado sea grave, la pena será de máximo 14 años (Parliament of the United Kingdom, 1990).
Procedimiento	Al hallarse el carding dentro de los delitos de estafa y apropiación fraudulenta, el procedimiento que se lleva a cabo es el ordinario. No obstante, se puede optar por el procedimiento abreviado (procede en delitos con pena de hasta 10 años) para reducir el tiempo de condena.	El carding, regulado por la ley federal contra el Fraude y actividades vinculadas al acceso a dispositivos, se clasifica en el sistema judicial federal penal, Al sustentarse de una manera similar al Ecuador podemos decir que manejan un procedimiento ordinario principalmente debido a que implica casos mayoritariamente vinculados con ciudadanos y gobiernos extranjeros en relación con los Estados Unidos.	El proceso judicial en Indonesia sigue una sustanciación ordinaria, similar al de otras jurisdicciones analizadas. El carding, al ser clasificado dentro de los delitos informáticos contra la sociedad y el Estado, resulta en una condena penal, dictada por un juez o tribunal competente, en estricta conformidad con las etapas procesales del caso (Sambodo & Wahyuningsih, 2021).	El código adjetivo regula el proceso judicial del carding, pues, en condena sumaria en Inglaterra y Gales corresponderá a una pena de máximo 12 meses o una multa que no supere el máximo legal de ambas partes. Mientras que, si hay acusación será una pena de máximo 5 años. Igualmente, si el acto resulta grave la pena será de 14 años.
Medidas preventivas	El Ecuador desde el 2021 ha reformado su legislación para establecer tipos penales contra los delitos informáticos, sin embargo, no se abordan completamente las amenazas cibernéticas. Es necesario que el país implemente una serie de iniciativas y políticas públicas (criminales digitales) para fortalecer la seguridad digital en el país. Actualmente, se encuentra desarrollando una normativa de	Estados Unidos ha implementado el sistema de seguridad conocido como "COMPSTAT", el cual busca agilizar la recopilación de datos estadísticos con el propósito principal de identificar problemas de atención prioritaria. Este sistema se fundamenta en el análisis científico y la utilización de información oportuna y de calidad. La recolección de datos se realiza a partir de diversas fuentes, tanto internas como	La firma del Convenio de Budapest en Indonesia ha mejorado la seguridad digital al abordar la evolución de los ciberdelincuentes transnacionales. Este tratado ha aplicado el principio "Aut Dedere Aut Judicare", que obliga a extraditar o juzgar internamente a los acusados de delitos graves. La ratificación del convenio destaca la colaboración internacional para la	Al ser un país con un avance significativo de la tecnología, es completamente fundamental la aplicación de tecnologías avanzadas de cifrado y autenticación. Esto ha sido implementado con la finalidad de proteger los datos personales para regular de manera más efectiva las transacciones digitales en el Reino Unido. Además, la Ley de Uso Indebido de Computadoras se alineó con el Convenio de

	Ecuador	*Estados Unidos*	*Indonesia*	*Reino Unido*
	respuesta rápida para supervisar y actuar en contra de los incidentes cibernéticos (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).	externas. Un aspecto destacado de COMPSTAT es su enfoque en la "rendición de cuentas". Una vez identificado un problema y desarrollada una estrategia, recae en la responsabilidad del oficial correspondiente asegurarse de que se tomen los pasos necesarios.	detención y sanción de los perpetradores, proporcionando una base jurídica para la asistencia mutua en la investigación y enjuiciamiento de la ciberdelincuencia.	Budapest para establecer más tipos penales. A pesar de la salida del Reino Unido de la Unión Europea varias de las leyes de la legislación relativa a la misma se siguen aplicando con el fin de permitir el flujo de ayuda internacional.
Jurisdicción extraterritorial	Ecuador ejerce jurisdicción extraterritorial de manera limitada conforme lo determina el Art. 14.2 del COIP y, generalmente depende de acuerdos bilaterales de cooperación o asistencia mutua.	Se argumenta que resulta indispensable para abordar amenazas transnacionales y salvaguardar los intereses de Estados Unidos en un mundo cada vez más interconectado, bajo las leyes federales 18 U.S.C § 1028, 1029, 1030, 1037, 1343, 1362.	La jurisdicción extraterritorial de Indonesia se basa en su legislación nacional y tratados internacionales, aplicándose en casos de delitos graves con conexiones significativas con el país, como delitos cibernéticos transnacionales o terrorismo.	El Reino Unido tiene jurisdicción extraterritorial limitada, pero puede perseguir delitos cometidos por sus ciudadanos en el extranjero. En este caso depende de la cooperación con entidades como la Unión Europea para enjuiciar a los delincuentes.
Cooperación internacional	Ecuador participa en acuerdos internacionales, pero, su capacidad para la cooperación internacional puede variar. En el caso de ciberdelitos no se encuentra suscrito a ningún instrumento internacional.	Estados Unidos ha firmado varios tratados y acuerdos en materia de ciberdelitos, incluyendo el Convenio de Budapest sobre Ciberdelincuencia, que establece cooperación internacional en la lucha contra el crimen cibernético. Además, participa en Tratados de Asistencia Legal Mutua en Asuntos Penales y acuerdos bilaterales de cooperación en seguridad cibernética con otros países. Estos acuerdos permiten el intercambio de evidencia digital, la	En el área de ciberdelitos, Indonesia ha firmado tratados internacionales como el Convenio de Budapest sobre Ciberdelincuencia y participa en la Iniciativa ASEAN sobre Ciberseguridad para fortalecer la capacidad regional en la lucha contra la delincuencia cibernética. Además, colabora con INTERPOL en operaciones conjuntas, intercambio de información y capacitación del personal para abordar los desafíos de la ciberseguridad. Estos acuerdos y	El Reino Unido coopera estrechamente con otros países a través de tratados internacionales y la Europol para combatir ciberdelitos. Cabe aclarar que el Reino Unido al encontrarse fuera de la Unión Europea no implica que no exista una cooperación internacional, pues, ambos conjuntamente se proveen asistencia mutua. Asimismo, el país colabora con empresas de seguridad informática como KASPERSKY y demás.

	Ecuador	*Estados Unidos*	*Indonesia*	*Reino Unido*
		extradición de sospechosos y la colaboración en la protección de infraestructura crítica. Estados Unidos demuestra así su compromiso con la cooperación internacional para combatir los delitos cibernéticos y proteger la seguridad digital.	colaboraciones reflejan el compromiso de Indonesia con la cooperación internacional en la prevención y represión de delitos cibernéticos, protegiendo así la seguridad digital y la privacidad en línea.	
Otras consideraciones	De todos los países estudiados, se denota que el único país que no posee una normativa que señale de manera efectiva el carding dentro de un tipo penal único es el Ecuador, puesto que, los demás países como Estados Unidos, Indonesia y Reino Unido lo tienen bien definido e incluso se destaca la manera en la que gozan de una mejor cooperación internacional por estar suscritos y ratificados en los instrumentos internacionales pertinentes a la ciberdelincuencia.			

Nota: *Estudio jurídico comparado del ciberdelito del carding en diferentes legislaciones.*
Fuente: *Elaboración propia.*

Análisis:

Esta tabla proporciona una visión comparativa de cómo cuatro jurisdicciones (Ecuador, Estados Unidos, Indonesia, y el Reino Unido) abordan el ciberdelito del carding desde el punto de vista legal. A continuación, se destacan algunos aspectos clave:

1. **Definición y caracterización del carding:**

Ecuador aborda el carding dentro de los tipos penales de estafa y apropiación fraudulenta, sin contar con una definición específica en su legislación. Estados Unidos clasifica el carding como la utilización no autorizada de información de tarjetas de crédito, penalizado bajo la ley federal contra el fraude con el uso de tarjetas de crédito. Indonesia tipifica el carding como un delito informático contra la sociedad y el Estado, aplicando el principio de Derecho Internacional para la extradición o enjuiciamiento interno. El Reino Unido penaliza el acceso no autorizado a datos de tarjetas de crédito bajo la Ley de Uso Indebido de Computadoras de 1990.

2. **Pena:**

Ecuador establece penas de hasta 7 años por estafa y de 1 a 3 años por apropiación fraudulenta. Estados Unidos impone multas y penas privativas de libertad de 10 a 15 años, dependiendo de la gravedad del delito. Indonesia regula las sanciones administrativas y penales según la normativa legal y reglamentaria. El Reino Unido impone penas de 12 meses a 14 años o una multa pecuniaria según la gravedad del acceso no autorizado.

3. **Procedimiento:**

Ecuador sigue un procedimiento ordinario, con la opción de procedimiento abreviado para delitos con pena de hasta 10 años. Estados Unidos clasifica el carding en el sistema

judicial federal penal, optando por un procedimiento ordinario. Indonesia utiliza un procedimiento ordinario para los delitos informáticos, similar a otras jurisdicciones. El Reino Unido sigue un proceso judicial ordinario, con la posibilidad de condena sumaria para ciertos casos.

4. **Medidas preventivas:**

Ecuador destaca la necesidad de implementar iniciativas y políticas públicas para fortalecer la seguridad digital. Estados Unidos utiliza el sistema COMPSTAT para recopilar datos estadísticos y enfocarse en la rendición de cuentas. Indonesia se beneficia del Convenio de Budapest y aplica el principio *"Aut Dedere Aut Judicare"* para la cooperación internacional. El Reino Unido emplea tecnologías avanzadas de cifrado y autenticación, además, alineándose su normativa con el Convenio de Budapest.

5. **Jurisdicción extraterritorial y cooperación internacional:**

Ecuador ejerce jurisdicción extraterritorial limitada y depende de acuerdos bilaterales para la cooperación internacional. Estados Unidos demuestra un compromiso sólido con la cooperación internacional a través de tratados y acuerdos bilaterales. Indonesia basa su jurisdicción extraterritorial en legislación nacional y tratados internacionales, colaborando con INTERPOL. El Reino Unido tiene jurisdicción extraterritorial limitada y coopera a través de tratados internacionales y Europol, incluso después de su salida de la Unión Europea.

Finalmente, esta tabla destaca las diferencias y similitudes en las diferentes legislaciones y los enfoques legales de las jurisdicciones analizadas en la lucha contra el ciberdelito del carding. Además, la cooperación internacional y las medidas preventivas emergen como elementos clave en la respuesta a este fenómeno delictivo que atenta contra los bienes jurídicos protegidos.

4.2. Evaluación de la relevancia jurídica del ciberdelito del carding en el ámbito digital para garantizar la eficacia normativa.

4.2.1. Encuesta dirigida a jueces penales del cantón Riobamba, provincia de Chimborazo

4.2.1.1. Resumen de las variables sociodemográficas

El análisis de las variables sociodemográficas revela datos significativos y relevantes sobre el grupo de individuos analizados. En cuanto al género, el 69% son masculino y el 31% femenino. En términos de edad, la mayoría se encuentra en el rango 45 a 54 años, representando el 54% del grupo, lo que indica que es una población relativamente madura. En relación con el nivel educativo, el total de la población posee una educación de posgrado/maestría, lo que destaca un alto nivel de formación académica en el grupo. Estos datos proporcionan una visión detallada de las características demográficas y educativas del grupo, mostrando una población con un nivel educativo elevado especializada en Derecho Penal.

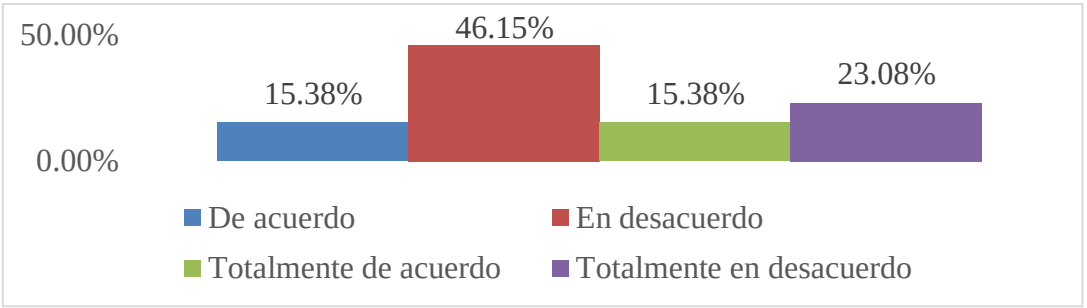
4.2.1.2. Análisis e interpretación de resultados

Tabla 2. Adecuación de la normativa actual al ciberdelito del carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	2	15.38%
En desacuerdo	6	46.15%
Totalmente de acuerdo	2	15.38%
Totalmente en desacuerdo	3	23.08%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 1. Adecuación de la normativa actual al ciberdelito del carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

Los resultados de la tabla revelan una percepción mayoritariamente negativa sobre la adecuación de la normativa actual en el país para abordar el ciberdelito del carding. Con un 46.15% en desacuerdo y un 23.08% totalmente en desacuerdo, la mayoría de los

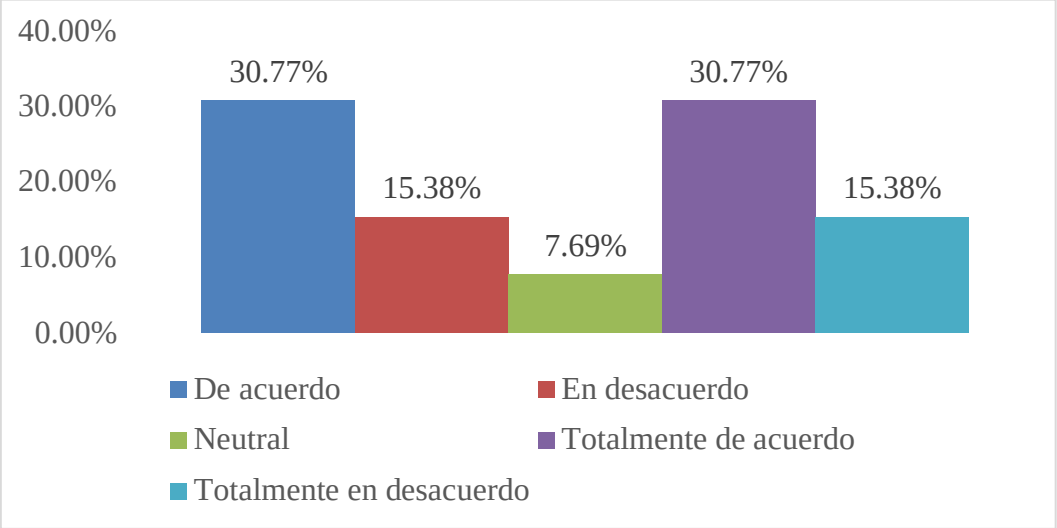
encuestados expresan preocupación sobre la efectividad de las leyes existentes en la lucha contra este tipo específico de ciberdelito. Solo un 15.38% está de acuerdo y otro 15.38% totalmente de acuerdo, señalando una necesidad evidente de revisión y mejora de la normativa para abordar de manera más eficaz el fenómeno criminal del carding.

Tabla 3. La falta de claridad en la legislación como obstáculo en la sanción del ciberdelito del carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	4	30.77%
En desacuerdo	2	15.38%
Neutral	1	7.69%
Totalmente de acuerdo	4	30.77%
Totalmente en desacuerdo	2	15.38%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 2. La falta de claridad en la legislación como obstáculo en la sanción del ciberdelito del carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

Los resultados de la tabla indican que el 30.77% de los participantes están de acuerdo y otro 30.77% están totalmente de acuerdo en que la falta de claridad en la legislación es un obstáculo para establecer sanciones a personas que cometen los ciberdelitos de carding. Este porcentaje significativo de respuestas afirmativas sugiere que existe una preocupación considerable acerca de la ambigüedad o insuficiencia de la legislación actual para abordar de manera efectiva y precisa este tipo de delitos. El 15.38% en desacuerdo y otro 15.38%

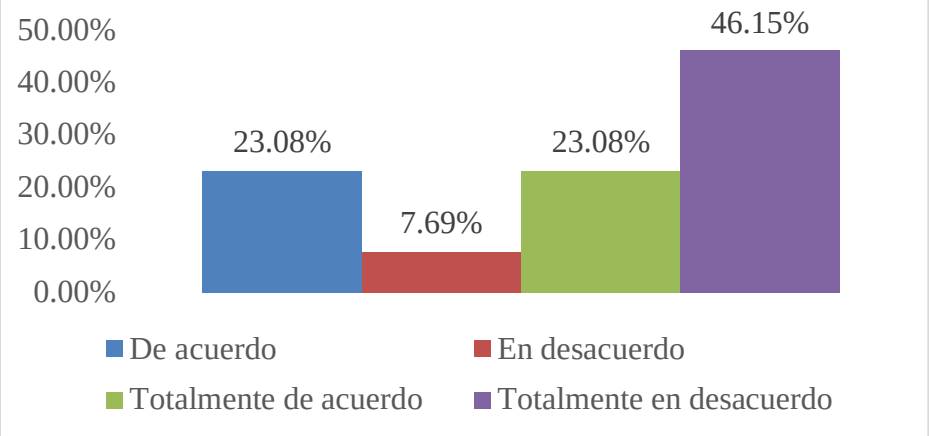
totalmente en desacuerdo indican una minoría que no percibe la falta de claridad como un problema significativo en este contexto, mientras que el 7.69% se mantiene neutral. Estos resultados sugieren la necesidad de una revisión y clarificación de la legislación penal para fortalecer la capacidad estatal de imponer sanciones adecuadas en casos de carding.

Tabla 4. Las leyes penales vigentes poseen la flexibilidad necesaria para abordar eficazmente la constante evolución de las tecnología de carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	3	23.08%
En desacuerdo	1	7.69%
Totalmente de acuerdo	3	23.08%
Totalmente en desacuerdo	6	46.15%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 3. Las leyes penales vigentes poseen la flexibilidad necesaria para abordar eficazmente la constante evolución de las tecnología de carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

Los resultados de la tabla sugieren que existe una preocupación significativa entre los participantes sobre la agilidad de las leyes penales actuales para seguir el ritmo de la evolución de las tecnologías de carding. El 46.15% de los encuestados están totalmente en desacuerdo, lo que indica una percepción generalizada de que las leyes penales no son lo suficientemente ágiles. Además, el 23.08% está de acuerdo y otro 23.08% está totalmente de acuerdo, lo que representa un porcentaje sustancial que comparte la opinión de que las leyes actuales no son lo suficientemente ágiles. Por otro lado, el 7.69% en desacuerdo sugiere que hay una minoría que cree que las leyes penales son lo suficientemente ágiles. En conjunto, estos resultados señalan una inquietud generalizada acerca de la capacidad de la legislación actual para mantenerse al día con la rápida evolución de las tecnologías asociadas al carding.

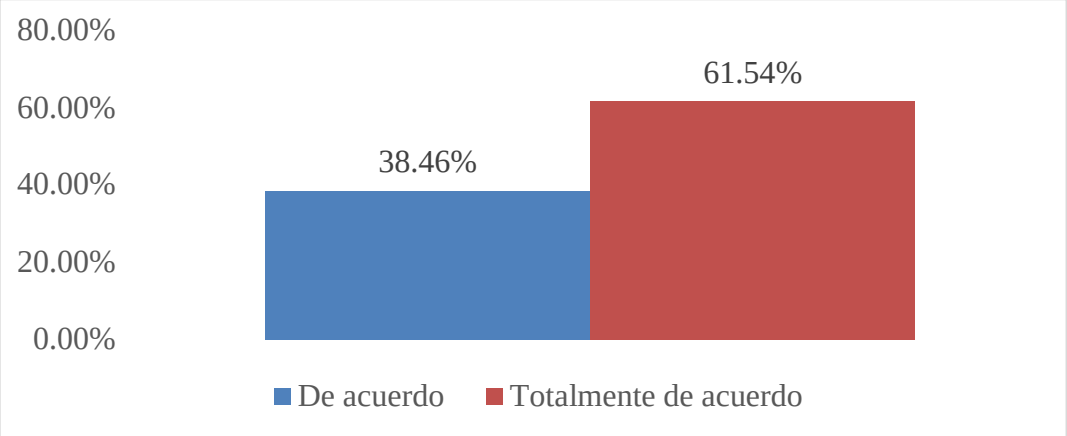
Esto sugiere la necesidad de considerar actualizaciones y reformas en el marco legal para abordar eficazmente estos delitos tecnológicos.

Tabla 5. La necesidad imperante de desarrollar políticas criminales digitales específicas para regular los ciberdelitos, específicamente sobre el carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	5	38.46%
Totalmente de acuerdo	8	61.54%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 4. La necesidad imperante de desarrollar políticas criminales digitales específicas para regular los ciberdelitos, específicamente sobre el carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

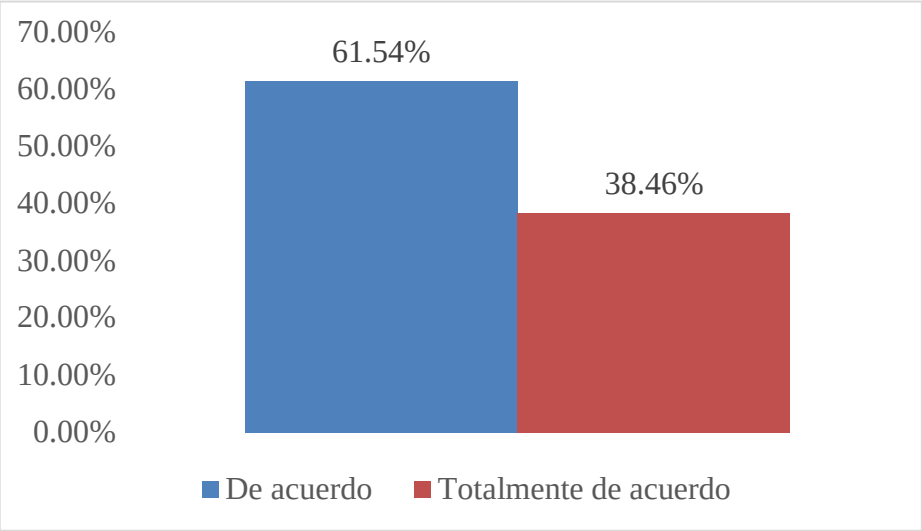
La tabla refleja un claro consenso entre los participantes en la necesidad de crear políticas criminales digitales que regulen los ciberdelitos, especialmente aquellos que afectan a sistemas financieros como el carding. El 61.54% de los encuestados está totalmente de acuerdo, y el 38.46% está de acuerdo. Esto indica que la mayoría de los participantes perciben la importancia y la urgencia de establecer políticas criminales específicas para abordar los ciberdelitos. La alta proporción de respuestas "Totalmente de acuerdo" sugiere una fuerte convicción en la necesidad de medidas jurídicas regulatorias más específicas y efectivas para hacer frente a los desafíos que plantea el ciberdelito en el ámbito financiero. Este consenso respalda la idea de que la formulación de políticas digitales es esencial para abordar adecuadamente los ciberdelitos como el carding.

Tabla 6. La rápida evolución de las técnicas de carding plantean dificultades particulares para la legislación y los procedimientos judiciales.

Opciones	Frecuencia	Porcentaje
De acuerdo	8	61.54%
Totalmente de acuerdo	5	38.46%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 5. La rápida evolución de las técnicas de carding plantean dificultades particulares para la legislación y los procedimientos judiciales.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

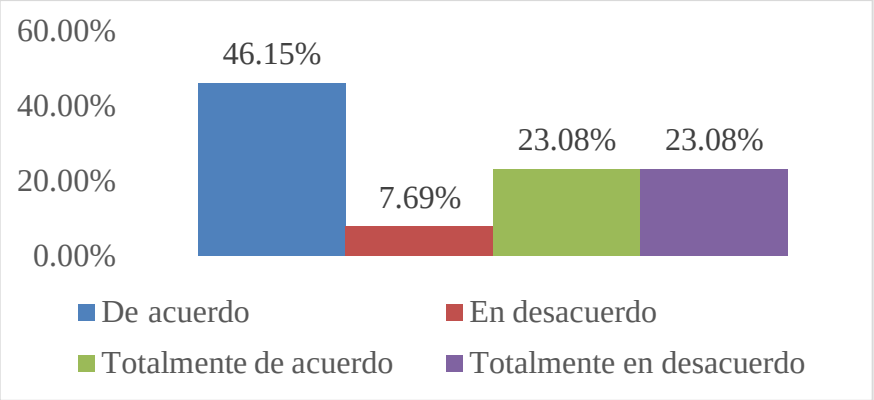
El análisis de la tabla muestra un fuerte consenso entre los participantes en relación con la velocidad de evolución de las técnicas de carding y los desafíos que plantea a la legislación y los procedimientos judiciales. El 61.54% está de acuerdo, y el 38.46% está totalmente de acuerdo, lo que indica que prácticamente todos los encuestados reconocen la rápida evolución de las técnicas de carding como un factor que presenta desafíos específicos para la legislación y los procedimientos judiciales. Esta percepción destaca la necesidad de que la legislación y los procedimientos judiciales se adapten de manera ágil y efectiva para hacer frente a las cambiantes tácticas utilizadas por los delincuentes cibernéticos en el ámbito del carding. La rápida evolución tecnológica plantea la demanda de una respuesta legal y judicial igualmente dinámica para abordar apropiadamente estos desafíos en constante cambio.

Tabla 7. La falta de conocimiento tecnológico por parte de los jueces representa un inconveniente para abordar eficazmente el carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	6	46.15%
En desacuerdo	1	7.69%
Totalmente de acuerdo	3	23.08%
Totalmente en desacuerdo	3	23.08%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 6. La falta de conocimiento tecnológico por parte de los jueces representa un inconveniente para abordar eficazmente el carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

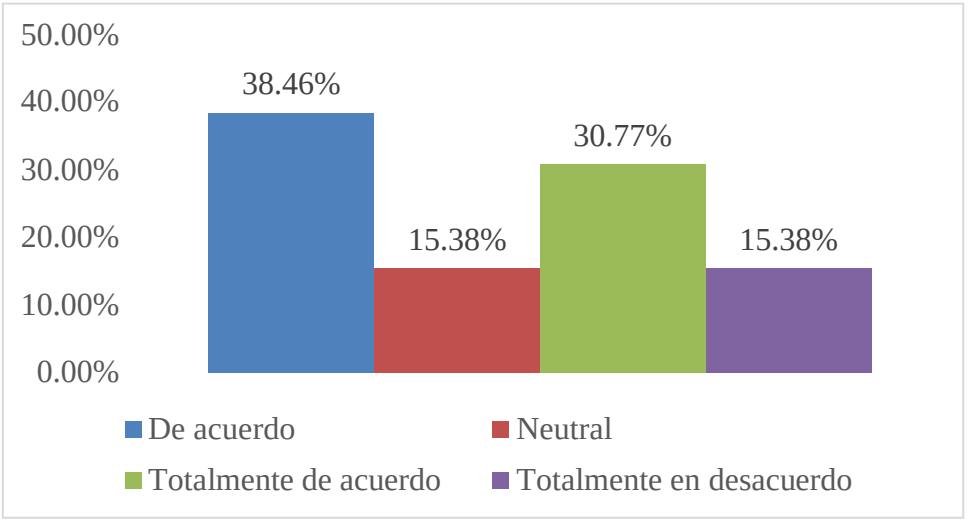
El análisis de la tabla indica que hay una percepción compartida entre los encuestados sobre la relevancia del conocimiento tecnológico de los jueces al abordar el carding. El 46.15% está de acuerdo, y el 23.08% está totalmente de acuerdo, lo que sugiere que la falta de conocimiento tecnológico de los jueces se percibe generalmente como un desafío significativo. Por otro lado, solo el 7.69% está en desacuerdo, y el 23.08% está totalmente en desacuerdo, lo que indica que hay una minoría que no ve la falta de conocimiento tecnológico de los jueces como un impedimento significativo. Este resultado destaca la importancia de mejorar la capacitación y la comprensión tecnológica de los administradores de justicia para abordar eficazmente los casos de carding y demás delitos cibernéticos.

Tabla 8. La necesidad de implementar capacitaciones judiciales más amplias en temas técnicos y digitales.

Opciones	Frecuencia	Porcentaje
De acuerdo	5	38.46%
Neutral	2	15.38%
Totalmente de acuerdo	4	30.77%
Totalmente en desacuerdo	2	15.38%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 7. La necesidad de implementar capacitaciones judiciales más amplias en temas técnicos y digitales.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

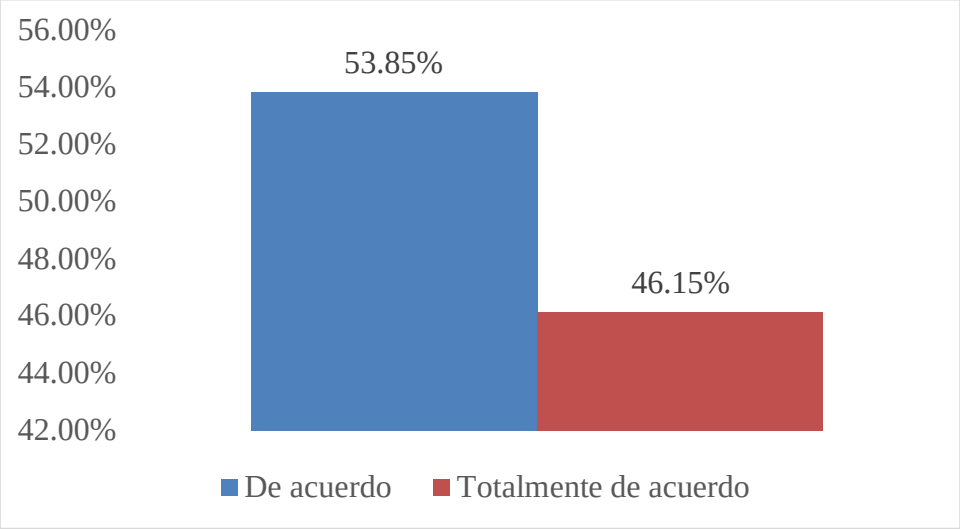
Analizando los datos, observamos que el 38.46% de los encuestados está "de acuerdo" y el 30.77% está "totalmente de acuerdo" con la necesidad de una mayor capacitación judicial en temas técnicos y digitales para garantizar una efectiva aplicación de la ley en casos de carding. En conjunto, el 69.23% de los encuestados respalda la idea de una mayor capacitación. Este resultado destaca la percepción general de que la capacitación adicional en asuntos técnicos y digitales es esencial para mejorar la capacidad del sistema judicial para abordar eficazmente los casos de carding y otros delitos cibernéticos. Sin embargo, también es relevante señalar que hay un 15.38% de encuestados que están neutrales o totalmente en desacuerdo, lo que podría indicar la existencia de opiniones divergentes sobre la necesidad de esta capacitación adicional.

Tabla 9. La colaboración internacional es crucial para el tratamiento del ciberdelito del carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	7	53.85%
Totalmente de acuerdo	6	46.15%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 8. La colaboración internacional es crucial para el tratamiento del ciberdelito del carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

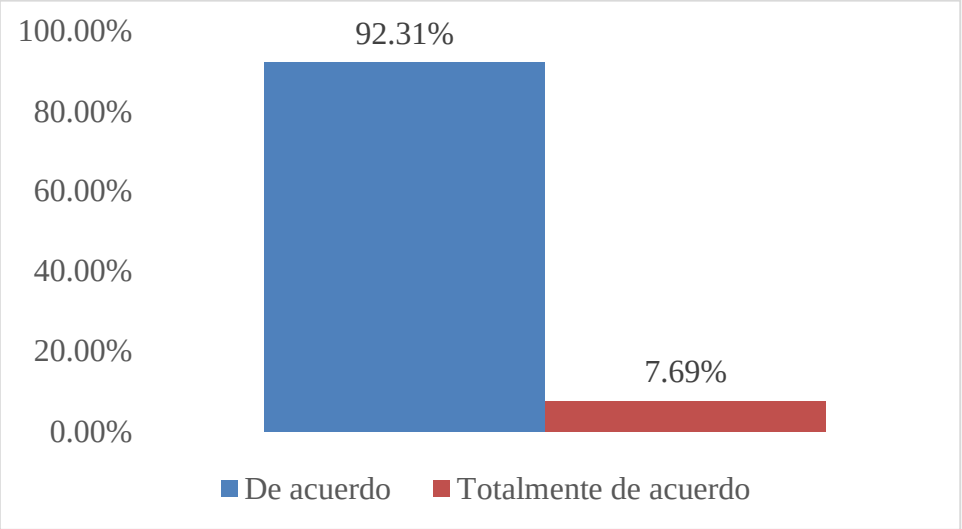
En base a la tabla proporcionada, se observa que el 53.85% de los encuestados está "de acuerdo" y el 46.15% está "totalmente de acuerdo" con la idea de que la colaboración internacional es esencial para superar desafíos legales en el tratamiento del ciberdelito del carding. Esto indica un respaldo significativo a la importancia de la colaboración internacional para abordar de manera efectiva los desafíos legales asociados con el carding. La tendencia general muestra una conciencia de la necesidad de trabajar en conjunto a nivel internacional con otros países para enfrentar eficazmente y lograr sancionar los delitos cibernéticos.

Tabla 10. El Ecuador debería participar de manera más activa a nivel internacional, especialmente suscribiendo tratados internacionales, para regular delitos digitales.

Opciones	Frecuencia	Porcentaje
De acuerdo	12	92.31%
Totalmente de acuerdo	1	7.69%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 9. El Ecuador debería participar de manera más activa a nivel internacional, especialmente suscribiendo tratados internacionales, para regular delitos digitales.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

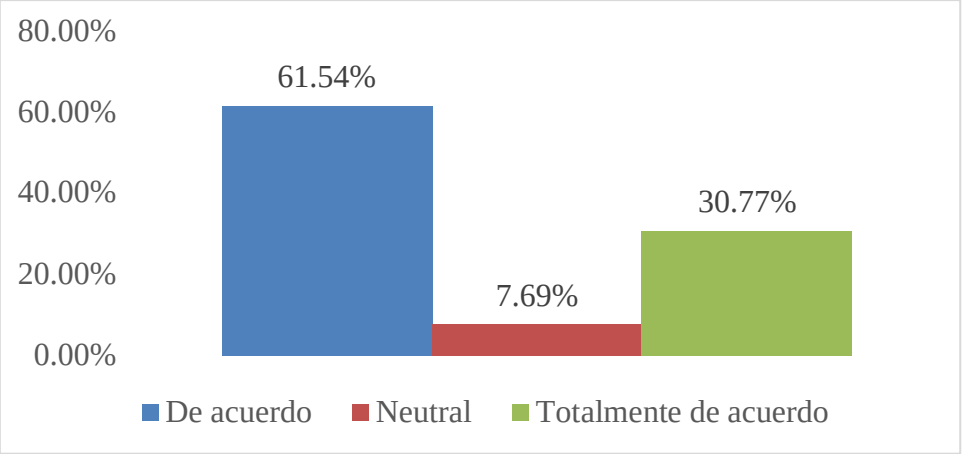
El análisis de la tabla refleja una perspectiva abrumadoramente favorable hacia la necesidad de que Ecuador tenga una participación más activa internacionalmente, especialmente en la suscripción de instrumentos internacionales para regular los delitos digitales. El 92.31% de los encuestados está "de acuerdo", mientras que el 7.69% está "totalmente de acuerdo". Estos resultados indican una clara percepción de que la cooperación internacional y la adhesión a tratados internacionales son esenciales para abordar los delitos digitales de manera efectiva. La mayoría de los participantes respalda la idea de fortalecer la colaboración y el compromiso a nivel internacional para mejorar la capacidad del Ecuador en la lucha contra los delitos digitales, sustancialmente contra aquellos como el carding.

Tabla 11. La jurisdicción, tanto nacional como extraterritorial, se presenta como un desafío al momento de sancionar a los delincuentes de carding.

Opciones	Frecuencia	Porcentaje
De acuerdo	8	61.54%
Neutral	1	7.69%
Totalmente de acuerdo	4	30.77%
Total general	13	100.00%

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Gráfico 10. La jurisdicción, tanto nacional como extraterritorial, se presenta como un desafío al momento de sancionar a los delincuentes de carding.



Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis:

El análisis de la tabla revela que el 61.54% de los encuestados están "de acuerdo" y el 30.77% están "totalmente de acuerdo" en que la jurisdicción nacional y extraterritorial presenta dificultades al momento de sancionar a los delincuentes del carding, dada la naturaleza transnacional de este delito. Este resultado sugiere la existencia de una preocupación significativa entre los participantes sobre los desafíos asociados con la jurisdicción al abordar el carding, y una proporción considerable sostiene una opinión más enfática al respecto. Por otro lado, el 7.69% adopta una postura "neutral", lo que indica que hay una minoría que no tiene una opinión clara o no se ha decidido sobre la dificultad de la jurisdicción en el tratamiento de los delitos de carding a nivel transnacional.

Análisis general de la encuesta a jueces:

El análisis de la tabla revela percepciones críticas sobre la legislación y el abordaje del ciberdelito del carding. El desacuerdo significativo con la adecuación de la normativa actual y la percepción de obstáculos derivados de la falta de claridad legal resaltan inquietudes sobre la eficacia de la legislación existente. Además, la preocupación sobre la adaptabilidad de las leyes actuales a la evolución tecnológica sugiere la necesidad de reformas ágiles. El consenso sobre la creación de políticas criminales digitales específicas para el carding y la identificación del desafío de la rápida evolución tecnológica subrayan la urgencia de enfoques más especializados y adaptables. La reconocida dificultad debido a la falta de conocimiento tecnológico de los jueces resalta la necesidad de capacitación judicial especializada para una efectiva aplicación de la ley en casos de carding. En general, se destaca una llamada a una legislación más clara y ágil, así como a enfoques judiciales mejor informados y especializados en el ámbito tecnológico para sancionar los delitos digitales.

4.3. Análisis de las perspectivas legales específicas que enfrentan los sistemas judiciales al tratar el ciberdelito del carding.

Tabla 12. Problemas que enfrenta el sistema judicial ecuatoriano.

	Jueces de Unidad Judicial Penal	**Jueces de Tribunal de Garantías Penales**	**Jueces de Sala Penal**
La falta de claridad en la legislación es un obstáculo para establecer sanciones en los delitos del carding	Sí, la falta de claridad dificulta la aplicación de sanciones adecuadas. Sí, por principio de legalidad, ya que, si no está en la norma no hay sanción. Sí, porque no existe definición sobre este delito en el COIP.	No, ya existe legislación para castigar el delito. No, se genera muchos tipos penales abiertos. No, ya existen elementos suficientes para el delito.	Sí, no existe una tipificación del delito en particular. Sí, no está tipificado el delito en la norma. Sí, hay una falta de tipificación del delito.
Las leyes penales son lo suficientemente ágiles para abordar la evolución de las tecnologías de carding	No, la efectividad de las leyes depende de su adaptación a las tecnologías. No, aún no se contemplan varios delitos. No, porque estamos atrasado en la tecnología en todo aspecto.	Sí, existen leyes que sancionan los ciberdelitos. Sí, el derecho debe responder a hechos ya sucedidos. Sí, existe elementos adjetivos ágiles para estos delitos.	No, las leyes penales no son evolutivas de manera uniforme. No, las leyes penales no evolucionan de manera inmediata. No, las normas no evolucionan al ritmo de la ejecución de los delitos digitales.
Es necesario de la creación de políticas criminales digitales para regular los ciberdelitos, como el carding	Sí, estas políticas son necesarias para establecer medidas preventivas y sanciones. Sí, porque requiere atención estatal para prevenir y erradicar estos delitos. Sí, pues es un delito relativamente nuevo y la ciudadanía requiere seguridad.	Sí, además se debería crear unidades especializadas en la Policía Nacional manejadas por inteligencia para tratar estos delitos. Sí, pues se permite prevenir estos delitos. Sí, para prevenir toda forma de este delito.	Sí, para permitir la especificación del delito. Sí, para delimitar apropiadamente el tipo penal. Sí, pues permite la especificación aplicable del delito.

Nota: *Encuesta dirigida a jueces penales en el cantón Riobamba, provincia de Chimborazo.*
Fuente: *Elaboración propia.*

Análisis general:

El análisis de las respuestas proporcionadas por los señores/as jueces/zas de la unidad judicial penal, del tribunal de garantías penales y de la sala penal con sede en el cantón Riobamba, provincia de Chimborazo, evidencia una diversidad de perspectivas en relación con la claridad de la legislación, la agilidad de las leyes penales y la necesidad de políticas criminales digitales para abordar los ciberdelitos, específicamente el carding como problemáticas que enfrentan los sistemas judiciales en la actualidad.

Con respecto a la falta de claridad en la legislación en relación con los delitos de carding, existen criterios diferentes. Mientras que, los jueces de sala y de unidad penal consideran que la falta de claridad dificulta la aplicación de sanciones adecuadas y abogan por la necesidad de una tipificación más específica del delito, los jueces de tribunal de garantías penales argumentan que ya existe legislación suficiente y que la falta de claridad no es un obstáculo significativo.

En lo que refiere a la agilidad de las leyes penales para abordar la evolución de las tecnologías de carding, las respuestas varían. Aunque los jueces de sala y unidad penal reconocen la necesidad de leyes más ágiles y específicas para hacer frente a los delitos digitales en constante evolución, por el contrario, los jueces de tribunal de garantías penales consideran que las leyes existentes son suficientes y que la adaptabilidad depende de la interpretación y aplicación efectiva de dichas leyes.

En cuanto a la creación de políticas criminales digitales para regular los ciberdelitos, existe consenso en la necesidad de estas políticas para establecer medidas preventivas y sanciones. Al respecto, se destacan opiniones que sugieren que la prevención y erradicación de estos delitos podría lograrse mediante la creación por parte del Estado de unidades especializadas en la Policía Nacional manejadas por inteligencia y la especificación adecuada del tipo penal como enfoques complementarios para abordar este fenómeno delictivo.

Los criterios proporcionados por los administradores de justicia reflejan la complejidad y la diversidad de perspectivas entre los diferentes jueces penales en relación con la claridad de la legislación, la constante agilidad que debe tener las leyes penales con la tecnología y la necesidad de políticas criminales digitales para abordar los ciberdelitos, particularmente el carding.

4.4.Propuesta de reforma al Código Orgánico Integral Penal para tipificar el ciberdelito del carding

REPÚBLICA DEL ECUADOR

EL PLENO DE LA ASAMBLEA NACIONAL DEL ECUADOR.

CONSIDERANDO

Que, la Constitución de la República fue publicada en el Registro Oficial No. 449 de 20 de octubre de 2008.

Que, el artículo 75 de la Constitución de la República, consagra que, "Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión".

Que, el artículo 76 garantizan a toda persona el derecho al debido proceso consagrado como una serie de garantías básicas que deben ser cumplidas en el ejercicio de cualquier acción dentro del marco constitucional del país.

Que, el artículo 82 de la Constitución de la República, consagra el derecho a la seguridad jurídica basado en el respeto a la Constitución y a las normas legales, jurídicas, claras públicas y aplicadas por las autoridades competentes. Garantizando la inexistencia de abuso de poder de ninguna autoridad.

Que, el artículo 167 de la Constitución establece que la potestad de administrar justicia la ejercen los órganos jurisdiccionales de la Función Judicial.

Que, el artículo 169 de la Constitución establece que, "El sistema procesal es un medio para la realización del justicia. Las normas procesales consagrarán los principios de simplificación, uniformidad, eficacia, inmediación, celeridad y economía procesal, y harán efectivas las garantías del debido proceso".

Que, el artículo 424 de la Constitución de la República enuncia el principio universalmente vigente de supremacía constitucional. Pues, nada puede regir por encima de la Constitución y, en caso de conflicto dispone el artículo 425 se aplica la norma jerárquica superior.

Que, el ordenamiento jurídico debe ser único, coherente y completo.

Que, existen contradicciones y ambigüedades que obligan a precisarlas.

Que, hay vacíos normativos que deben ser llenadas en miras a garantizar plenitud y seguridad jurídica.

Que, es evidente que en algunos artículos vigentes se ha incurrido en errores de técnica legislativa.

En ejercicio de las atribuciones contenidas en el artículo 120 numeral 6 de la Constitución de la República del Ecuador y el artículo 9 numeral 6 de la Ley Orgánica de la Función Legislativa, expide la siguiente:

LEY ORGÁNICA REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL

Art. 186

SUPRÍMASE:

Art. 1.- Suprímase el numeral 1 y 2 del artículo 186.

AGRÉGASE:

Art. 2. – Agrégase a continuación del artículo 186, el siguiente artículo:

"Art 186.1. – Carding. – La persona que, manipulando fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para apropiarse de los datos de la tarjeta de crédito, débito, pago o similares de un tercero, defraude, sustraiga o transfiera los valores, con el propósito de obtener un beneficio patrimonial para sí mismo o para una tercera persona, será sancionada con una pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. *Defraude, sustraiga o transfiera valores haciendo uso de una tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.*
2. *Defraude, sustraiga o transfiera valores mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares."*

Art. 190

REFÓRMASE

Art. 3. – Refórmese el inciso primero del artículo 190, de la siguiente manera:

"Art. 190.- Apropiación fraudulenta. – La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes o derechos en perjuicio

de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.”

4.5. Discusión de resultados

Conforme al análisis a través de un enfoque de Derecho Comparado del ciberdelito del carding para determinar su regulación jurídica, los autores Castro y Elizalde (2021) y Sambodo y Wahyuningsih (2021), concuerdan de que la materialización de los ciberdelitos en la actualidad y en especial el de carding se manifiestan por medios electrónicos, aspecto de esta actividad delictiva que de acuerdo con la investigación reside en el desconocimiento de la mayoría de las víctimas las cuales mantienen sus conocimientos tecnológicos muy discretos y son fáciles de engañar. Bajo esta misma línea de investigación, Muharam y Bundianto (2021) resaltan que, la existencia de la falta de leyes penales suficientes para regular específicamente este tipo de actividad delictual, criterio el cual coincide esta investigación realizada, debido a la escasa regulación jurídica de los Estados y la falta de auxilio internacional con tratados gubernamentales.

La revisión teórica de los autores Arifin et al. (2020) y Marbun & Setiyono (2023) muestra que el carding es un delito que surge de otros delitos como la estafa, fraude, lavado de dinero y robo de identidad, pero se distingue, en su verbo rector que yace en el defraude a través de internet que implica la obtención ilícita de la información de las tarjetas de crédito. Esta conclusión implica evidentemente el uso de sistemas o programas de software malicioso o malware diseñados para hackear. Además, los autores Marbun & Setiyono (2023) resaltan que a más de lo expuesto este ciberdelito debe estar penalizado como una forma de obtención y uso ilegal de la información de las tarjetas magnéticas utilizando técnicas de ingeniería social, comúnmente el *phishing, skimming y cashing.*

Partiendo de esta premisa, es notable el cambio que tiene otras jurisdicciones con respecto al Ecuador, como lo menciona Farto Crespo (2021) el código penal ecuatoriano no maneja la tipicidad del carding como una infracción propia y lo engloba como parte del delito de estafa dejando la mayoría de los casos en esta índole en la impunidad. Esta discrepancia es notable con otras legislaciones estudiadas, pues, de acuerdo con Spiezia (2022) la firma de convenios internacionales como El Convenio internacional sobre la ciberdelincuencia de Budapest (2004), es importante para la implementación de estrategias efectivas en contra de los perpetradores cibernéticos, argumentado que el lugar de operación de los infractores suele ser distinto al de la víctima.

Del estudio jurídico comparado y crítico del ciberdelito del carding para determinar sus bases jurídicas como tipo penal, Juca-Maldonado y Medina-Peña (2023) consideran que es fundamental implementar leyes propias en cada país para enfrentar este tipo de ciberdelitos, este criterio se apega al establecimiento del tipo penal en otras legislaciones como: La Ley Federal en contra del Fraude Electrónico de Estados Unidos (2006), El Reglamento Gubernamental Nro. 71 de Indonesia (2019) y La Ley de Uso Indebido de Computadoras de Reino Unido (1990). Estas legislaciones se caracterizan por juzgar al carding de manera individual, sin estar dentro de otros tipos penales, evidenciándose así, la carente regulación jurídica del Ecuador, misma que, lo ha puesto en el ojo del huracán frente a los delitos cibernéticos, a comparación de otras naciones que han implementado normativa especializada ante estas infracciones de manera eficaz.

En el análisis de la relevancia jurídica del ciberdelito del carding en el ámbito digital, basado en la encuesta dirigida a los 13 juzgadores penales con sede en el cantón Riobamba, provincia de Chimborazo, se ha determinado una percepción en torno al tratamiento jurídico de este fenómeno delictual. La discrepancia notoria en cuanto a la adecuación de la normativa actual refleja obstáculos derivados, como la ineficacia de las leyes existentes y la falta de claridad legal para abordar este tipo de delito. Además, la carente adaptabilidad de las leyes actuales a la evolución tecnológica subraya la necesidad apremiante de reformas ágiles para seguir el ritmo de los avances en el carding. Los hallazgos de estos resultados coinciden con las afirmaciones de los autores Gómez Fonseca (2023) y Castro y Elizalde (2021) quienes sostienen que el impacto de las tecnologías trae consigo el surgimiento de nuevas formas delictivas, exigiendo una adaptación constante de la normativa jurídica por parte del Estado para sancionar estas conductas y prevenir daños en la sociedad.

Conjuntamente, el reconocimiento de la dificultad derivada de la falta de conocimiento tecnológico de los jueces destaca la importancia de la capacitación judicial especializada para garantizar una aplicación efectiva de la ley en casos de carding. Asimismo, la necesidad urgente de una participación más activa del país en la colaboración internacional se revela como un elemento crucial para superar desafíos, especialmente en el ámbito de la jurisdicción y abordar el ciberdelito de carding. En esa línea, Toro-Álvarez (2023) señala que la complejidad de los delitos cibernéticos radica en su carácter transnacional, requiriendo la participación de organismos públicos y privados. Concordantemente los autores Peters y Hindocha (2020), Evdokimov & Hobonkova (2022) y Nahorniuk-Danyliuk et al. (2022) sostienen que, por su compleijidad, los ciberdelitos trascienden las barreras nacionales a través de varias jurisdicciones, por lo cual, es imperativo una mayor coordinación y asistencia entre organismos y organizaciones internacionales e intergubernamentales para combatir eficazmente la ciberdelincuencia.

En el análisis de las respuestas de los jueces penales para identificar las perspectivas legales específicas que enfrentan los sistemas judiciales en el tratamiento del ciberdelito del carding, se revela una diversidad de opiniones en torno a la adecuación de la normativa actual. Se evidencia un desacuerdo significativo, esencialmente en lo referente a la falta de claridad legal y la agilidad de las leyes penales frente a la evolución tecnológica. Los jueces de sala penal y unidad penal perciben la falta de claridad como obstáculo para sancionar el ciberdelito y reconocen la necesidad de leyes más agiles para enfrentar los delitos digitales. En contraste, los jueces de tribunal de garantías penales sostienen que la legislación actual es suficiente, dependiendo de una interpretación y aplicación efectiva de las leyes existentes. Sobre esta discrepancia, se concuerda totalmente con el criterio de los jueces de sala y unidad penal, y se alinea con las posiciones de los autores Ángulo (2023) y García-Brito y Arciniegas-Castro (2023) quienes resalta que la escasa regulación normativa y los vacíos legales vulneran los derechos de los implicados, debiéndose actualizar la legislación con una reforma al COIP para abarcar los delitos cibernéticos y no dejarlos en la impunidad.

En cuanto a la necesidad de políticas criminales digitales específicas para abordar el carding recibe un respaldo general entre los jueces, quienes coinciden en la necesidad de

estas políticas para establecer medidas preventivas y sanciones. Esta perspectiva concuerda con los planteamientos de los autores Juca-Maldonado & Medina-Peña (2023), quienes ya han señalado que, a pesar de las iniciativas y políticas públicas implementadas en Ecuador para fortalecer la seguridad digital, estas han sido insuficientes. Por ende, es fundamental considerar las sugerencias de los juzgadores, enfocándose en la institución de unidades especializadas de la Policía Nacional y la especificación adecuada del tipo penal como enfoques complementarios para abordar el ciberdelito del carding.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El análisis comparativo de la normativa sobre el carding en Ecuador, Estados Unidos, Indonesia y Reino Unido muestra diversas perspectivas y desafíos legales. Como parte de los resultados se observa una escasa legislación de este ciberdelito por parte del Ecuador a comparación de las otras naciones investigadas, la falta de una ley específica que sancione este tipo de conductas criminales convierte al Ecuador en un blanco fácil para la propagación de la ciberdelincuencia. Es imprescindible para el país la cooperación internacional y la suscripción de tratados internacionales para la regulación del carding, especialmente por la naturaleza transnacional de este ciberdelito.
- El exhaustivo estudio de la relevancia jurídica del ciberdelito del carding, basado en la encuesta a los jueces penales en Riobamba, Chimborazo, revela una significativa discrepancia de opiniones y una percepción compartida sobre los desafíos vinculados a la normativa actual. Los obstáculos evidentes, como la ineficacia y la falta de claridad legal, subrayan la imperante exigencia de reformas legislativas ágiles que se adapten a la rápida evolución tecnológica.
- Acerca de las perspectivas legales específicas relacionadas con el tratamiento del ciberdelito del carding revelan un evidente desacuerdo en la percepción sobre la adecuación de la normativa vigente. Las divergencias de los juzgadores coinciden con las posturas de los autores quienes subrayan la necesidad de actualizar la legislación para abordar los delitos cibernéticos y prevenir la impunidad. La demanda de políticas criminales digitales específicas para abordar el carding recibe respaldo unánime tanto por los juzgadores como por los autores dada la insuficiencia de las actuales iniciativas en Ecuador para combatir los ciberdelitos especialmente el carding.
- Finalmente, el ciberdelito del carding en Ecuador se manifiesta de forma predominante a través de medios electrónicos, explotando el desconocimiento tecnológico de las víctimas, aprovechando directamente la falta de legislación penal adecuada para abordar específicamente este tipo de delito y resaltando la falta de cooperación internacional mediante tratados internacionales.

5.2. Recomendaciones

Se propone al Estado ecuatoriano considerar la urgente necesidad de fortalecer la cooperación internacional y la armonización de su legislación para abordar de manera más efectiva el ciberdelito del carding. Esto implica la suscripción de tratados internacionales que faciliten la colaboración entre países en la lucha contra estos delitos, así como la revisión y actualización constante de las leyes nacionales.

Se recomienda a la Asamblea Nacional del Ecuador implementar reformas legislativas ágiles y específicas que aborden el ciberdelito del carding con el único fin de subsanar la falta de claridad y la ineficacia de las leyes existentes con relación a este delito. Esto debido a que, en el Ecuador a través de este estudio se ha determinado la impunidad de múltiples casos con relación a los ciberdelitos por la falta de leyes específicas.

Se insta al Consejo de la Judicatura a fortalecer la capacitación judicial especializada para superar las dificultades derivadas de la falta de conocimiento tecnológico de los servidores judiciales. Dada la naturaleza de los delitos cibernéticos, se sugiere una participación más activa por parte de los jueces, enfocándose en una mayor instrucción con relación al surgimiento de nuevos delitos tecnológicos.

Por último, se recomienda considerar las propuestas sobre la imperante necesidad de crear políticas criminales digitales específicas para abordar el carding y se sugiere respaldar la instauración de unidades especializadas en la Policía Nacional, en consonancia con las sugerencias de los jueces, para fortalecer la respuesta judicial frente al tratamiento de este ciberdelito.

BIBLIOGRAFÍA

Ali, A. (2021). *International Journal of advanced humanities Research" (IJAHR) Cyberspace and Organized Crime: The New Challenges of the 21st Century*. https://ijahr.journals.ekb.eg/

Angulo, S. (2023). *El auge del cibercrimen en el país dispara el interés por los seguros*. Expresso. https://www.expreso.ec/actualidad/economia/auge-cibercrimen-pais-dispara-interes-seguros-168387.html

Arellano Cruz, J. L., & Mendivil Cortez, C. V. (2020). Teoría Del Delito Y Teoría Del Caso. *Revista de Investigación Académica Sin Frontera: División de Ciencias Económicas y Sociales*, *33*, 1–43. https://orcid.org/0000-0003-0803-5518

Arifin, R., Atikasari, H., & Waspiah. (2020). *Article History The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud*. *11*, 235–246.

Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. *Registro Oficial 449 de 20-Oct.-2008*, 1–217.

Asamblea Nacional Constituyente. (2014). Código Orgánico Integral Penal. *Registro Oficial Nº 180 de 10-Feb.-2014*, 1–144.

Asamblea Nacional de la República del Ecuador. (2022). *Memorando Nro. AN-CRIM-2022-0012-M sobre el Informe favorable del Tratado entre la República del Ecuador y la República Popular de China sobre asistencia legal mutua* (Issue 593).

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Revista Amazonia Investiga*, *10*(38), 113–122. https://doi.org/10.34069/ai/2021.38.02.10

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. *The Encyclopedia of Criminology and Criminal Justice*, 1–5. https://doi.org/10.1002/9781118517383.wbeccj244

Campbell-Kelly, M., & Garcia-Swartz, D. D. (2005). The history of the internet: The missing narratives. *Journal of Information Technology*, *28*(1), 18–33. https://doi.org/10.1057/jit.2013.4

Castro, B., & Elizalde, D. (2021). *LOS CIBERDELITOS Y SU TIPIFICACIÓN EN EL CÓDIGO ÓRGANICO INTEGRAL PENAL*.

Chou, C. H. (2022). Software Cracking and Degrees of Software Protection. *B.E. Journal of Theoretical Economics*, *23*(2), 577–600. https://doi.org/10.1515/bejte-2021-0029

Commission of the European Communities. (2007). *Towards a General Policy on the Fight Against Cybercrime*. Brussels: Commission of the European Communities. https://eur-lex.europa.eu/EN/legal-content/summary/towards-a-general-policy-on-the-fight-against-cybercrime.html

Council of Europe. (2001). *Convenio sobre la Ciberdelincuencia*. 1–26.

Esteve Molto, J. E. (2020). Crimen internacional y jurisdicción penal nacional: de la justicia universal a la jurisdicción penal interestatal. *Anuario Español de Derecho Internacional*, *36*, 526–529. https://doi.org/10.15581/010.36.39688

Evdokimov, K. N., & Hobonkova, K. V. (2022). On the problem of improving international cooperation in countering cybercrime. *Siberian Law Herald*, *3*(98), 90–95.

https://doi.org/10.26516/2071-8136.2022.3.90

Fahamsyah, E., Taniady, V., Rachim, K. V., & Riwayanti, N. W. (2022). Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention. *De Jure: Jurnal Hukum Dan Syar'iah*, *14*(1), 140–159. https://doi.org/10.18860/j-fsh.v14i1.15731

Farto Crespo, H. (2021). El delito de estafa en el Código Orgánico Integral Penal. Breve análisis del tipo penal y las reformas del 2019. *Revista Derecho Penal Central*, *III*(3), 157–170.

Fiscalía General del Estado. (2013). *Instructivo de cooperación penal internacional*. 1–164.

García Brito, P. J., & Arciniegas Castro, C. L. (2023). Las nuevas tecnologías frente al código orgánico integral penal. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *4*(4), 116–127. https://doi.org/10.56712/latam.v4i4.1202

Geiran, V. (2022). Improving interagency collaboration, innovation and learning in criminal justice systems: supporting offender rehabilitation. S.Hean, B.Johnsen, A.Kajamaa & L.Kloetzer (Eds.) Cham, Switzerland: Palgrave Macmillan/Springer Nature Switzerland AG. 2021. 475p. *The Howard Journal of Crime and Justice*, *61*(3), 399–401. https://doi.org/10.1111/hojo.12491

Giménez Solano, J. V. (2011). *Hacking y ciberdelito*. 123.

Gómez Fonseca, J. (2023). *El ciberdelito: un necesario agravante de la estafa en el código penal colombiano*. 1–106.

Juca-Maldonado, F., & Medina-Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Revista Científica Portal de La Ciencia*, *4*(2), 325–337. https://doi.org/https://doi.org/10.51247/pdlc.v4i3.394

Kamalova, G. G. (2020). Some Questions of Criminal Legal Responsibility in the Field of Application of Artificial Intelligence Systems and Robotics. *Bulletin of Udmurt University. Series Economics and Law*, *30*(3), 382–388. https://doi.org/10.35634/2412-9593-2020-30-3-382-388

Manaf, I. (2023). *Carding Crime Analysis as A Form of Cyber Crime in Indonesia's Criminal Law*. *01*(01), 1–7. https://doi.org/10.4108/eai.16-4-2022.2320085

Marbun, T. S., & Setiyono, J. (2023). The Criminal Law Policy against Carding's Crimes as a Form of Cyber Crime. *International Journal of Social Science and Human Research*, *06*(07), 4521–4526. https://doi.org/10.47191/ijsshr/v6-i7-83

Meijerink, T. J. (2013). Carding. Crime prevention analysis Tristan. In *Bachelor's thesis, University of Twente* (Vol. 165, Issue DEC30).

Mejía Lobo, M., Hurtado Gil, S. V., & Grisales Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociais*, *XXIX*(2), 356–372.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional De Ciberseguridad Del Ecuador*.

Morán Giler, M. C., Arandia Zambrano, J. C., & Del Pozo Carrasco, J. G. (2022). Análisis de los elementos constitutivos del delito de estafa; estudio España y Ecuador. *Dilemas Contemporáneos: Educación, Política y Valores*, 1–40. https://doi.org/10.46377/dilemas.v10i18.3450

Muharam, N., & Budianto, A. (2022). *Carding Crime Analysis as A Form of Cyber Crime*

in Indonesia's Criminal Law. https://doi.org/10.4108/eai.16-4-2022.2320085

Nahorniuk-Danyliuk, O., Trach, S., Rossokxa, S., Tsutskiridze, M., & Yermakov, Y. (2022). Use of specific forms of international cooperation in special criminal proceedings. *Revista Amazonia Investiga*, *11*(58), 57–64. https://doi.org/10.34069/ai/2022.58.10.6

Office of the Law Revision Counsel of the House of Representatives. (2006). 18 U.S.C. § 1028. *Public Law 118-39*, 1–76.

Oxford. (2024a). *Definition of card noun*. Oxford Learner's Dictionaries.

Oxford. (2024b). *Definition of cybercrime noun*. Oxford Learner's Dictionaries.

Parliament of the United Kingdom. (1990). Computer Misuse Act. *1990 CHAPTER 18*, *18*, 20. https://doi.org/10.4324/9781843143024-67

Fraud Act, 2006 CHAPTER 35 19 (2006). https://doi.org/10.4324/9780203759776-17

Peters, A., & Hindocha, A. (2020). *Third Way US Global Cybercrime Cooperation: A Brief Explainer*. https://about.jstor.org/terms

Policía Nacional del Ecuador. (2015). *Delitos Informáticos o Ciberdelitos*. https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/

Quevedo González, J. (2017). *Investigación y prueba del ciberdelito Programa de Doctorado en Derecho y Ciencia Política Línea de Investigación : Derecho procesal*. 505. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Real Academia Española. (2024). *Definición de "ciberdelito."* Asociación de Academias de La Lengua Española.

Sambodo, C. G., & Wahyuningsih, S. E. (2021). The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions. *Law Development Journal*, *3*(2), 240. https://doi.org/10.30659/ldj.3.2.240-247

Santos Villareal, G. M. (2010). La Corte Penal Internacional. *Cámara de Diputados*.

Sekretariat Negara. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71. *Media Hukum*, 90.

Spesivov, N. V. (2023). From Fantastic Theories to Objective Reality: Is there Future for Artificial Intelligence and Predictive Technologies in Administration of Criminal Justice? *Lex Russica*, *76*(2), 81–90. https://doi.org/10.17803/1729-5920.2023.195.2.081-090

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum*, *23*(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

Tarhan, K. (2022). Historical Development of Cybersecurity Studies: a Literature Review and Its Place in Security Studies. *Przeglad Strategiczny*, *15*, 393–414. https://doi.org/10.14746/ps.2022.1.23

Toro-Álvarez, M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. *Revista Logos Ciencia & Tecnología*, *15*(2), 162–173.

United Nations. (2000). Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna , 10-17 April 2000. *Crimes Related to Computer Networks*, *90954*(July), 1–15.

United Nations. (2020). *14th United Nations Congress Congress on Crime Prevention and*

Crime Prevention and Criminal Justice (Vol. 50611).

United States Government Accountability Office. (2007). *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*. *June*. http://www.gao.gov/products/GAO-07-705

UNODC. (2013). UNITED NATIONS OFFICE ON DRUGS AND CRIME. Vienna. Comprehensive Study on. Cybercrime. Draft. February 2013. UNITED NATIONS. *United Nations Office on Drugs and Crime*, *February*, 1–320. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC. (2024). *Sharing Electronic Resources and Laws on Crime Portal*. United Nations Office on Drugs and Crime.

Van Hardeveld, G. J. (2018). *Deviating from the Cybercriminal Script: Exploring the Contextual Factors and Cognitive Biases Involved in Carding*. *September*.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1–2), 63–72. https://doi.org/10.1365/s43439-020-00012-5

Zambrano Pasquel, A. (2023). *Manual de Derecho Procesal Penal y Técnicas de Litigación* (Tomo I). Corporación de Estudios y Publicaciones.

6. ANEXOS

6.1. Validación del instrumento

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Dr. Béquer Carvajal Flor.
Especialidad: Derecho Penal
Titulo de la investigación: La regulación jurídica del carding en atención del Derecho Comparado.
Objetivo del instrumento: Evaluar la relevancia jurídica del abordaje del carding e identificar los preceptos legales internacionales que enfrenta el sistema judicial.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún item)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no escencial	No Importante	
1	/		/		/		/		/			
2	/		/		/		/		/			
3	/		/		/		/		/			
4	/		/		/		/		/			
5	/		/		/		/		/			
6	/		/		/		/		/			
7	/		/		/		/		/			
8	/		/		/		/		/			
9	/		/		/		/		/			
10	/		/		/		/		/			

Firma de Validador
Nombre: BECQUER CARVAJAL FLOR.
Cèdula: 0999245092.

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Dr. Danny Silva Conde
Especialidad: Derecho Penal
Titulo de la investigación: La regulación jurídica del carding a través del derecho comparado.
Objetivo del instrumento: Evaluar la relevancia jurídica del cibe-delito del carding e identificar los preceptos legales internacionales que enfrenta el sistema judicial

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún item)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no escencial	No Importante	
1	/		/		/		/		/			
2	/		/		/		/		/			
3	/		/		/		/		/			
4	/		/		/		/		/			
5	/		/		/		/		/			
6	/		/		/		/		/			
7	/		/		/		/		/			
8	/		/		/		/		/			
9	/		/		/		/		/			
10	/		/		/		/		/			

Firma de Validador
Nombre: Danny Silva Conde
Cèdula: 0604509968

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Edison Bonifaz
Especialidad: Investigación Jurídica.
Titulo de la investigación: La regulación jurídica del ciberdelito del carding a través del derecho comparado.
Objetivo del instrumento: Evaluar la relevancia jurídica del ciberdelito del carding e identificar las perspectivas legales internacionales que enfrenta el sistema judicial.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún ítem)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no escencial	No Importante	
1	/		/		/		/		/			
2	/		/		/		/		/			
3	/		/		/		/		/			Colocar Jurisdicción
4	/		/		/		/		/			"
5	/		/		/		/		/			"
6	/		/		/		/		/			
7	/		/		/		/		/			
8	/		/		/		/		/			
9	/		/		/		/		/			
10	/		/		/		/		/			
11	/		/		/		/		/			
12	/		/		/		/		/			
13	/		/		/		/		/			
14	/		/		/		/		/			
15	/		/		/		/		/			
16	/		/		/		/		/			

Firma de Validador
Nombre: Edison Bonifaz
Cèdula: 060303 2009.

6.2. Cuestionario

Preguntas de interés de la investigación

Dimensión 1: Relevancia jurídica del ciberdelito del *carding*

1. ¿La normativa actual en el país aborda adecuadamente el ciberdelito del *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

2. ¿La falta de claridad en la legislación sobre el tipo penal es un obstáculo al establecer las sanciones a las personas que adecuan sus actos a los delitos del *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

3. ¿Las leyes penales actuales son lo suficientemente ágiles para seguir el ritmo de la evolución de las tecnologías de *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

4. ¿Es necesario la creación de políticas criminales digitales que regulen los ciberdelitos, concretamente los que atentan contra sistemas financieros como el *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Dimensión 2: Problemas que enfrentan los sistemas judiciales

5. ¿La rapidez con la que evolucionan las técnicas de *carding* plantea desafíos específicos para la legislación y los procedimientos judiciales? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

6. ¿Considera que la falta de conocimiento tecnológico de los jueces es un desafío para abordar el *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

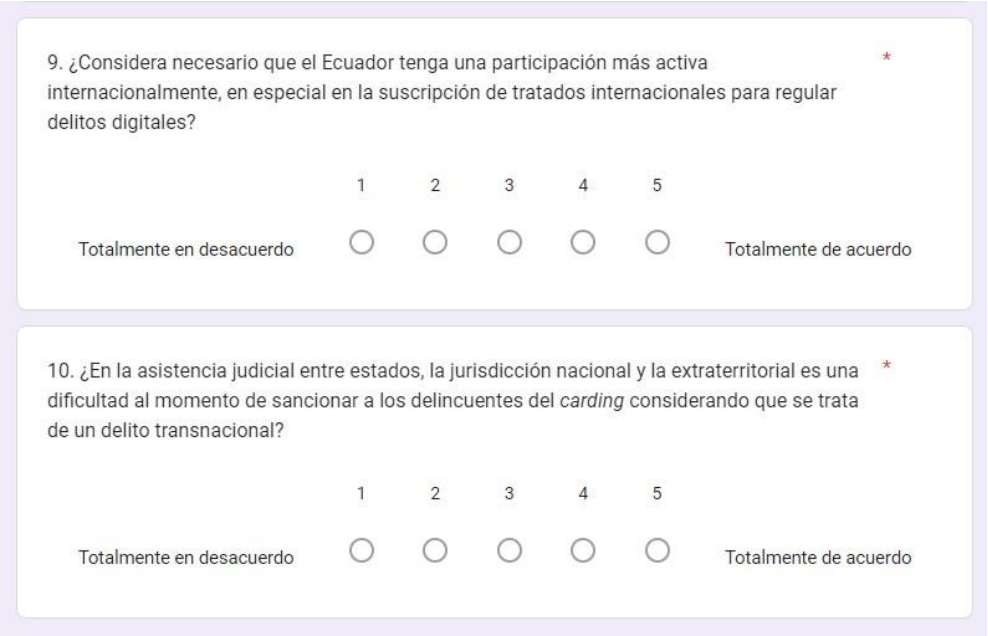
7. ¿Cree usted que se necesita una mayor capacitación judicial en temas técnicos y digitales para garantizar una efectiva aplicación de la ley en casos de *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

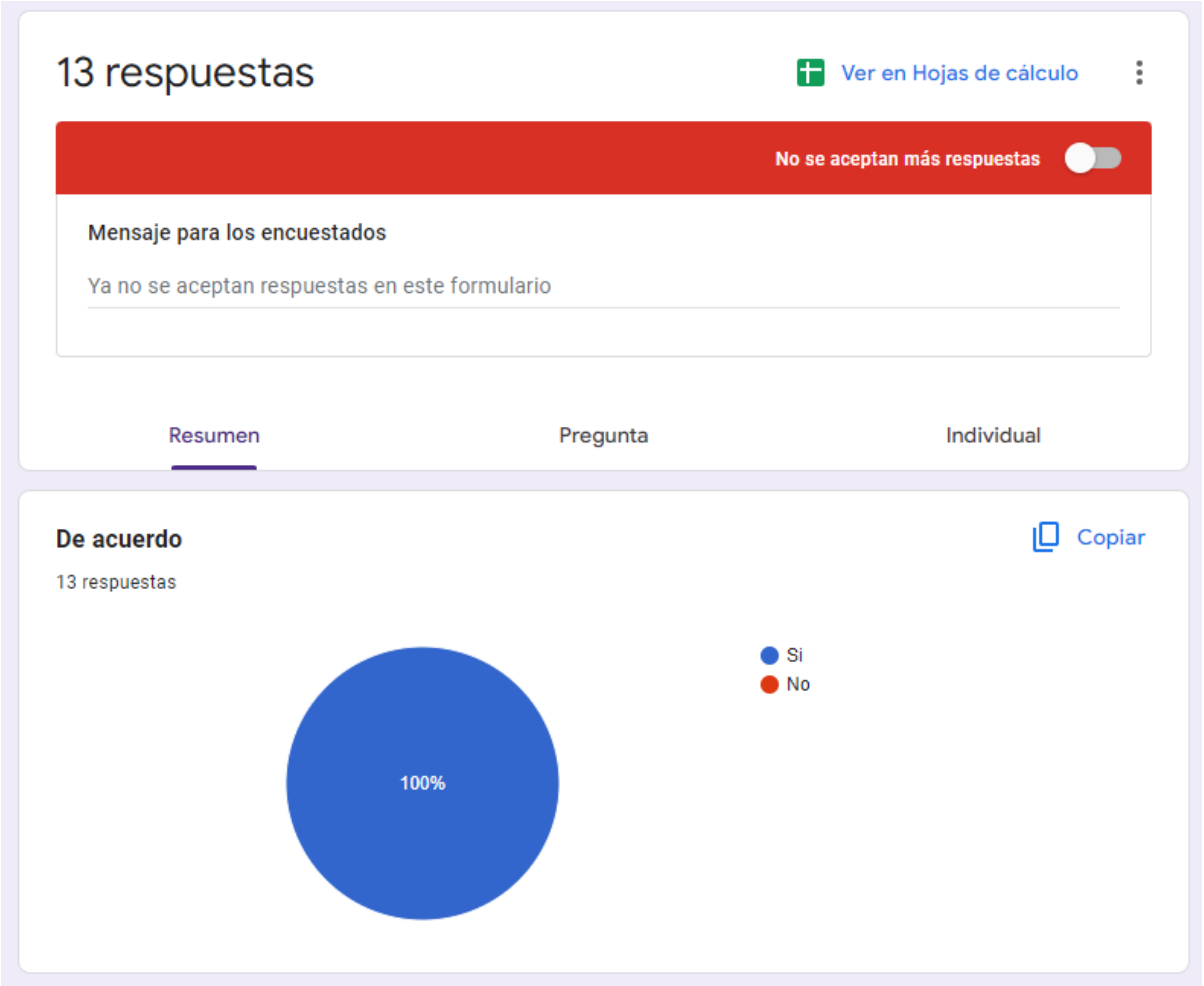
Dimensión 3: Colaboración internacional

8. ¿La colaboración internacional es esencial para superar desafíos legales en el tratamiento del ciberdelito del *carding*? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo



6.3. Aplicación del instrumento



La regulación jurídica del ciberdelito del *carding*

The form La regulación jurídica del ciberdelito del *carding* is no longer accepting responses. Try contacting the owner of the form if you think this is a mistake.