UNIVERSIDAD TECNOLOGICA ECOTEC

FACULTAD:

DERECHO Y GOBERNABILIDAD

TITULO:

“DIAGNÓSTICO DE LA SITUACIÓN JURÍDICA DE LA CIBERDELINCUENCIA EN EL ECUADOR EN EL PERIODO 2022”

LINEA DE INVESTIGACIÓN

GESTION DE LAS RELACIONES JURIDICAS

MODALIDAD DE TITULACION:

TRABAJO DE INVESTIGACIÓN

CARRERA:

DERECHO

TITULO A OBTENER:

ABOGADO

AUTOR:

ADRIÁN PAÚL GALÁN GUIZADO

TUTOR:

MGTR. ROGER NIETO

GUAYAQUIL 2023

DEDICATORIA

Este logro no habría sido posible sin su apoyo incondicional y amor constante. A ustedes, mis padres que han sido mi guía, mi hermana Nayeli que a su manera ha estado pendiente de mí, mi abuelita Nidia que se vive preocupando, pero su preocupación me llena de felicidad y a toda mi querida familia, les dedico con profundo cariño y gratitud este trabajo. Sus sacrificios, aliento y amor han sido la fuerza que me impulsó en este camino. Gracias por estar siempre a mi lado. A Mochi y a Oddie, donde quiera que estén.

AGRADECIMIENTO

A mis padres Wilman y Blanca, a Nidia, a mi hermana Nayeli, por su apoyo incondicional, por el tiempo que me regalaron para que yo sea capaz de tanto, por las pequeñas cosas que me motivan a seguir cada día, por el cariño, por un hogar amoroso, por los merecidos llamados de atención, por tanto, amor. Gracias.

A mis profesores por inspirarme y motivarme siendo personas profesionales y por ser catedráticos excepcionales con amor a la profesión. Gracias.

CERTIFICADO DE REVISION FINAL

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 7 de diciembre de 2023

Magíster
Andrés Madero Poveda
Decano de la Facultad
De Derecho
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: "Diagnóstico De La Situación Jurídica De La Ciberdelincuencia En El Ecuador En El Periodo 2022" según su modalidad PROYECTO DE INVESTIGACIÓN, PROPUESTA TECNOLÓGICA; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **Galán Guizado Adrián Paúl,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

Firmado electrónicamente por:
ROGER HECTOR NIETO MARIDUENA

Mgtr/ PhD.. Roger Nieto Maridueña

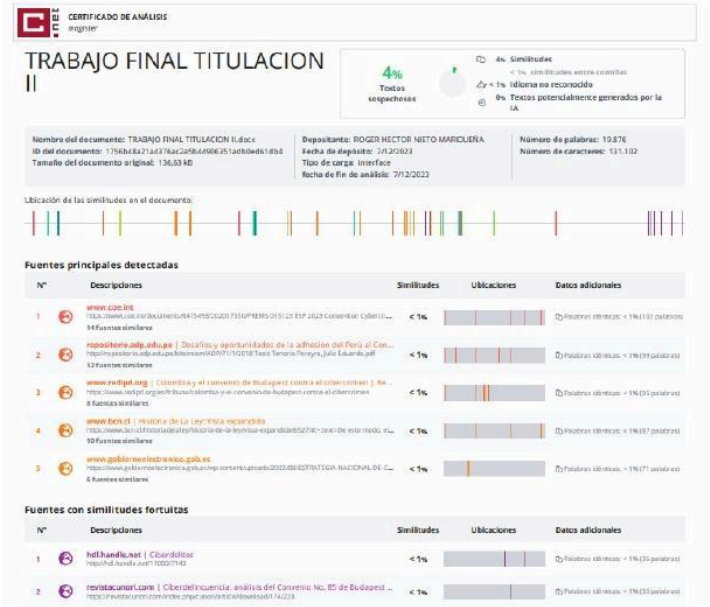
Tutor(a)

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Roger Nieto Maridueña, tutor del trabajo de titulación "Diagnóstico De La Situación Jurídica De La Ciberdelincuencia En El Ecuador En El Periodo 2022" elaborado por Adrián Paúl Galán Guizado , con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 4% mismo que se puede verificar en el siguiente link: (https://app.compilatio.net/v5/folder). Adicional se adjunta print de pantalla de dicho resultado.



Firmado electrónicamente por:
ROGER HECTOR NIETO MARIDUENA

FIRMA DEL TUTOR
Mgtr. ROGER NIETO MARIDUEÑA

RESUMEN

Este estudio examina la situación actual de Ecuador en el ámbito de la ciberseguridad, utilizando estadísticas proporcionadas por organismos internacionales especializados en este campo. Se analiza la implementación del Convenio Internacional de Budapest en el sistema judicial y sus implicaciones legales, incluyendo una comparación de las leyes que regulan los delitos informáticos en países de la región que han ratificado este convenio. Además, se incluyen entrevistas con profesionales legales que trabajan en este ámbito para obtener una perspectiva realista y profesional de la situación nacional en materia de ciberseguridad.

ABSTRACT

This study examines Ecuador's current situation regarding cybersecurity, utilizing statistics provided by international organizations specialized in this field. It analyzes the implementation of the Budapest International Convention within the judicial system and its legal implications, including a comparative analysis of laws regulating cybercrimes in countries within the region that have ratified this convention. Additionally, interviews with legal professionals working in this field are included to obtain a realistic and professional perspective on the national cybersecurity situation.

Índice de contenido

Introducción

Es inevitable hablar acerca de la tecnología cuando se trata del desarrollo de la humanidad, como lo plantea (Pérez Lindo, 1995), los avances tecnológicos nos conducen más allá de las normas naturales y culturales establecidas. Elementos como los miembros biónicos, la reproducción asistida, los robots con inteligencia artificial, los cultivos creados mediante ingeniería genética y los sistemas de información señalan que la humanidad se encuentra avanzando hacia un orden que va más allá de lo natural y lo cultural, un orden cuyo significado nos resulta esquivo. A este punto es correcto decir que los últimos grandes saltos en la humanidad se encuentran marcados por la tecnología, con esta comparación se marca la idea de lo involucrado que se encuentra la tecnología en los diferentes aspectos de la vida de los seres humanos, desde la medicina hasta el entretenimiento, y por supuesto, el derecho, como base importante de la sociedad contemporánea también se encuentra afectado, tanto como mecanismo del Estado, y más importante aún, como sistema regulador de la sociedad.

De acuerdo con un reportaje presentado por el diario El Comercio, los ataques perpetrados por grupos delictivos cibernéticos son habituales en la nación. Según un reporte numérico presentado por la Unidad de Ciberdelitos de la Policía, se han documentado 3,183 incidentes delictivos de índole informática desde el año 2020 hasta el 6 de julio de 2022. En el transcurso del año 2020, se registraron 682 casos; para el año 2021, la cifra ascendió a 1,851, y en poco más de seis meses de 2022, la Policía ha iniciado 650 investigaciones a nivel nacional. (El Comercio, 2022)

Es así que existe la rama del Derecho Penal conocida como “Delitos Electrónicos” que se encuentra positivizada en la legislación ecuatoriana en su

mayoría en el capítulo Tercero, “Delitos Contra El Buen Vivir”, sección tercera “Delitos Contra La Seguridad De Los Activos De Los Sistemas De Información Y Comunicación” y cuya finalidad es el sanciona miento de los delitos cometidos en entornos o espacios digitales.

Ecuador en esta materia se encuentra desconectado e incluso se podría decir desfasado en relación a los demás Estados, ya que no cuenta con la infraestructura cibernética para la correcta persecución de estos delitos, colaboración interinstitucional y al mismo tiempo, apoyo inter estados para afrontar este problema, considerando adicionalmente que a nivel normativo el país adolece de atrasos legislativos en materia tecnológica, esto se evidencia en el informe llamado Índice Global de Ciberseguridad presentado por la Unión Internacional de Telecomunicaciones, la cual es una agencia de las Naciones Unidas que se encarga de evaluar y asistir a los estados en temas de seguridad cibernética, en este informe ecuador ocupa el último lugar (19) en la evaluación en América por debajo de países como Belice o Venezuela e incluso por debajo de países que no presentaron toda la documentación solicitada por el organismo, además en el ranking mundial el país se ubica en el puesto No. 119 de 130, solo por encima de países como Mongolia, Iraq. (International Telecommunication Union, 2020)

Entonces es seguro decir que es necesario analizar el marco jurídico internacional dentro del cual se encuentra el convenio Budapest que regula la colaboración internacional, así como también sugiere una lista taxativa de delitos informáticos, mismo que no se encuentra ratificado por el Ecuador. (Observatorio del Principio 10, 2022)

El convenio mencionado fue firmado por más de 50 países en 2001, entró en funcionamiento el 2004, y se creó con la finalidad de Aumentar la colaboración con los demás países que son signatarios del Convenio, así como teniendo en cuenta los significativos cambios generados por la digitalización, la continua convergencia y la globalización de las redes informáticas, en otras palabras, con el fin de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. Por este motivo es indispensable que se realice la ratificación de este acuerdo, para de esta manera reforzar el sistema judicial y dar herramientas al Estado, así como apoyo, en la lucha contra la ciberdelincuencia. (Asociación Ecuatoriana de Ciberseguridad , 2021) (Consejo de Europa, 2001)

Adicional a lo antes mencionado, varios países latinoamericanos en mira de proteger los datos personales en línea de sus ciudadanos se han adherido / acogido a las disposiciones del presente convenio, sin embargo, a pesar de esfuerzos internos (de colectivos) no se ha suscrito al mismo, dejando en la impunidad una serie de delitos que van desde seguridad de bienes públicos, hasta delitos contra la sexualidad de menores.

De cara a lo antes mencionado, el objeto del trabajo radica en ddeterminar las consecuencias jurídicas de la aplicación del convenio internacional Budapest sobre la Ciberdelincuencia en el sistema judicial penal en Ecuador, lo cual, será posible por medio de determinar la situación jurídica actual con respecto a ciberdelincuencia, realizar comparación de legislaciones de países vecinos que son parte del convenio de Budapest, para lograr formular una propuesta de acciones de

mejoras encaminadas a la ratificación del convenio Budapest como instrumento para el combate de la ciberdelincuencia en el Ecuador.

Esto será posible mediante un estudio de corte no experimental por tratarse de un fenómeno jurídico de actualidad como lo es la ciberdelincuencia, con enfoque cualitativo de trabajo y métodos de deducción, explicación, análisis, y técnicas como la revisión literaria de textos académicos y legales, además de entrevistas a profesionales del tópico que mantienen una actividad laboral consistente, lo cual les permite tener una visión realista de la situación del derecho en materia de delitos electrónicos en el país.

Planteamiento del Problema

Ataque 2017 Ramsomware Wannacry

En mayo 12 del 2017 se produjo un ataque cibernético que puso en jaque a varios sistemas informáticos alrededor del mundo, afectando desde usuarios civiles individuales, hasta empresas multinacionales como Honda o Nissan. El ataque dejaba los equipos (Pc) inservibles mediante el secuestro de los mismos, los usuarios que sufrieron este ataque reportaron una variedad de efectos, desde el bloqueo de documentos hasta el bloqueo total de los equipos.

Ransomware, el cual es el virus que se utilizó para realizar este ataque, actúa encriptando archivos importantes impidiendo el acceso a ellos, o bloqueando el uso del computador para impedir su funcionamiento. Para devolver el control de los sistemas a los usuarios, así como para devolver la información secuestrada, los atacantes pedían, acorde a un reportaje de la BBC, un pago de $300 (Trecientos dólares americanos) en Bitcoin para asegurar su anonimato, sin embargo, la devolución de la información no siempre era exitosa ya que los atacantes, en algunos casos no tenían forma de acceder a los computadores atacados (BBC, 2017)

En el momento del ataque se reportaron infecciones en 99 naciones, entre las que se incluyen Rusia y China, así como FedEx Uno de los organismos más impactados fue el Servicio Nacional de Salud (NHS) en Inglaterra y Escocia, lo cual provoco la eliminación de la información de cientos de usuarios, así como el entorpecimientos de los servicios médicos, provocando el desvió de ambulancias, complicaciones en el traslado de pacientes, además de que los pacientes no podían recibir sus medicamentos. (BBC, 2017)

Con el tiempo las afectaciones de este ataque, acorde a un artículo presentado por Cloudflare, empresa de ciberseguridad, en su página web en 2021, expresan que el virus se extendió por más de 200 000 ordenadores en más de 150 países y se estima que provocó $4.000 millones (cuatro mil millones de dólares americanos) de costos en daños alrededor de todo el mundo. (Cloudflare, 2021)

A nivel Latinoamérica se encuentra el caso del país vecino Bolivia, que en su Ley Penal, se refiere a los delitos electrónicos en solo dos artículos en su legislación, el primero hace referencia al acceso ilícito y se refiere a este como "Manipulación Informática" en su artículo 363 bis., que en el mismo nos dice que, la persona que con el propósito de obtener un beneficio indebido, manipule la transferencia o el procesamiento de datos informáticos para obtener un resultado incorrecto o evitar un proceso que habría sido correcto, causando una pérdida económica a un tercero, enfrentará una pena de prisión de uno a cinco años y una multa de sesenta a doscientos días. (La Asamblea Legislativa Plurinacional, 1972)

En este articulado se pueden encontrar varios "vacíos" en cuanto a su composición si se la compara con legislaciones más avanzadas en este tópico, como ejemplo, no se hace mención o diferenciación de quien obtiene o de quien dispone de la información ilegalmente obtenida, al contrario, se podría decir que esta norma no califica la actividad del sujeto activo con la claridad necesaria del caso, además no hace referencia a aspectos como el sabotaje de sistemas empresariales mediante el uso de tecnología, el espionaje informático, el aprovechamiento indebido de recursos informáticos o a otras acciones específicas como el fraude electrónico dentro de su contenido.

Lo que se encuentra aparte de los dos artículos antes expuestos son dos tipificaciones en las cuales una, se encuentra en la ley Nº 393, en la cual se encuentra el artículo 477 en la que hala de la “Acción de protección de la privacidad” en la cual nos habla del derecho al acceso a la información personal y cuando esta violentado, además en el mismo nos deriva a la “Constitución Política del Estado” en la cual básicamente repiten lo explicado en el articulado y prosigue a hablar de cuando procederá una acción de protección de información.

Otro tipo de delito en esta normativa que se acerca al tema principal del presente trabajo se encuentra en el artículo 323 Bis. en el cual se establece el delito de la pornografía infantil en el cual se expresa que, quien, con la intención de grabar videos, tomar fotografías, filmar, mostrar o describir a través de sistemas informáticos, electrónicos o similares. y en su numeral primero del segundo párrafo, en el que se habla del agravamiento de la pena en los casos en los que la persona afectada sea un menor de edad o una persona con discapacidad, que si bien es cierto brinda castigo a esta conducta, no plantea un orden jurídico y es claro ver que el legislador no planea en desarrollar más el capítulo de delitos electrónicos en el código penal de este país. (La Asamblea Legislativa Plurinacional, 1972)

En razón de la falta de ratificación del Convenio Budapest sobre Ciberdelincuencia, la Asociación Ecuatoriana de Ciberseguridad (AECI) desde 2021, siendo consciente de las necesidades de seguridad informática en el país, ha llevado a cabo recolecta de firmas mediante la plataforma de change.org , y buscan cumplir la meta de 1.500 firmas y a la actualidad más de 1,290 personas han firmado, esto con la finalidad de dar difusión al mensaje, expandir conciencia acerca de la existencia de herramientas como el convenio, que pueden ser utilizadas por los estados ante la lucha contra la delincuencia informática, que abarca desde

terrorismo cibernético hasta actividades como el grooming (forma en la pederastas utilizan técnicas de engaño a través de entornos virtuales para acercarse a sus víctimas, siendo estas menores de edad) sea publicado en los medios de comunicaciones locales, esto acorde a la descripción que se encuentra en la propuesta presentada en la página de change.org, con lo anterior expuesto se da a notar que es necesario la ratificación del convenio y la creación de políticas que refuercen la ciber seguridad jurídica del país. (Asociación Ecuatoriana de Ciberseguridad , 2021)

Para mejorar la situación en el país es necesario, primero, la ratificación del convenio de Budapest ya que mediante y gracias a la finalidad de este es contar con el apoyo de la comunidad internacional, así como con la vinculación de fallos de cortes extranjeras en temas concernientes a materia penal, esto acorde a los artículos que se encuentran en el convenio. También es necesario que se adopten medidas legislativas y de otro tipo, como la creación de mecanismos o herramientas que faciliten la colaboración internacional como se establece en el propio Convenio Budapest, que puedan ser necesarias para la tipificación de delitos informáticos, tal como se encuentra en el artículo número 2 del artículo del convenio Budapest.

El cual establece que cada nación implementará las disposiciones legales y otras medidas pertinentes para establecer como un crimen en su jurisdicción el acceso intencional y no autorizado a la totalidad o parte de un sistema informático. Es posible que se requiera que la transgresión se realice infringiendo medidas de seguridad, con el propósito de adquirir datos informáticos u otros fines ilícitos, o en relación con un sistema informático vinculado a otro sistema informático. (Consejo Europeo, 2001)

Si bien es cierto la tecnología ya lleva más de una década en auge, también es sabido que las regulaciones a esta, así como a las formas de comunicación y de comercialización que el desarrollo de herramientas tecnológicas como el internet, han sido limitadas ya que el derecho al ser una de las ciencias sociales más antiguas que existen a la actualidad y a la importancia que esta tiene dentro de las instituciones de un estado, se suele ser reacio a la adaptación de estas nuevas tecnologías, así como a reconocer la importancia de la regulación de las mismas. Se tiene como ejemplos de esta importancia el ciber ataque sufrido por el Banco Pichincha en el 2021 el cual interrumpió las operaciones en las bancas virtuales, así como el caso del 14 de julio de este mismo año, en el cual la Corporación Nacional de Telecomunicaciones (CNT) fue víctima de un ataque el cual la puso en estado de emergencia institucional a una compañía tan grande y que pertenece al estado como lo es CNT, y estos son solo una prueba de lo importante que es la fortificación del sistema judicial.

Con esta investigación los resultados esperados son determinar si la ratificación del convenio de la ciberdelincuencia, Budapest, es una solución óptima y además si es viable de acuerdo a la normativa ecuatoriana. También se busca definir cuáles serían las consecuencias o resultados jurídicos que se obtendrían en el sistema judicial ecuatoriano teniendo como supuesto la ratificación del convenio por parte del país.

Para lograr estas metas se buscará realizar comparación de legislaciones con países vecinos y los que son parte del convenio Budapest, así como el análisis del convenio mismo para determinar la viabilidad de la ratificación del mismo.

La pregunta que desarrolla el problema y que se plantea para resolver en este trabajo de investigación es:

¿Qué consecuencias jurídicas acarrearía en el sistema penal ecuatoriano la aplicación del convenio internacional “Budapest” sobre ciberdelincuencia?

Objetivos

Objetivo General:

Determinar las consecuencias jurídicas de la aplicación del convenio internacional “Budapest” sobre la Ciberdelincuencia en el sistema judicial penal en Ecuador.

Objetivos Específicos

1.- Determinar la situación jurídica actual con respecto a ciberdelincuencia.

2.- Realizar comparación de legislaciones de países vecinos que son parte del convenio de Budapest.

3.- Formular una propuesta de acciones de mejoras encaminadas a la ratificación del convenio “Budapest” como instrumento para el combate de la ciberdelincuencia en el Ecuador.

Justificación:

Es imperante que el derecho se acople al paso del tiempo, y al desarrollo de nuevas tecnologías que requieran regulación por parte del Estado, además es de tomar en cuenta que, a diferencia de otras materias penales, los delitos electrónicos están en constante cambio ya que con cada nueva herramienta tecnológica se crean nuevas formas de cometer delitos

La difusión de imágenes y/o ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad se empezaron a debatir mediante el uso de nuevas tecnologías.

La amenaza de los delitos que pueden ser cometidos bajo modalidad cibernética equivale a un abanico muy grande el cual no hace más que aumentar, desde piratería de películas hasta pornografía infantil, se debe comprender lo importante de la situación, y con esto lo útil que sería tener apoyo internacional y más que apoyo ser parte de la solución.

De igual manera el entretenimiento y las personas que de este hacen su vida necesitan tener la seguridad respectiva de acuerdo al contenido que crean y comparten al mundo y en la actualidad no hay mejor forma de compartir trabajos artísticos audiovisuales que mediante el internet y las plataformas de streaming.

Además, es fundamental que Ecuador se una y se comprometa con el convenio para disponer de un recurso compartido que permita procesar los actos delictivos y fomentar una colaboración internacional más efectiva. Como se menciona, ratificar el convenio nos brindaría la herramienta necesaria de cooperación interestatal para luchar contra la ciberdelincuencia, que es una modalidad delictiva que crece constantemente.

CAPITULO I

MARCO TEÓRICO

CONTEXTO HISTÓRICO Y DEFINICIONES. –

Contexto Histórico. –

La tecnología ha sido un indiscutible salto para la humanidad en un amplio rango de categorías, desde la comunicación, medicina, comercio, la tecnología y el uso de estas está provocando una metamorfosis en la sociedad, que no se ha visto desde la revolución industrial, cambiando la forma en la que las personas desarrollan sus actividades diarias.

Todo individuo se ve influenciado por una base cultural, ética y moral que va adquiriendo a lo largo de su vida a partir de sus experiencias. Por otro lado, el psicólogo Carl G. Jung propuso una teoría en la que destaca la existencia de un lenguaje simbólico compartido por todas las personas, independientemente del tiempo o lugar en el mundo. Este lenguaje se compone de símbolos que transmiten un contenido psíquico más allá de la comprensión racional. En resumen, sería un conocimiento al que el ser humano puede acceder inconscientemente a través de un lenguaje universal que conecta a todas las personas de manera similar. (Galeano, 2011)

Román Gubern, en "La Hipótesis del Lago", argumenta que el hombre primitivo al ver su reflejo en el agua, interpretó esa imagen como una representación de sí mismo, lo que antes era una representación visual se transformó gradualmente en una representación más racional. Con el tiempo, el cerebro humano fue aumentando de tamaño y, simultáneamente, las habilidades sociales, mentales y prácticas se expandieron hasta alcanzar el estado actual. Este desarrollo humano incluyó el desarrollo de la razón, la inteligencia social, el lenguaje, las habilidades manuales, así como habilidades para la supervivencia y la caza. (Galeano, 2011)

Es así como la humanidad se encuentra en un punto en la historia en la que, para generaciones recientes la vida sin la tecnología sería impensable, esta diferenciación en cuanto a la afectación que la tecnología ha tenido en las personas, las generaciones o los saltos generacionales se evidencian en cuanto a que tanto los miembros de las mismas pueden manipular las tecnologías, los individuos pertenecientes a los baby boomers y la Generación X han integrado la tecnología a medida que avanzaban en sus vidas. Por otro lado, los millennials, la Generación Z y la Generación Alpha han crecido inmersos en un ambiente digital desde temprana edad, lo que se refleja en sus distintos patrones de consumo y utilización de las herramientas digitales, pero al paso que aumenta el uso de la tecnología han aumentado los métodos en que estos medios tecnológicos son utilizados para causar daño o cometer actividades moralmente reprobables. (Fundación Fepropaz, 2023)

La creación de la Web o Internet ha desarrollado una cultura enteramente nueva, el que las personas posean una herramienta tan poderosa y masivamente accesible como esta, formula nuevas oportunidades, así como problemas. El desarrollo de aplicaciones y sitios web que son utilizados para una amplia gama de actividades, así como el anonimato para poder acceder a estas casi sin restricción, ha forzado a que las instituciones de control, tanto nacionales como internacionales, creen nuevos reglamentos, estatutos y tratados para regular el uso de las mismas. (Campos, 2019)

En un informe que presenta NORTON, prestador de servicios de software para protección informática, realizado sobre 21 países, se establecía que el número total de consumidores afectados por delitos cibernéticos en 2016, fue de 689.4 millones, lo cual se traduce en un valor de $125,900 millones de dólares

estadounidenses en costos por este tipo de actividad criminal. Cabe recalcar que NORTON, acorde a la página de datos estadísticos mundial Statista, solo en el año fiscal 2022 tuvieron una ganancia de 3.3 billones de dólares estadunidenses. (Statista Research Department, 2023) (Symantec Corporation, 2016)

Al revisar los datos de la economía de esta prominente compañía de ciberseguridad se comprende, por una parte, la necesidad de los usuarios de protección ante las amenazas que ofrece la red. Y por otra parte da un vistazo al inequívoco hecho de lo lucrativo que son estas actividades delictivas para quienes las cometen y lo representativo que es el impacto en la economía mundial.

En fechas más actuales, y de acuerdo con las proyecciones de Cybersecurity Ventures, se estima que, en el año 2023, el costo anual global de los delitos cibernéticos llegará aproximadamente a los 8 trillones de dólares americanos. A posteridad este mismo estudio prevé un aumento en el costo de los daños causados por estos delitos, que se espera alcance los 10.5 trillones de dólares para el año 2025. (Morgan, 2020)

Para aterrizar los valores antes discutidos con una analogía, tomando el valor de daño financiero que se realizó a la comunidad mundial únicamente en el 2021, $6 trillones de dólares americanos, comparado a la economía mundial, “sería la tercera economía más grande del mundo después de Estados Unidos y China.” Como nos explica Steve Morgan en la Cybercrime Magazine. (Morgan, 2020)

Haciendo un pequeño análisis comparativo de los valores de las lesiones monetarias causadas por el crimen cibernético alrededor del mundo en los años 2016 y 2022, siendo $125,900 millones de dólares estadounidenses para el 2016 y 8 trillones de dólares americanos para el estimado del 2023, se nota una diferencia

abismal en las cantidades así como el crecimiento exagerado que esta economía ha tenido, lo cual está estrechamente relacionado a la globalización y la expansión en la tecnología alrededor del mundo.

Que, según un informe de Cisco, se prevé que para el año 2023 la cantidad de dispositivos en red en el planeta sea tres veces mayor que la población humana. Además, para el año 2022, se habrá integrado un trillón de sensores en red en nuestro entorno, con la perspectiva de llegar a 45 billones en las dos próximas décadas, pudiendo inferir que, a perspectiva actual, esta expansión descontrolada no se encuentra en ningún tipo de recesión.

En datos más actuales se observa el “ESET Security Report 2023” (ESR) presentado por ESET, empresa dedicada a la protección de sistemas informáticos, este es un informe en el cual se analiza el panorama de seguridad cibernética específicamente en empresas de América Latina y algunos hallazgos relevantes extraídos del mismo revelan que el 69% de las entidades en América Latina experimentaron algún tipo de incidente de seguridad en el transcurso del último año.

Además, respecto a la detección de códigos maliciosos en campañas de phishing, se identificó que los países con los mayores porcentajes son; Ecuador con un 8%; seguido por Costa Rica, con un 7,2%; Colombia, con un 5,7%; Guatemala, con un 5,2%; y El Salvador, con un 5,1%. Lo cual, acorde al ESR, corona al país como el más inseguro en cuanto a seguridad cibernética, hablando únicamente en el sector de empresas privadas. (Harán, 2023)

Según el último Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, una agencia de las Naciones Unidas, Ecuador ocupa el puesto 119 de 182 países en términos de vulnerabilidad frente a ataques cibernéticos es

decir que Ecuador se une a Argentina, Brasil, Colombia, México y Perú como uno de los países latinoamericanos más afectados por los delitos informáticos, principalmente por la presencia de códigos maliciosos, conocidos como malware. (Onofa, 2022)

En octubre de 2021, el Banco Pichincha, el principal banco privado de Ecuador, sufrió un ataque cibernético que resultó en la interrupción de sus operaciones, dejando inoperativos los cajeros automáticos y el portal de banca en línea. Este ataque fue catalogado como uno de los mayores incidentes a nivel mundial ese año. Esta situación marcó la segunda ocasión en pocos meses en que el banco fue afectado; en febrero, fue víctima de otro ataque cibernético que también impactó al Ministerio de Finanzas de Ecuador, según reportes del sitio de noticias Welivesecurity, perteneciente a la empresa de seguridad en internet ESET. (Onofa, 2022)

Con todo lo anterior expuesto, es claro e indiscutible el aumento del terrorismo, espionaje, sabotaje, robo de información privilegiada, violación a los derechos de autor, entre otras modalidades que hacen uso del ciberespacio y las plataformas de información lucran afectando a la seguridad estatal de cada país, así como la seguridad de empresas multinacionales, Organismos Internacionales, tanto gubernamentales como no gubernamentales, sin mencionar a los ciudadanos de los estados. (Castro & Monteverde, 2018)

La capacidad de llevar a cabo estos delitos a través de Internet facilita que los criminales, sin complicaciones significativas, puedan encontrarse en un país determinado, utilizar servicios de otro y, finalmente, atacar a una o más víctimas en un tercer país involucrado. Esta característica de transaccionalidad plantea un

desafío para el campo del Derecho, en particular para los sistemas jurídicos penales, que deben reconocer la necesidad de establecer ciertos niveles mínimos de coordinación para combatir de manera efectiva este tipo de actividad delictiva. (Temperini, 2014)

En cuanto a cómo se encuentra el país en tema de ciberseguridad y los esfuerzos o medidas que ha tomado el gobierno para llegar a un mejoramiento de la situación nacional en cuanto a seguridad informática, en 2022 se presentó una propuesta que se bautizó como “Estrategia Nacional De Ciberseguridad Del Ecuador”, misma que fue presentada por el Ministerio de Telecomunicaciones y Sociedad de la Información del gobierno anterior en la cual la cumplía funciones de ministra la abogada Vianna Maino. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Esta estrategia presenta seis pilares para cumplir con su objetivo, el cual acorde la estrategia es “proteger la soberanía del estado, la protección de la información de las instituciones y los ciudadanos, y garantizar que las acciones e iniciativas en materia de ciberseguridad sean holísticas, coherentes y estén en concordancia con los valores fundamentales compartidos.” (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022, p. 12)

El primer pilar se titula “Gobernanza y coordinación Nacional” en el cual el ministerio expresa que la colaboración sólida y la administración efectiva de la ciberseguridad en Ecuador son fundamentales para establecer un entorno donde los ataques cibernéticos no puedan detener la economía nacional, minimizar al máximo el impacto en las organizaciones y la sociedad ecuatoriana, y evitar que los esfuerzos de digitalización sean ineficaces y estén expuestos a riesgos mayores de

ciberseguridad. De esta manera, Ecuador busca incorporar la ciberseguridad como un componente esencial y prioritario en el desarrollo digital del país, a través de un enfoque coherente y coordinado en la gobernanza nacional. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Para cumplir con este pilar la estrategia propone tres objetivos los cuales son: Objetivo 1.1: Crear un enfoque global para la gestión de la seguridad cibernética; objetivo 1.2: Promover la construcción de una comunidad cohesionada que involucre a expertos en seguridad cibernética de diversas áreas involucradas; Objetivo 1.3: Crear un conjunto de leyes y regulaciones completas que faciliten la gestión nacional de la seguridad digital y la defensa cibernética. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Lo cual en resumen propone fortalecer las instituciones gubernamentales que tienen relevancia en el control de datos así como ciberseguridad en general, como ejemplo en las líneas de acción que sugiere la Estrategia se proponen medidas como crear una estructura institucional que defina las funciones, responsabilidades y roles de todas las entidades gubernamentales relevantes en el ámbito de la seguridad integral o la seguridad del Estado, dentro de la cual se integre la ciberseguridad, además de reforzar la función del coordinador nacional de políticas de ciberseguridad dentro del Comité Nacional de Ciberseguridad. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Incluso plantea establecer una perspectiva integral en la asignación de recursos para cumplir los objetivos estratégicos de la estrategia nacional. Este enfoque se alinearía con el plan de implementación, el cual sería supervisado por el Comité Nacional de Ciberseguridad. El presupuesto comprendería gastos regulares,

integrándose en el presupuesto nacional, junto con la asignación específica de recursos para proyectos o iniciativas respaldadas por programas especiales. Las fuentes de financiamiento podrían ser tanto internas como de donantes internacionales. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Con lo cual de una u otra manera trata de presentar medidas con las cuales será posible llevar a cabo la estrategia, además en el mismo establecen que en nuestro país, la atmósfera para invertir en tecnología ha sido positiva, lo que ha propiciado oportunidades de inversión en el campo de la ciberseguridad. Desde un punto de vista legal, hemos implementado acciones para ratificar y poner en práctica el Convenio de Budapest sobre la Ciberdelincuencia. El país recibió una invitación el 30 de marzo de 2022 para unirse a este tratado, una acción que fortalecerá significativamente nuestra capacidad para enfrentar la ciberdelincuencia que cruza fronteras. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022)

Delitos Informáticos: Definiciones Y Posturas De Autores. –

Como expresa Narda J. Ortiz Campos en su artículo Normativa Legal sobre Delitos Informáticos en Ecuador, internacionalmente se conocen con diferentes designaciones los delitos informáticos, tales como, delitos electrónicos, cibercrimen, ciberdelitos, delitos relacionados con las computadoras, crímenes por computadora, entre otros. El término más común por los autores en la doctrina del derecho penal informático es el de delito informático. (Campos, 2019)

Originalmente el termino delito informático surgió en la última década de los años noventa, al mismo tiempo que se producía la proliferación de Internet, específicamente en Francia. En este contexto, se estableció el grupo "G8" con el

propósito de analizar los desafíos emergentes relacionados con la delincuencia vinculada al uso de Internet. Inicialmente, se empleó la denominación "delito informático" para describir los crímenes perpetrados en la red o en sistemas de telecomunicaciones. (Zambrano-Mendieta et al., 2016)

Otra conceptualización de “delitos informáticos” se encuentran en perspectivas como la del abogado Julio Téllez Valdés quien nos dice que proporcionar una definición precisa de los delitos informáticos no resulta sencillo, ya que se trata de una categoría especial. Esto se debe a que, para que se considere un acto como un "delito" en el sentido de acciones específicas definidas por la ley, es necesario que el término "delitos informáticos" esté incluido en los códigos penales, lo cual no ha ocurrido en algunos países. (Valdés, 2008)

Pero al hacer un esfuerzo para realizar una conceptualización de la ambigüedad antes discutida el abogado nos dice que, los delitos informáticos pueden ser descritos de dos maneras: como acciones ilegales que involucran computadoras, ya sea como herramienta o como objetivo o como acciones que encajan en los criterios legales típicos, siendo antijurídicas y atribuibles a culpabilidad, y que involucran computadoras, ya sea como medio o propósito. (Valdés, 2008)

Mientras que Davara Rodríguez nos brinda un concepto distinto y nos dice que delito informático es aquel que se lleva a cabo con la asistencia de la computación o métodos adicionales. Esta idea presenta, para varios estudiosos, el inconveniente de enfocarse exclusivamente en la informática como el único medio para cometer este tipo de delitos, sin tener en cuenta que lo informático también puede referirse al blanco de la infracción. (Rodríguez, 2020)

Cualquier acto delictivo en el que el perpetrador emplee un método o técnica informática en su comisión, utilizando componentes de un sistema informático o telemático, o afectando intereses legales protegidos, como la privacidad, la propiedad intelectual y el software. Es otra definición emitida por el autor Henry William. (Torres-Torres, 2002)

Las diversas opiniones de los expertos resaltan que el delito informático, en lugar de representar una categoría delictiva específica, abarca diversas formas de actividad criminal relacionadas de alguna manera con las computadoras. Es apropiado emplear el término "Delitos Informáticos" en su forma plural, ya que se utiliza para describir múltiples conductas ilícitas en lugar de una única categoría general. Se usará el término "delito informático" cuando se haga referencia a una de estas modalidades delictivas en particular. (Casanoba, 1995)

Se puede observar cómo, si bien las perspectivas antes descritas no concuerdan en su totalidad, la definición de delitos informáticos es clara y la comprensión de lo que abarca este tipo de actividad antisocial se encentra reconocida a nivel mundial.

Previo a que se conocieran como “delito informático”, se buscaba proteger los datos personales que, gracias a los nuevos medios de comunicación y tratamiento de datos automatizados creados en los años sesenta, habían creado nuevas formas de vulnerar este bien jurídico. La protección de la data personal y su tratamiento automatizado se puso en duda y se crearon convenios y tratados para asegurar la colaboración de la comunidad internacional.

Entre estos se encuentra el convenio de Estrasburgo, de 28 de enero de 1981, en el cual se considera que es importante extender la salvaguardia de los

derechos y libertades esenciales de las personas, especialmente el derecho a la privacidad, en vista del aumento en la transferencia transfronteriza de datos personales sometidos a procesos automatizados. (Council of Europe, 1981)

En cuanto a la motivación por la cual se desarrolló este convenio, el mismo es su primer artículo “Objeto y fin” nos dice que, el propósito de este convenio es asegurar que en el territorio de cada una de las partes, sin importar su nacionalidad o residencia, se respeten los derechos y las libertades fundamentales de cada individuo, en particular el derecho a la privacidad, en lo que respecta al procesamiento automatizado de sus datos personales. (Council of Europe, 1981)

En otras palabras, se vela por la forma en la que se utilizan los datos privados de los individuos de los estados, también castigando y calificando de punible a los actos en los cuales tanto el uso no autorizado de estos datos, así como si el uso de estos datos tiene un fin antisocial o de beneficio para quien los usa y perjuicio para quien es el legítimo dueño de los mismos.

Sobre estos el convenio nos dice en su artículo seis que, la información personal que revele detalles como el origen racial, opiniones políticas, creencias religiosas u otras convicciones, así como datos personales relacionados con la salud o la vida sexual, no puede ser procesada automáticamente a menos que la legislación nacional proporcione salvaguardias adecuadas. Esta misma regla se aplicará a datos personales relacionados con condenas penales. (Council of Europe, 1981)

Los datos personales no son intrínsecamente sensibles o vulnerables, su sensibilidad depende del contexto en el que se utilicen. Dado que existen múltiples contextos posibles, la forma más apropiada de protección legal sería de naturaleza

preventiva. Sería inviable intentar enumerar todos los bienes legales o intereses dignos de protección y tratar de sistematizar las diferentes facetas del problema en relación con diversos intereses legales, como la privacidad, la libertad, el honor, entre otros. El único criterio viable consiste en establecer un mecanismo preventivo impulsado por el Estado y supervisado por los afectados a través del ejercicio de derechos instrumentales. (Higueras, 1983)

La sensibilidad de los datos personales, que varía según su uso o contexto, significa que, si es factible separar ciertos casos de uso, se debe analizar si el uso de datos personales exige una protección preventiva particular o no. (Higueras, 1983)

A continuación, se presentará un análisis de derecho comparado entre estados de la región, se notará como con el paso del tiempo y el avance de la tecnología, analizado anteriormente, ha empujado a las naciones de Latinoamérica a reconocer estas actividades como una amenaza y la necesidad de crear mecanismo de protección a las nuevas formas de violentar los bienes jurídicos de la población de los propios estados.

DELITOS INFORMÁTICOS EN EL MARCO LEGAL LATINOAMERICANO. –

El avance de las herramientas tecnológicas y sus amenazas no ha pasado inadvertido en América latina, en el marco legal de esta región los delitos informáticos se encuentran tipificados en algunas de las legislaciones de los miembros de la misma.

En varios Estados, se puede identificar legislación reciente, desarrollada en los últimos 5 años, que establece sanciones penales para conductas que anteriormente no se reconocían como delitos, o al menos no habían alcanzado un

nivel de gravedad en la región que justificara su clasificación como ataques informáticos específicos. Para ilustrar esto, en algunos países se han establecido más de 15 disposiciones legales relacionadas con delitos informáticos. (Temperini, 2014)

Tal como menciona Temperini, solo en el caso de la información personal, el continuo aumento del mercado clandestino de información actúa como un motor que genera una gran cantidad de ataques informáticos, en su mayoría dirigidos a la obtención de bases de datos que contienen información personal. (Temperini, 2014)

El siguiente es un análisis de las legislaciones de algunos países de la región comparando con el catálogo de delitos electrónicos encontrados en el Convenio sobre la Ciberdelincuencia Budapest, para fines de este trabajo de tomaran en cuenta los títulos 1 (uno) y 2 (dos) del convenio.

1. Titulo 1 – Delitos Contra La Confidencialidad, La Integridad Y La Disponibilidad De Los Datos Y Sistemas Informáticos.

1.1. Acceso Ilícito. –

1.1.1. Brasil.

En la legislación brasileña en su Código Penal habla de quien Ingresar sin autorización a dispositivos informáticos pertenecientes a terceros, ya estén o no conectados a una red de computadoras, con la intención de obtener, modificar o eliminar datos o información, o de introducir debilidades con el propósito de obtener beneficios ilegítimos, esto en el artículo 154-A. y determina la pena de prisión en uno a cuatro años y una multa. (Congreso Nacional de Brasil, 1940)

Pero en este artículo, a diferencia de los vistos hasta el momento, la el legislador brasileño nos da, a tipo de lista, los detalles o acciones que servirán de agravantes para el mismo delito, en esta arista nos dice que: delitos informáticos

En referencia las actividades: Quien fabrique, ofrezca, distribuya, venda o propague dispositivos o programas de computadora con el propósito de facilitar la comisión de la conducta descrita en el encabezado, incurrirá en la misma pena. La pena se incrementará en un rango de un tercio a dos tercios si la invasión resulta en un daño económico. (Congreso Nacional de Brasil, 1940)

Si como resultado de la intrusión se obtiene contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, información confidencial definida por ley, o se obtiene un control remoto no autorizado del dispositivo invadido, se impondrá una pena de reclusión de dos a cinco años, y multa. Además, si se divulgan, se comercializan o se transmiten los datos o la información obtenida a terceros, en cualquier forma, la pena se incrementará en un rango de un tercio a la mitad. (Congreso Nacional de Brasil, 1940)

En referencia al sujeto pasivo la pena se aumentará en un tercio a la mitad si el delito se comete contra;

- Presidente de la República, gobernadores y alcaldes;
- Presidente del Supremo Tribunal Federal;
- Presidente de la Cámara de Diputados, del Senado Federal, de una Asamblea Legislativa Estatal, de la Cámara Legislativa del Distrito Federal o de un Concejo Municipal;

- o el director máximo de la administración directa e indirecta federal, estatal, municipal o del Distrito Federal. (Congreso Nacional de Brasil, 1940)

Como apunte adicional, se encuentra el artículo 154-B. en el que se habla de que solo procederán mediante representación, a menos que el delito se cometa contra la administración pública en cualquiera de los niveles de gobierno (Unión, Estados, Distrito Federal o Municipios), o contra compañías que tienen concesiones para prestar servicios públicos. Representación es un concepto legal en el cual una persona actúa o lleva a cabo acciones en nombre de otra, ya sea por autorización expresa de la persona representada o por designación legal para representarla, generando consecuencias legales en el ámbito patrimonial y jurídico del representado. (Congreso Nacional de Brasil, 1940)

1.1.2. Chile.

En cuanto a Chile, el Estado en el 2022 aprobó el proyecto de ley número 21.459 “Establece Normas Sobre Delitos Informáticos, Deroga La Ley N° 19.223 Y Modifica Otros Cuerpos Legales Con El Objeto De Adecuarlos Al Convenio De Budapest” con su título 1; “De los delitos informáticos y sus sanciones” y en su artículo numero dos habla del acceso ilícito, y se establece que quien acceda a un sistema informático sin autorización o excediendo la autorización otorgada, eludiendo medidas de seguridad, enfrentará sanciones que incluyen prisión menor en su grado mínimo o multa (once a veinte unidades tributarias mensuales). (Congreso Nacional de Chile, 2022)

Si el acceso busca apropiarse o utilizar la información del sistema, la pena será prisión menor de grado mínimo a medio. Esta misma pena se aplica a quienes divulguen información obtenida ilícitamente, a menos que sea la misma persona que

obtuvo la información, en cuyo caso la pena será de prisión menor de grado medio a máximo. (Congreso Nacional de Chile, 2022)

En el caso de esta norma a diferencia de las anteriores no solo habla de quien accede a la información, también de dirige a que quien, aunque no haya obtenido por sus propios medios a información disponga de esta, es decir a quien disponga de dicha información por cualquier medio se le extenderá la misma cantidad de pena de quien obtuvo dicha información.

1.1.3. Colombia.

La legislación de este país positiviza este crimen en su código penal en el artículo 269A, “acceso abusivo a un sistema informático”, nos dice, la persona que, sin autorización o fuera de los términos acordados, ingrese total o parcialmente a un sistema informático, ya sea que esté protegido o no por medidas de seguridad, o que permanezca dentro del sistema en contra de la voluntad del titular legítimo, enfrentará una pena de prisión que oscilará entre cuarenta y ocho y noventa y seis meses, junto con una multa que varía de cien a mil salarios mínimos legales mensuales vigentes. (Senado de la Republica de Colombia, 1890)

Se puede observar cómo este artículo refiere únicamente a quien accede a una parte o todo el sistema informático y no a quien hace uso y goce de lo obtenido a través de este, además cabe recalcar que al momento de mencionar que el acceso se puede hacer por fuera de lo acordado, se hace referencia a un tipo de abuso de confianza o extralimitación de un acuerdo o una sesión de derecho o acceso a determinado sistema informático.

1.1.4. Conclusión Acceso ilícito y Convenio Budapest. –

Como se puede observar, en relación, a las demás legislaciones analizadas con respecto al acceso ilícito, la legislación tanto chilena y brasileña poseen un desarrollo más amplio y detallado en cuanto a los diferentes frentes que poseen estas actividades típicas. Y este desarrollo se infiere es el resultado de la ratificación del convenio de Budapest por parte de estos países, el convenio aborda este tema en el artículo 2 del mismo establece que, cada país tomará las medidas legales y otras disposiciones necesarias para considerar como un delito en su jurisdicción el acceso intencional y no autorizado a un sistema informático completo o parcial. Estos delitos pueden requerir la violación de medidas de seguridad, con el fin de obtener datos informáticos u otro propósito criminal, o estar relacionados con un sistema informático conectado a otro sistema informático. (Consejo de Europa, 2001)

Lo que incurriría en el país el adoptar la legislación de los países firmantes, ante lo anteriormente expuestos, aquellos que tienen ratificados el Convenio Budapest son:

- Brasil; adhesión realizada el 30 de noviembre de 2022.

- Colombia; adhesión realizada 16 de marzo de 2020

- Chile; adhesión realizada en abril de 2017

- Argentina; adhesión realizada en junio de 2018

- Perú; adhesión realizada en marzo de 2019

1.2. Interceptación Ilícita. –

1.2.1. Brasil.

En el gigante latinoamericano en su legislación contempla el delito de interceptación ilícita en su Código Penal, específicamente en el artículo 10 de la Ley 9.296/1996. Esta ley regula las interceptaciones telefónicas y telemáticas y describe las circunstancias y condiciones bajo las cuales se pueden realizar legalmente estas interceptaciones por parte de las autoridades competentes. (Congreso Nacional Brasileño, 1996)

El artículo 10 de dicha ley establece que constituye delito el establecer como una acción criminal la interferencia en comunicaciones telefónicas, de telecomunicaciones o informáticas, así como la divulgación indebida de información confidencial o mensajes, excepto en los casos autorizados legalmente. Esta disposición penaliza la interceptación de comunicaciones sin la autorización debida o en situaciones no contempladas por la ley. (Congreso Nacional Brasileño, 1996)

Es importante mencionar que las leyes relacionadas con la interceptación de comunicaciones están sujetas a condiciones y procedimientos específicos establecidos por la legislación brasileña para garantizar los derechos fundamentales de privacidad y protección de datos de los ciudadanos. Además, el país el pasado 30 de noviembre del 2022, Brasil finalizó su incorporación al Convenio sobre Ciberdelincuencia Budapest, y según una declaración conjunta del Ministerio de Relaciones Exteriores y el Ministerio de Justicia y Seguridad Pública, este convenio busca promover y facilitar la cooperación a nivel internacional en la lucha contra los delitos cometidos en el entorno digital.

Aunque la ratificación del convenio es reciente en Brasil, y se lleva debatiendo la ratificación del mismo desde el año 2019, es correcto decir que su legislación ha sido de las más avanzadas de la región y aunque han tenido presente

estos delitos desde principio de siglo, como con la promulgación de leyes tal como la expuesta anteriormente, la cual fue creada en 1996, aun antes de la creación del convenio estudiado en este trabajo investigativo.

1.2.2. Chile

En Chile esta conducta se encuentra castigada por la ley Núm. 21.459, la cual, como se expuso anteriormente, se creó para adecuar el cuerpo legal del país al convenio de Budapest y en su artículo tres habla de la interceptación ilícita y se estable que quien intervenga indebidamente, obstruya o interfiera, empleando métodos técnicos, en la transmisión de información no pública dentro de un sistema informático o entre dos o más de estos, será sancionado con la pena de prisión de grado medio. (Congreso Nacional de Chile, 2022)

A su vez, aquel que, sin la autorización adecuada, capture datos de sistemas informáticos utilizando métodos técnicos que involucren emisiones electromagnéticas provenientes de los mismos, recibirá una pena de prisión que oscilará entre los grados medio y máximo. (Congreso Nacional de Chile, 2022)

1.2.3. Colombia.

En el país vecino Colombia esta actividad se encuentra tipificada en la ley 1273 creada en el 2009, misma creada para la modificación del Código Penal del mismo país, y se crea el bien jurídico tutelado denominado como “de la protección de la información y de los datos". En su capítulo primero habla de los actos que vulneran la privacidad, la integridad y la accesibilidad de los datos y los sistemas informáticos. (El Congreso de Colombia, 2009)

Y en su artículo 269C., interceptación de los datos informáticos, nos dice que quien, sin autorización judicial previa, realice la interceptación de datos informáticos

en su origen, destino o dentro de un sistema informático, así como también las emisiones electromagnéticas provenientes de un sistema que los transporte, será sancionado con una pena de prisión que va desde 36 hasta 72 meses.

1.2.4. Conclusión “Interceptación Ilícita” y Convenio Budapest

En conclusión, a la comparación normativa realizada entre los países que tienen ratificado el Convenio es correcto decir que, si bien estos países presentan en sus legislaciones disposiciones que castigan la interceptación ilegal de datos informáticos, existen diferencias en la redacción de sus leyes y en la gravedad de las penas establecidas, aunque todas convergen en proteger la confidencialidad y la integridad de los datos en el entorno digital.

Por otra parte, el Convenio Budapest en su artículo 3 nos dice lo siguiente acerca de la interceptación ilícita.

En su artículo 3 el convenio Budapest trata el delito de interceptación ilícita y establece que cada nación deberá tomar las medidas jurídicas y pertinentes para considerar como un crimen dentro de su marco legal interno la interceptación premeditada e ilegítima, mediante métodos técnicos, de información informática transmitida de manera privada dirigida hacia un sistema informático, originada en un sistema informático o realizada dentro del mismo. Esto incluye las emisiones electromagnéticas generadas por un sistema informático que transmita dicha información. Las disposiciones pueden requerir que el delito se cometa con una intención criminal o en relación con la conexión entre sistemas informáticos. (Consejo de Europa, 2001)

1.3. Ataque A La Integridad De Los Datos. –

1.3.1. Brasil.

En la legislación de este país, el ataque a los datos y la destrucción de los mismos, se encuentra tipificado en su norma penal en el artículo 154-A que también habla del acceso ilícito al decir que acceder de manera indebida al dispositivo informático de alguien, independientemente de si está conectado a una red informática o no, al vulnerar el sistema de seguridad con el fin de obtener, modificar o eliminar datos, es decir un ataque a la integridad de os mismos o información sin contar con la autorización expresa o implícita del dueño del dispositivo, o instalar vulnerabilidades para obtener beneficios ilícitos. (Congreso Nacional de Brasil, 1940)

En cuanto a la pena con la que se castiga este delito, esta se encuentra explicada en el inciso de Acceso ilícito, al ser el mismo artículo.

1.3.2. Chile.

En la legislación chilena se establece la pena a esta conducta en el artículo 4 de la Ley 21.459 creada para adecuar su normativa a conforme a su ratificación del tratado internacional Budapest, y establece que si alguien manipula, daña o elimina información digital sin autorización, enfrentará una pena de prisión menor en su nivel intermedio, lo cual se traduce a una pena de 10 años y un día, si dicha acción provoca un daño significativo al propietario de dichos datos. (Congreso Nacional de Chile, 2022)

1.3.3. Colombia.

En la norma de este país se positiviza la pena de esta conducta en la Ley 1273 de 2009 en el artículo 269D. de la misma y se establece que quien, sin la autorización correspondiente, elimine, deteriore, dañe, altere, borre o suprima datos informáticos, así como cualquier sistema de procesamiento de información o sus

elementos o componentes lógicos, será sentenciado a una pena de prisión entre 48 y 96 meses, además de una multa que oscilará entre 100 y 1000 salarios mínimos legales mensuales vigentes. (El Congreso de Colombia, 2009)

1.3.4. Conclusión “Ataque a la integridad de los datos” y Convenio Budapest.

En conclusión, en Brasil, Chile y Colombia se encuentran contempladas y penalizadas las acciones relacionadas con el acceso indebido a dispositivos informáticos y la manipulación, daño o destrucción de datos sin la autorización correspondiente. En Brasil, se castiga el acceso ilícito y la alteración de datos según el artículo 154-A, mientras que, en Chile, la Ley 21.459 tipifica esta conducta y establece penas de prisión menor, con penas más graves si hay daño significativo a los datos. Por su parte, en Colombia, la Ley 1273 de 2009 penaliza la manipulación, alteración o supresión de datos informáticos con penas de prisión entre 48 y 96 meses, además de multas considerables. Estas legislaciones buscan proteger la integridad y seguridad de la información digital y garantizar la privacidad de los datos de los ciudadanos.

Mientras que el Convenio sobre Ciberseguridad Budapest acerca de este delito en su artículo cuatro determina que cada país deberá implementar disposiciones legales y otras medidas necesarias para considerar como un crimen en su jurisdicción cualquier acción intencional e ilegítima que cause daño, eliminación, deterioro, alteración o supresión de datos informáticos, los países pueden decidir mantener el derecho de requerir que los actos mencionados en el primer párrafo causen daños significativos. (Consejo de Europa, 2001)

1.4. Ataques A La Integridad Del Sistema. –

1.4.1. Colombia.

En la legislación colombiana este delito se encuentra registrado en el código penal de este país como “Daño Informático” y en el mismo establece que quien, careciendo de autorización, cause destrucción, daño, borrado, deterioro, alteración o eliminación de datos informáticos, un sistema de procesamiento de información o sus partes o componentes lógicos, será sancionado con una pena que va desde 48 a 96 meses de prisión, además de una multa que oscila entre 100 y 1000 salarios mínimos legales mensuales vigentes. (El Congreso de Colombia, 2009)

Este enunciado es una disposición que establece las consecuencias legales para aquellos individuos que sin la debida autorización realicen acciones que afecten los datos informáticos, sistemas de procesamiento de información o sus componentes lógicos. En términos generales, la norma describe dos sanciones principales:

- Pena de prisión: La persona que lleve a cabo alguna de las acciones mencionadas sin autorización podría enfrentar una pena de prisión que va desde 48 a 96 meses. Esta es una sanción seria y significativa en términos de tiempo, reflejando la gravedad del delito relacionado con la alteración o daño a los datos informáticos.
- Multa económica: Además de la pena de prisión, se estipula una multa monetaria. Esta multa puede variar entre 100 y 1000 salarios mínimos legales mensuales vigentes. Esta sanción económica pretende ser una medida disuasoria adicional y posiblemente una forma de compensar los daños causados por la alteración o destrucción de los datos.

En resumen, esta normativa establece medidas punitivas considerables para disuadir y castigar la alteración ilegal de datos informáticos o sistemas de procesamiento de información sin autorización. Su objetivo principal parece ser proteger la integridad y la seguridad de los sistemas informáticos y los datos, así como disuadir a las personas de llevar a cabo acciones dañinas o malintencionadas contra estos activos digitales.

1.4.2. Chile.

En este país encontramos este delito en el artículo primero de la Ley Núm. 21.459 y establece que quien entorpezca o dificulte el correcto desempeño, total o parcial, de un sistema informático al introducir, transmitir, dañar, perjudicar, alterar o eliminar datos informáticos, será penalizado con presidio menor en sus niveles medio a máximo. (Congreso Nacional de Chile, 2022)

El enunciado hace referencia a la penalización de acciones que causen interrupción o bloqueo del funcionamiento adecuado de un sistema informático. Establece sanciones para aquellos individuos que deliberadamente interfieran con la normal operatividad de un sistema informático mediante la introducción, transmisión, daño, alteración o eliminación de datos informáticos. Esta acción se considera un delito que puede acarrear una condena de presidio menor en sus grados medio a máximo. Este tipo de disposiciones busca proteger la integridad y el correcto funcionamiento de los sistemas informáticos, así como la seguridad de los datos y la información contenida en ellos.

Estas medidas son congruentes con los principios del Convenio de Budapest sobre Ciberdelincuencia. Este convenio, enfocado en combatir delitos informáticos a nivel internacional, propone la armonización de leyes y políticas para enfrentar

amenazas cibernéticas transfronterizas. El enunciado refleja las disposiciones destinadas a disuadir y castigar tales acciones, concordando con el espíritu del Convenio de Budapest que busca estandarizar la legislación y fortalecer la cooperación internacional para combatir la ciberdelincuencia.

1.4.3. Perú.

En este país vecino, encontramos en su legislación la Ley N° 30171 del 2014 la cual fue creada para sustituir el articulado de la Ley Nº 30096, y en el mismo se establece que quien, de manera intencional y sin legitimidad, deshabilite total o parcialmente un sistema informático, bloquee el acceso a este, dificulte o evite su funcionamiento o la prestación de sus servicios, será sancionado con prisión no menor de tres años ni mayor de seis, además de ochenta a ciento veinte días de multa. (Congreso de la Republica de Perú, 2014)

El artículo penaliza las acciones ilegítimas que interfieren con el funcionamiento normal de un sistema informático. Estas acciones incluyen la inutilización deliberada, la interrupción del acceso, el entorpecimiento o la imposibilidad de su operatividad o de sus servicios. La medida implica sanciones penales severas, con una pena de prisión no menor de tres años ni mayor de seis, acompañada de una multa de ochenta a ciento veinte días. Esta disposición busca prevenir y castigar actividades que obstaculicen el funcionamiento adecuado de los sistemas informáticos, asegurando la integridad y estabilidad de la infraestructura tecnológica. Además, pretende disuadir a individuos o entidades de llevar a cabo acciones que afecten negativamente la disponibilidad y el acceso a los servicios digitales.

1.4.4. Conclusión “Ataque a la integridad del sistema” y Convenio Budapest.

El análisis de las disposiciones legales de Colombia, Chile y Perú revela una convergencia en la regulación penal de los delitos informáticos en América Latina. Las leyes de estos países imponen sanciones a quienes interfieran ilegalmente con sistemas o datos informáticos sin autorización.

En Colombia, se establecen penas de prisión de 48 a 96 meses y multas de 100 a 1000 salarios mínimos legales mensuales vigentes para quienes causen daño, borrado, deterioro, alteración o eliminación de datos o sistemas informáticos sin permiso. Chile, por otro lado, castiga con presidio menor en sus niveles medio a máximo a quienes obstaculicen o dificulten el funcionamiento adecuado de sistemas informáticos mediante acciones como la introducción, transmisión, daño, perjuicio, alteración o eliminación de datos.

En el caso de Perú, la ley prevé penas de prisión no menores de tres años ni mayores de seis, junto con multas de ochenta a ciento veinte días, para aquellos que deshabiliten total o parcialmente un sistema informático, bloqueen su acceso o impidan su funcionamiento legítimo.

Estos marcos legales tienen como objetivo proteger la integridad de los sistemas informáticos y los datos, aplicando sanciones proporcionales y significativas para desalentar cualquier acción que interfiera con el funcionamiento normal de la infraestructura tecnológica. Además, se alinean con los principios del Convenio de Budapest sobre Ciberdelincuencia, que busca estandarizar y fortalecer las leyes internacionales para combatir los delitos cibernéticos.

Por otra parte, el convenio Budapest en el artículo 4 establece que cada nación deberá implementar leyes y otras medidas necesarias para considerar como un delito en su jurisdicción cualquier acto intencional e ilegítimo que cause un obstáculo significativo al funcionamiento de un sistema informático. Esto puede incluir la introducción, transmisión, daño, eliminación, deterioro, alteración o supresión de datos informáticos. (Consejo de Europa, 2001)

1.5. Abuso De Los Dispositivos. –

1.5.1. Chile.

En la legislación de este país se encuentra en la norma en la ley Núm. 21.459 en el artículo 8 y establece que la persona que, con el propósito de cometer los delitos establecidos en los artículos del 1ro al 4to (Ataque a la integridad de un sistema informático; Acceso ilícito; Interceptación ilícita; y Ataque a la integridad de los datos informáticos de esta ley), entregue, obtenga para usar, importe, difunda o de cualquier manera ponga a disposición uno o más dispositivos, programas informáticos, contraseñas, códigos de seguridad o acceso, u otros datos similares, elaborados o adaptados principalmente para cometer dichos delitos, será penalizada con la condena de presidio menor en su grado mínimo y una multa de cinco a diez unidades tributarias mensuales. (Congreso Nacional de Chile, 2022)

Este enunciado aborda la penalización de conductas asociadas con la preparación o facilitación de delitos informáticos en el marco de la legislación pertinente. Se refiere a la sanción para aquellos que entreguen, obtengan, importen, difundan o pongan a disposición dispositivos, programas informáticos, contraseñas, códigos de seguridad u otros datos diseñados o adaptados específicamente para cometer delitos según lo estipulado en ciertos artículos de la ley.

- Tipificación de acciones previas a la comisión de delitos informáticos: El texto se enfoca en penalizar acciones que tienen como objetivo preparar o facilitar la comisión de delitos informáticos. Se mencionan actos como la entrega, obtención, importación, difusión o puesta a disposición de herramientas y datos que se han creado o adaptado específicamente para cometer estos delitos.
- Sanciones establecidas: Se establece la pena de presidio menor en su grado mínimo y una multa que oscila entre cinco y diez unidades tributarias mensuales como consecuencia por llevar a cabo estas acciones. Estas sanciones pretenden desincentivar la preparación o facilitación de delitos informáticos al imponer castigos proporcionales a la gravedad de estas conductas.

En resumen, esta disposición legal busca prevenir y castigar la preparación o facilitación de delitos informáticos al penalizar la adquisición, distribución o puesta a disposición de herramientas y datos específicamente diseñados para llevar a cabo actividades delictivas relacionadas con la informática.

1.5.2. Conclusión “Abuso de los dispositivos” y Convenio Budapest.

Este es el delito que menos se encuentra tipificado en la normativa de países latinoamericanos, sin embargo, se puede encontrar esta conducta castigada como parte de otros artículos en varias normas. Por otro lado, el convenio Budapest sobre este delito establece que cada país deberá establecer en su legislación las medidas necesarias para considerar como un crimen, dentro de su propio territorio, la realización intencionada e ilegítima de ciertos actos. Estos actos incluyen la producción, venta, adquisición para uso propio, importación, difusión o cualquier otra

forma de disponibilidad de cualquier dispositivo, incluyendo programas informáticos, diseñados o adaptados principalmente para cometer delitos establecidos en los artículos 2 a 5 de este acuerdo. También se considerará delito la posesión de elementos especificados en los apartados i) o ii) del inciso a) de este artículo con la intención de usarlos para cometer los delitos indicados en los artículos 2 a 5. Algunos países podrán requerir una cantidad específica de dichos elementos para determinar la responsabilidad penal según su legislación interna. (Consejo de Europa, 2001)

Este artículo no se entenderá como imponiendo responsabilidad penal en casos donde la producción, venta, adquisición para uso propio, importación, difusión o cualquier otra forma de disponibilidad mencionada en el párrafo 1 de este artículo no esté dirigida a cometer uno de los delitos especificados en los artículos 2 a 5 del acuerdo. Esto incluye situaciones como pruebas autorizadas o la protección de un sistema informático. Las naciones tienen la opción de reservarse el derecho de no aplicar el párrafo 1 de este artículo, siempre y cuando esta reserva no afecte la venta, distribución u otras formas de disponibilidad de los elementos mencionados en el apartado 1 a) ii) de este artículo. (Consejo de Europa, 2001)

2. Título 2 – Delitos Informáticos

2.1. Falsificación Informática. -

2.1.1. Chile.

En la normativa chilena este delito se encuentra tipificado en la Ley Núm. 21.459 en el artículo cinco y en este se establece que quien, de manera inapropiada, modifique, altere, dañe o elimine datos informáticos con la intención de hacer que se consideren como verdaderos o sean utilizados para crear documentos

auténticos, será penalizado con una condena de presidio menor en sus grados intermedio a máximo. (Congreso Nacional de Chile, 2022)

Si esta acción es realizada por un funcionario público en abuso de su cargo, será castigado con una pena más severa, que va desde el presidio menor en su grado máximo hasta el presidio mayor en su grado mínimo.

Este artículo de la ley chilena enfoca la penalización de acciones relacionadas con la manipulación de datos informáticos con el fin de hacer que se consideren auténticos o sean usados para crear documentos genuinos. En su primer párrafo, describe que cualquier persona que de manera indebida introduzca, altere, dañe o elimine datos informáticos con el objetivo de que se perciban como auténticos o se utilicen para generar documentos auténticos, estará sujeta a una condena que varía desde el presidio menor en sus grados intermedio a máximo.

El mismo busca sancionar la manipulación malintencionada de datos, reconociendo la importancia de mantener la integridad y autenticidad de la información almacenada en sistemas informáticos. Asimismo, la ley contempla una agravante específica en caso de que la acción sea llevada a cabo por un funcionario público en abuso de su cargo. En tal situación, se impone una pena más severa, extendiéndose desde el presidio menor en su grado máximo hasta el presidio mayor en su grado mínimo.

Pretende proteger la validez y autenticidad de la información digital y establece penalizaciones que reflejan la gravedad de las acciones de manipulación o alteración de datos informáticos, especialmente cuando son perpetradas por funcionarios públicos en un contexto de abuso de poder. Su objetivo fundamental es

mantener la integridad de los sistemas informáticos y disuadir prácticas fraudulentas que comprometan la veracidad de la información almacenada en estos sistemas.

2.1.2. Conclusión “Falsificación informática” y Convenio Budapest.

En Chile, se aborda la manipulación indebida de datos informáticos, condenando la alteración, daño o eliminación de datos con penas desde el presidio menor en sus grados intermedio a máximo. Se reconoce la importancia de proteger la autenticidad e integridad de la información digital, aumentando las penas si la acción es perpetrada por un funcionario público abusando de su cargo. El propósito fundamental es preservar la validez de la información en sistemas informáticos y desalentar la conducta fraudulenta.

En el Convenio Budapest el delito de Fraude Informático establece que cada país deberá implementar las leyes y disposiciones necesarias para considerar como un crimen, en su jurisdicción interna, la manipulación, modificación, eliminación o supresión deliberada e ilegítima de datos informáticos con el propósito de generar información falsa que pueda ser presentada o utilizada como auténtica en asuntos legales, independientemente de si los datos son legibles o comprensibles de manera directa. Algunos países pueden requerir la presencia de una intención dolosa o de naturaleza delictiva similar para establecer la responsabilidad penal. (Consejo de Europa, 2001)

2.2. Fraude Informático. –

2.2.1. Perú.

En la normativa peruana este delito se encuentra positivizado por el artículo 8 “Fraude Informático” en la Ley No. 30171 que modifica a la anterior norma, “Ley 30096”, que regulaba los delitos informáticos.

En el mismo se establece que la persona que intencionalmente busque obtener un beneficio ilegítimo perjudicando a un tercero mediante el diseño, introducción, alteración, eliminación, supresión o duplicación de datos informáticos, o cualquier tipo de intervención o manipulación en el funcionamiento de un sistema informático, enfrentará una pena de prisión no menor de tres años ni mayor de ocho, además de sesenta a ciento veinte días de multa. Si la acción afecta el patrimonio del Estado destinado a actividades de asistencia o programas de apoyo social, la pena será más severa, con una privación de libertad que oscilará entre cinco y diez años, acompañada de ochenta a ciento cuarenta días de multa. (Congreso de la Republica de Perú, 2014)

El artículo se enfoca en abordar acciones ilícitas relacionadas con la informática que persiguen obtener un beneficio indebido perjudicando a terceros. Estipula que la manipulación, alteración, eliminación, duplicación o cualquier intervención en sistemas informáticos con la finalidad de obtener ventajas indebidas conlleva penas de prisión que van desde tres hasta ocho años, acompañadas de multas entre sesenta y ciento veinte días. (Congreso de la Republica de Perú, 2014)

Adicionalmente, destaca que, si estas acciones afectan el patrimonio estatal dedicado a labores de asistencia o programas de apoyo social, las sanciones serán más rigurosas, imponiendo penas de prisión que fluctúan entre cinco y diez años, junto con multas de ochenta a ciento cuarenta días.

Este artículo busca prevenir y sancionar comportamientos que interfieran con la operatividad normal de sistemas informáticos, asegurando la integridad de la información y protegiendo los intereses de terceros y del Estado. Las sanciones son proporcionales a la gravedad de los perjuicios ocasionados, demostrando especial

preocupación por resguardar los recursos dirigidos a actividades sociales y de asistencia, con el propósito de desincentivar acciones que puedan afectar negativamente estos ámbitos.

2.2.2. Chile.

En la legislación del país del sur el delito de “Fraude Informático” se encuentra en el artículo siete de la Ley Núm. 21.459 y en el mismo se establece que quien, con el propósito de obtener ganancias económicas para sí mismo o para otro, altere un sistema informático causando daño a otro individuo, ya sea a través de la manipulación, modificación, daño o eliminación de datos, o por cualquier intervención en el funcionamiento del sistema informático, será sancionado de la siguiente manera:

1) Si el daño supera los cuarenta valores tributarios mensuales, la pena será de presidio menor en sus grados medio a máximo y una multa entre once y quince unidades tributarias mensuales.

2) Si el daño está entre cuatro y cuarenta valores tributarios mensuales, la pena será de presidio menor en su grado medio y una multa entre seis y diez unidades tributarias mensuales.

3) Si el daño no excede las cuatro unidades tributarias mensuales, la pena será de presidio menor en su grado mínimo y una multa entre cinco y diez unidades tributarias mensuales.

Si el daño supera las cuatrocientas unidades tributarias mensuales, se impondrá la pena de presidio menor en su grado máximo y una multa entre veintiuna y treinta unidades tributarias mensuales.

Asimismo, se considerará autor del delito a aquel que, con conocimiento o pudiendo conocer la ilicitud de la conducta mencionada en el primer párrafo, facilite los medios para cometer el delito. (Congreso Nacional de Chile, 2022)

El artículo especifica las sanciones para aquellos que, con la intención de obtener beneficio económico para sí mismos o terceros, manipulen un sistema informático. En primer lugar, define tres categorías de penalización en relación con el valor del perjuicio causado cuando el mismo supera las cuarenta unidades tributarias mensuales, se establece una condena de presidio menor en sus grados medio a máximo y una multa entre once y quince unidades tributarias mensuales.

Si el perjuicio está entre cuatro y cuarenta unidades tributarias mensuales, la pena será de presidio menor en su grado medio y una multa entre seis y diez unidades tributarias mensuales o si este no excede las cuatro unidades tributarias mensuales, la sanción será de presidio menor en su grado mínimo y una multa de cinco a diez unidades tributarias mensuales.

En casos donde el perjuicio supere las cuatrocientas unidades tributarias mensuales, se impone la pena más severa: presidio menor en su grado máximo y multa entre veintiuna y treinta unidades tributarias mensuales.

Además, se incluye una disposición sobre la complicidad en el delito, considerando autor a aquel que, conociendo o pudiendo conocer la ilegalidad de la conducta descrita inicialmente, facilita los medios para cometer el delito. Esta disposición amplía la responsabilidad a individuos que colaboren en la comisión del delito, independientemente de su participación directa en la manipulación del sistema informático.

2.2.3. Conclusión “Fraude Informático” y Convenio Budapest.

Las leyes de Perú y Chile se ocupan de abordar acciones ilícitas relacionadas con la manipulación de sistemas informáticos, aunque difieren en sus enfoques y sanciones.

En Perú, se penaliza la intención de obtener un beneficio ilícito dañando a terceros mediante la manipulación de datos informáticos o la interferencia en sistemas informáticos. Las sanciones van desde tres hasta ocho años de prisión, con multas de sesenta a ciento veinte días. Si este acto afecta al patrimonio estatal destinado a actividades sociales, las penas aumentan notablemente, oscilando entre cinco y diez años de prisión, junto con ochenta a ciento cuarenta días de multa.

En contraste, la legislación chilena penaliza a quienes causan perjuicio a otros con el objetivo de obtener ganancias económicas manipulando un sistema informático. Las penas varían según el perjuicio ocasionado, desde el presidio menor hasta multas, en función de la magnitud del daño provocado.

En resumen, ambas leyes tienen como objetivo prevenir y castigar conductas que dañan la integridad de sistemas y datos informáticos. La normativa peruana se centra en el perjuicio causado a terceros y al Estado, imponiendo sanciones proporcionales a la afectación, mientras que la ley chilena considera más el daño económico causado y establece penas basadas en esa consideración.

En cuanto al Convenio Budapest, este en su artículo ocho establece que los países implementarán las leyes o acciones pertinentes para considerar como un crimen en su sistema legal interno cualquier acción deliberada e ilegítima que cause daño económico a otra persona mediante la manipulación, alteración, eliminación o supresión de datos informáticos. Esto incluye cualquier interferencia en el funcionamiento de un sistema informático con la intención dolosa o de naturaleza

delictiva de obtener un beneficio económico ilegal para uno mismo o para terceros. (Consejo de Europa, 2001)

2.3. Delitos relacionados con la pornografía infantil.

2.3.1. Chile.

En la legislación de este país se encentra tipificado esta conducta por la Ley Núm. 21.522 la cual fue creada en el año 2022 para ser introducida en el título séptimo del libro segundo del código penal de este país. En el artículo 367 del código penal chileno establece que quien promueva o facilite la explotación sexual de un individuo menor de dieciocho años será condenado a una pena de presidio mayor en su grado mínimo. (Congreso Nacional de Chile, 1874)

En caso de que este delito se cometa explotando a la víctima debido a su dependencia personal o económica, o si se lleva a cabo de manera habitual, la pena será de presidio mayor en cualquiera de sus grados, además de una multa que oscilará entre treinta y una a treinta y cinco unidades tributarias mensuales. (Congreso Nacional de Chile, 1874)

Para los efectos mencionados en el primer párrafo, se define la explotación sexual como la utilización de una persona menor de dieciocho años para realizar acciones de índole sexual a cambio de cualquier forma de compensación hacia la víctima o hacia terceros. (Congreso Nacional de Chile, 1874)

El marco legal establece castigos para aquellos que fomenten o faciliten la explotación sexual de menores de dieciocho años. En una primera instancia, impone una pena de presidio mayor en su nivel mínimo para quienes cometen este delito, no obstante, si la explotación se realiza aprovechando la dependencia personal o económica de la víctima, o si se verifica una repetición habitual de esta conducta, la

sanción será más severa, llegando al presidio mayor en cualquiera de sus grados, acompañada de una multa que oscilará entre treinta y una y treinta y cinco unidades tributarias mensuales.

El artículo define explotación sexual como la utilización de una persona menor de dieciocho años para participar en acciones de naturaleza sexual, a cambio de alguna forma de retribución dirigida tanto a la víctima como a terceros. El objetivo principal de este artículo es imponer sanciones contundentes contra conductas que afectan gravemente la integridad y los derechos de los menores. Además, introduce circunstancias agravantes si se abusa de situaciones de vulnerabilidad o si el delito se comete repetidamente.

De la misma manera en la legislación se encuentra el artículo 367 quáter el cual define que quien comercie, importe, exporte, distribuya, divulgue o presente material pornográfico o de explotación sexual, en cualquier forma de presentación, donde personas menores de dieciocho años hayan sido utilizadas en su elaboración, será castigado con la pena de presidio menor en su grado máximo. (Congreso Nacional de Chile, 1874)

La misma sanción mencionada en el párrafo anterior se aplicará a aquel que participe en la creación de este tipo de material pornográfico o de explotación sexual, quien de forma malintencionada almacene o adquiera material pornográfico o de explotación sexual, sin importar su formato, en el que personas menores de dieciocho años hayan sido utilizadas en su producción, será sancionado con presidio menor en su grado medio. (Congreso Nacional de Chile, 1874)

Para los propósitos de este artículo, se entenderá como material pornográfico o de explotación sexual, aquel que presente a menores de dieciocho años

involucrados en actividades sexuales explícitas, reales o simuladas, o que exhiba sus genitales con propósitos mayormente sexuales, o cualquier representación de estos menores donde se utilice su voz o imagen con los mismos fines.

El análisis del código penal se centra en delitos asociados a la explotación sexual de menores de dieciocho años, así como en la manufactura, distribución y tenencia de material pornográfico o de explotación sexual que implique a menores. (Congreso Nacional de Chile, 1874)

Se penaliza la promoción o facilitación de la explotación sexual de menores con penas de presidio mayor en su grado mínimo, agravadas en situaciones donde la víctima es explotada debido a su dependencia personal o económica, o cuando la acción es frecuente. Se define la explotación sexual como la utilización de menores en actividades sexuales a cambio de retribución. Se establecen castigos de presidio menor en su grado máximo para quien obtenga acciones sexuales de menores a cambio de alguna forma de retribución. (Congreso Nacional de Chile, 1874)

Asimismo, se sanciona la comercialización, producción y posesión de material pornográfico o de explotación sexual que involucre a menores, con penas que varían según la conducta delictiva, desde presidio menor en su grado máximo para la comercialización, hasta presidio menor en su grado medio para la posesión maliciosa de este material.

Los artículos siguientes abordan aspectos relativos a la comisión de estos delitos en el ámbito nacional y establecen disposiciones sobre reincidencia y la responsabilidad de autoridades o individuos con roles educativos o en contextos relacionados con menores.

Cuando estos delitos son perpetrados por autoridades, personas con roles educativos o en perjuicio de menores en contextos educativos o de transporte escolar, las penas serán más severas, salvo en casos donde exista violencia, intimidación, abuso de relación de dependencia, abuso de autoridad o confianza.

En síntesis, estos artículos abordan distintas formas de explotación sexual y conductas ilícitas relacionadas con la elaboración, distribución y posesión de contenido pornográfico o de explotación sexual que involucran a menores, teniendo en cuenta factores agravantes según el rol o posición de quien comete el delito.

2.3.2. Conclusión “Delitos relacionados con la pornografía infantil” y Convenio Budapest.

La legislación nacional chilena cuenta con disposiciones claras que penalizan la explotación sexual de menores y actividades relacionadas con la producción, distribución y posesión de material pornográfico que involucra a menores. Las penas varían según la gravedad del delito, desde sanciones más severas para quienes promueven la explotación hasta castigos menores para la posesión indebida de dicho material. Estos artículos también consideran circunstancias agravantes según el rol del perpetrador.

El Convenio Budapest establece que cada nación implementará medidas legales y otras disposiciones necesarias para considerar como un delito dentro de su marco jurídico interno la realización deliberada e ilegítima de los siguientes actos: la producción de pornografía infantil con la intención de difundirla a través de sistemas informáticos; la oferta o disponibilidad de pornografía infantil mediante sistemas informáticos; la difusión o transmisión de pornografía infantil a través de sistemas informáticos; la obtención de pornografía infantil para uno mismo o para

terceros a través de sistemas informáticos; y la posesión de pornografía infantil en un sistema informático o dispositivo de almacenamiento de datos informáticos.

Para los propósitos mencionados en el párrafo anterior, se entenderá por "pornografía infantil" cualquier material pornográfico que muestre la representación visual de un menor participando en conductas sexualmente explícitas, o una representación realista de una persona que parezca ser menor y participe en conductas sexualmente explícitas.

En referencia al párrafo anterior, se considerará "menor" a cualquier individuo menor de 18 años. Sin embargo, las naciones podrán establecer un límite de edad menor, que deberá ser de al menos 16 años. Además, las naciones podrán reservarse el derecho de no aplicar total o parcialmente los incisos d) y e) del párrafo 1, así como los incisos b) y c) del párrafo 2. (Consejo de Europa, 2001)

Delitos Electrónicos Y Su Positivización En Ecuador. –

El Código Penal Ecuatoriano y el Convenio de Budapest sobre Ciberdelincuencia comparten objetivos en la regulación de delitos informáticos y la protección de datos. Analicemos las similitudes y diferencias entre los artículos del código ecuatoriano relacionados con delitos informáticos y el contenido del Convenio de Budapest:

Artículos del Código Penal Ecuatoriano:

1. Revelación ilegal de base de datos (Artículo 229): Prohíbe revelar información protegida en sistemas electrónicos o informáticos, penalizando la violación de la privacidad con penas de uno a tres años, aumentando a tres a cinco años si el infractor es un servidor público o empleado bancario.

2. Interceptación ilegal de datos (Artículo 230): Establece penas de tres a cinco años para acciones como la interceptación no autorizada de datos, diseño de contenido digital para engañar o copia no autorizada de información de tarjetas de crédito.

3. Transferencia electrónica de activo patrimonial (Artículo 231): Penaliza la manipulación de sistemas informáticos con fines de transferencia ilegal de activos, castigando con penas de tres a cinco años.

4. Ataque a la integridad de sistemas informáticos (Artículo 232): Se sanciona con penas de tres a cinco años la alteración o daño deliberado de sistemas informáticos o tecnológicos con el fin de obstaculizar su funcionamiento.

5. Delitos contra la información pública reservada legalmente (Artículo 233): Castiga la destrucción u obtención ilícita de información clasificada, imponiendo penas de cinco a diez años.

6. Acceso no consentido a sistemas informáticos (Artículo 234): Sanciona el acceso no autorizado a sistemas informáticos, imponiendo penas de tres a cinco años, aumentando a cinco años si se explota dicho acceso para beneficio propio.

7. Falsificación informática (Artículo 234.1): Penaliza la manipulación de datos para generar documentos falsos con penas de tres a cinco años.

8. Agravación de penas por afectación a sistemas críticos (Artículo 234.2): Incrementa las penas en un tercio si el delito causa una grave perturbación en sistemas críticos.

9. Responsabilidad de personas jurídicas (Artículo 234.3): Establece la responsabilidad de personas jurídicas en los delitos de esta sección.

Comparación con el Convenio de Budapest:

El Convenio de Budapest complementa estos principios al abordar la cooperación internacional para combatir delitos cibernéticos y propone estándares para la regulación de la ciberdelincuencia, como:

1. Cooperación internacional: El Convenio destaca la importancia de la cooperación internacional para investigar y perseguir delitos cibernéticos.

2. Normas comunes: Propone estándares comunes entre países para la penalización y regulación de delitos informáticos.

3. Privacidad y protección de datos: Busca proteger la privacidad y la integridad de los datos en línea.

4. Responsabilidad de personas jurídicas: Aborda la responsabilidad penal de entidades corporativas en delitos cibernéticos.

Aunque el Código Penal Ecuatoriano aborda en detalle una amplia gama de delitos informáticos, el Convenio de Budapest ofrece directrices más amplias y estándares comunes para la cooperación internacional en la lucha contra la ciberdelincuencia.

En conclusión, es correcto establecer que, si bien la legislación ecuatoriana posee un catálogo de delitos electrónicos amplio y relativamente suficiente, los resultados no funcionan o no se dan como se debería esperar teniendo en cuenta lo anterior, a criterio del investigador Ecuador necesita poner en función las estructuras estales responsables de hacer uso de la norma y emplear las herramientas que esta brinda.

Además, aun con lo mencionado es necesaria la ratificación del Convenio Budapest sobre ciberdelincuencia ya que el país se beneficiaria de este en aspectos como:

1. Cooperación Internacional: El convenio promueve la cooperación entre países para investigar, prevenir y combatir delitos cibernéticos. Al ratificarlo, Ecuador podría acceder a un marco legal internacional que facilita la colaboración con otros países en la persecución de estos delitos.

2. Armonización Legal: El convenio establece estándares comunes para la definición de delitos informáticos y las medidas penales aplicables, lo que ayudaría a Ecuador a armonizar su legislación con las normativas internacionales, facilitando así la cooperación legal con otras naciones en casos de ciberdelincuencia.

3. Protección de Datos: Al ratificar el convenio, Ecuador se comprometería a resguardar la privacidad y seguridad de los datos en línea, proporcionando un marco legal más robusto para combatir la violación de la privacidad y otros delitos relacionados con la información.

4. Persecución Efectiva: La ratificación del convenio permitiría a Ecuador tener acceso a herramientas y recursos legales para perseguir y sancionar más eficazmente a los responsables de delitos informáticos, asegurando un enfoque más efectivo en la lucha contra la ciberdelincuencia.

5. Prevenir la impunidad: Al adoptar las medidas y herramientas estipuladas en el convenio, Ecuador podría fortalecer su capacidad para evitar que los delincuentes informáticos eludan la justicia al operar a través de fronteras internacionales.

En síntesis, la adhesión al Convenio de Budapest tendría el potencial de reforzar la habilidad de Ecuador para enfrentar el crimen cibernético a través de una mayor colaboración entre naciones, la alineación legal y una mayor salvaguardia de la información en línea.

CAPITULO II

METODOLOGIA DE LA INVESTIGACION

Metodología De La Investigación

El marco metodológico es el conjunto de acciones destinadas a describir y analizar el fondo del problema planteado, a través de procedimientos específicos que incluye las técnicas de observación y recolección de datos, determinando el "cómo" se realizará el estudio. (Azuero, 2019)

Este proyecto de investigación será de naturaleza correlativo ya que analizaran las variables para determinar si la ratificación del Convenio de Budapest sobre la Ciberdelincuencia crearía una mejora en el sistema penal nacional y si este es posible dada la legislación actual, se recolectarán datos de diversos autores, así como el empleo de métodos cualitativos para determinar la respuesta a la pregunta problémica que se plantea en este trabajo investigativo.

La técnica a utilizar será la técnica documental que permite la recopilación de información que permitirá analizar lo planeado y las fuentes de información bibliográfica como tesis de posgrado, revistas científicas, casos judiciales y, además, se aplicará la técnica de entrevistas a jurisconsultos conocedores de la presente materia a tratar a fin de que sus conocimientos ayuden a aportar a la actual investigación a desarrollar.

1. Método de Investigación

Enfoque de la investigación

Cualitativa:

Sobre el enfoque cualitativo los doctores Marini y Espínola infieren que, en la búsqueda de conocimiento científico, se destacan enfoques metodológicos identificados como cualitativos, los cuales se centran en el estudio de sus objetos de

investigación a través de técnicas e instrumentos específicos. Estas metodologías permiten obtener información directamente de los individuos involucrados en el fenómeno en cuestión, ya sea recopilando sus experiencias, opiniones, historias de vida, entre otros, o analizando documentos, informes, normativas escritas, archivos y cualquier material auténtico que contenga datos relevantes para describir detalladamente una situación o fenómeno específico. (Marini & Espíndola, 2016)

En esta investigación esto se materializa usando, opiniones y definiciones de autores, juristas y especialistas sobre los delitos electrónicos, se revisó bibliografía variada tanto de jurisprudencia como las normas de los países que se tomaron de muestra para la comparación de las jurisprudencias, realizando así un análisis documental.

Método de la Investigación:

Investigación Descriptiva

Una investigación descriptiva es un tipo de estudio científico que se enfoca en describir detalladamente un fenómeno, evento, situación o características específicas de una población, grupo o área de interés. Su objetivo principal es proporcionar una representación precisa y sistemática de cómo son las cosas, cómo están estructuradas o cómo se comportan.

Este tipo de investigación se centra en recopilar, organizar, presentar e interpretar datos de manera objetiva, sin manipular variables o intervenir en el entorno estudiado. Por lo general, se utiliza para identificar patrones, tendencias, correlaciones o relaciones entre variables, pero no busca establecer causas o explicar el porqué de un fenómeno.

En síntesis, la investigación descriptiva se dedica a detallar con exactitud las propiedades, comportamientos o características de un fenómeno en un momento particular, sin adentrarse en las causas o relaciones causales.

Técnicas de recolección de información:

Bibliográfica:

La técnica de recolección de información involucra identificar, adquirir y consultar diversas fuentes bibliográficas y otros recursos provenientes de conocimientos anteriores o datos recopilados previamente, con el propósito de utilizarlos de manera pertinente en un estudio específico. (Bastis Consultores, 2020)

Esta forma de recopilar información se basa en fuentes secundarias, es decir, en documentos que actúan como registros de sucesos pasados o históricos.

Dentro de las múltiples fuentes documentales disponibles, se encuentran aquellas de naturaleza hemerográfica, bibliográfica, escrita, audiovisual, visual, cartográfica y objetos tangibles como vestimenta, herramientas de trabajo, obras artísticas o artesanales, edificaciones, entre otras.

Para la realización de este trabajo investigativo se tomó información tanto de autores como de las legislaciones de los países sobre los cuales se realizó la comparación de legislaciones.

Entrevista:

Se realizan entrevistas a cinco profesionales del derecho que realizan actividades relacionadas con el tópico de la investigación, tanto a abogados en libre ejercicio como a un Agente Fiscal que cumple sus funciones en la ciudad de Quito y un académico de la Universidad Ecotec. Las preguntas realizadas en las entrevistas son las siguientes.

Preguntas:

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?
2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?
3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?
4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?
5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?
6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

CAPITULO III

ANALISIS E INTERPRETACION DE RESULTADOS

Análisis e interpretación de resultados

A continuación, se presentan las entrevistas realizadas a profesionales del derecho:

Entrevistas. -

A. Primera entrevista:

La primera entrevista fue realizada al Abogado David Vergara, quien es abogado en libre ejercicio y es profesor de Grado en la universidad Ecotec.

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

Considero personalmente que si es un avance que el ecuador ratifique internamente el Convenio de Budapest, porque así lo han hecho algunos países de la región, tales como Chile, Colombia, México, Costa Rica, Brasil, entre otras naciones que en realidad ven como un avance que exista legislación en materia de delitos electrónicos que sea armónica entre países para solicitar cooperación internacional, al ser este un tipo de delito que puede ser cometido en un país y tener sus efectos en otro, como en Ecuador.

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

Considero que el país no tiene suficientes herramientas, por el hecho de que fiscales, policías y jueces no están capacitados para combatir el delito informático, y en el ámbito privado las empresas invierten muy poco en contratar sistemas de ciberseguridad o de mecanismo para salvaguardar la información sensible, personal y privada de las empresas, por esa razón es importante cambiar el paradigma mental de muchas personas en el país para que vean la importancia de implementar sistemas de protección contra los delitos informáticos.

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

Consideraría que más que ratificar otro convenio internacional creería que Ecuador debería al menos tratar de concientizar la importancia a nivel del ciudadano de la protección de la información y también de los sistemas de ciberseguridad, entonces bajo ese criterio se debería tratar de incentiva a que las empresas, especialmente los bancos establezcan mecanismos más robustos de ciberseguridad y plantear multas en caso de que así no lo prevean, y con relación a las personas brindar capacitación a nivel estatal de la importancia de proteger la información personal y cuáles son las recomendaciones que se debería adoptar para que se pueda las probabilidades de ser víctima de uno de estos delitos.

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

Ecuador si tiene una regulación moderna de delitos informáticos en el COIP, tenemos entre 15 y 20 figuras delictuales, las cuales han sido reformadas y modificadas a lo largo de tiempo para adaptarse a estas nuevas realidades, entonces yo si pienso que si cumple Ecuador los estándares que incluso establece el convenio de Budapest, pero la importancia no va a estar tanto en la norma sino más bien en la prevención que debería ser algo del ciudadano.

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

El único cambio que representaría el convenio de Budapest seria la posibilidad de solicitar una extradición, pero como es un tratado internacional el mismo convenio señala la posibilidad de cuando dos países hayan adoptado internamente el convenio, se hayan adherido, eso tiene como resultado que se puede pedir cooperación internacional y pedir extradición de delincuentes que hayan cometido delitos que tengan efecto en un país y se hayan fugado a otro país.

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos

informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

Sí, podría mejorar ciertos artículos del Código Integral Penal de delitos informáticos, pero, consideró que el problema no radica tanto en la tipificación de la norma sino más bien en la prevención de la conducta, y ahí es cuando se deberían optar por mecanismos de ciberseguridad para poder resguardar la información personal, es decir que la protección debería existir “ex ante” y no “ex poste” al cometimiento de la infracción.

B. Segunda Entrevista:

Esta entrevista se realizó a la abogada María Belén Bernal quien es abogada en libre ejercicio y trabaja en un estudio jurídico en el cual ella se encarga de tomar casos de índole informático.

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

Si, puesto que la rama de derecho electrónico y los delitos informáticos no tiene gran campo de estudio en la actualidad. Considerando que es una rama relativamente nueva por los avances tecnológicos que enfrentamos día a día esto fortalecería los conocimientos sobre el tema muy importante.

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

No, puesto que comúnmente la ciudadanía en general no conoce los delitos informáticos que no solo constan desde falsificación de datos, va mucho más allá desde tenencia de pornografía infantil hasta la divulgación de la misma.

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

Considero que el protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de

sistemas informáticos, podría complementar al mejoramiento de la regulación de delitos electrónicos en el país.

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

No, puesto que no existe una correcta clasificación de los delitos informáticos dentro del COIP, ya que menciona que se dan por medios informáticos más no se lo identifica como un delito informático.

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

No creo que habría alguna repercusión negativa, lo que si ocurriría es que se establecería una correcta clasificación e identificación homogénea con respecto a los demás países de la región que han ratificado el convenio, de los delitos dentro del COIP.

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

Si, sería correcto, pondría un orden a la normativa y realizaría la importancia de la regulación de los delitos informáticos y la necesidad de la cooperación internacional.

C. Tercera entrevista:

Esta entrevista fue realizada el Agente fiscal, el abogado Christian Arregui Cueva quien trabaja en Quito como parte de la fiscalía general del Estado.

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

Es, definitivamente necesario, tanto la ratificación como la necesidad de que el país tome medidas para que los organismos del estado regulan estos temas, capaciten a sus integrantes en la importancia de este tema, tanto así que yo siendo agente de fiscalía desconocía de la existencia del tratado.

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

Creo que el país afronta una situación en la que debemos mejorar en términos de seguridad para los ciudadanos desde todos los ámbitos, incluyendo la ciberseguridad, entonces no, no creo que actualmente el sistema estatal cuente con las herramientas necesarias para cubrir la demanda de seguridad.

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

Como ya te mencioné, yo desconocía de la mera existencia del convenio Budapest, en todo caso no conozco de ningún tratado de esta índole que pueda beneficiar al país, sin embargo, creo que es necesario que la función judicial tome cartas en el asunto.

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

Los artículos están, el COIP presenta algunos artículos de delitos informáticos, pero te comento que en el ejercer del día a día no me han llegado muchos casos que yo recuerde de esta índole, y eso que llevo trabajando en la fiscalía alrededor de 15 años ya, creo que tanto el pueblo como el estado necesitan reconocer la importancia de la seguridad de los datos personales y demás afectaciones que conllevan la práctica de estas conductas antijurídicas.

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

No, pero como ya te comenté desconozco exactamente cuáles son las implicaciones de la ratificación del convenio, además no conozco que incluye el convenio aparte de lo que me has mencionado. (Se hace conocer al entrevistado de que el convenio incluye la posibilidad de la extradición) Ah bueno, eso sí sería algo importante y la verdad ayudaría mucho a resolver casos en la fiscalía.

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

No creo que sea necesario, creo que el COIP cumple con tipificar estas conductas, quizás una reforma para agregar artículos faltantes o mejorar uno que otro, pero no creo que sea conveniente crear una ley nueva.

D. Cuarta entrevista:

Esta entrevista fue realizada a la abogada María Nicole Anzules quien es abogada en libre ejercicio y trabaja mayormente con casos penales y ha llevado casos de delitos informáticos.

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

La ratificación del Convenio Internacional Budapest podría ser considerada como una herramienta valiosa para Ecuador en la lucha contra delitos cibernéticos. El convenio proporciona un marco legal que promueve la cooperación internacional y la armonización de leyes para combatir eficazmente los delitos informáticos.

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

Respecto a las herramientas del sistema judicial para combatir delitos electrónicos, creo que el país cuenta con una legislación actualizada, sin embargo, entidades

como la fiscalía o el consejo de la judicatura, no cuentan, en mi criterio, con agentes capacitados para llevar causas de este estilo, mayormente porque no existe en el país mucha jurisprudencia con la que trabajar.

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

Además del Convenio Budapest, existen otros acuerdos y tratados internacionales que podrían ser considerados para mejorar la regulación de delitos electrónicos en el país. Sin embargo, la elección de un mecanismo específico dependerá de las necesidades y prioridades del sistema legal ecuatoriano.

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

La tipificación de los delitos informáticos en el COIP puede ser una medida inicial para regular estas actividades delictivas. Sin embargo, se debe revisar periódicamente para asegurar que esté actualizado y refleje adecuadamente las complejidades y avances en el ámbito de la tecnología y la ciberseguridad.

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

La ratificación del Convenio Budapest probablemente implicaría cambios en el sistema normativo del país, lo que puede resultar beneficioso al fortalecer la lucha contra la ciberdelincuencia. No obstante, se deben analizar cuidadosamente los posibles efectos y ajustes necesarios en las leyes nacionales, pero realmente no creo que el país reciba algún efecto contraproducente.

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos

informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

Considerar como referencia los países que ya han ratificado el Convenio Budapest, como Chile, para crear un proyecto de ley que tipifique los delitos informáticos y regule la cooperación internacional puede ser una estrategia valiosa. Sin embargo, es crucial adaptar estas medidas al contexto y necesidades específicas del país, garantizando la protección de los derechos y libertades individuales. Pero si, creo que podría ser una buena idea.

E. Quinta entrevista.

Esta quinta y última entrevista fue realizada a la abogada Margarita Cabrera Cevallos, quien es abogada en libre ejercicio y se encuentra cruzando su doctorado en Derecho de Investigación.

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

Si, creo que el país necesita de manera urgente la colaboración internacional que brindaría la ratificación del convenio, porque ha quedado claro que, a pesar de contar con la normativa, el estado no es capaz de cumplir con la función de proteger a la ciudadanía de este tipo de actividad ilícita.

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

Creo que sí y no, el estado tiene las herramientas, mas no al personal capacitado para hacer uso de estas, tanto como a la población que no comprende ni atiende mucho a la importancia de la protección de los datos personales, así como los funcionaros estatales que desconocen lo serio de la situación del país en cuanto a ciber seguridad, y realmente es relativamente comprensible, teniendo en cuenta el ambiente de violencia que atraviesa el Ecuador.

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

No creo que la solución sea ratificar más tratados, al menos no por ahora, lo que sí creo es que el país necesita capacitarse acerca de ciberseguridad y acerca de las medidas que pueden tomar para protegerse de estas actividades punibles, y hablo de capacitar a la población en general, tanto empresas privadas como empresas públicas, en realidad a todos quienes conformamos el estado.

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

Definitivamente no, pero no es porque la tipificación del código penal esta tan inconclusa o no exista la tipificación de los delitos informáticos, porque la solución no está únicamente en crear norma, como ya te mencioné, en mi opinión necesario que todos quienes conformamos el estado tomemos cartas en el asunto y nos esforcemos en mejorar la situación actual que nos tiene por el piso ante la comunidad internacional.

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

No, no creo que la ratificación del tratado traiga resultados contraproducentes, sin embargo, sí creo que es necesario que se haga bien para que no quede en vano.

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

Me parece una idea interesante, y creo que podría ser útil para crear conciencia y dale la importancia que requiere a la ciberseguridad, sin embargo, no me parece que sea del todo necesario, porque realmente el articulado del COIP no dista tanto de lo que se expresa en el Convenio de Budapest.

2. Análisis e interpretación de resultados

Preguntas:

1- ¿Calificaría usted de necesario para el país que se dé la ratificación del Convenio Internacional Budapest (que trata sobre los delitos cibernéticos y la colaboración internacional para la lucha contra los mismos)? Si, no, ¿Por qué?

2- ¿Cree usted que el sistema judicial del país tiene herramientas suficientes para la lucha contra delitos de tipo electrónicos? Si, no, ¿Por qué?

3- Sin contar con el Convenio Budapest de Ciberseguridad, ¿Qué otro mecanismo, tratado, o convenio recomendaría usted para el mejoramiento de la regulación de delitos electrónicos en el país?

4- ¿Considera usted que la tipificación actual presentada en el COIP en cuanto la regulación de delitos informáticos cumple la función de regular este tipo de actividades delictivas?

5- ¿Cree usted que la ratificación del convenio sobre la ciberdelincuencia Budapest presentaría cambios al sistema normativo del país que podrían desenvolver en resultados contraproducentes?

6- ¿Cree usted que sería correcto que se tome como ejemplo lo que han hecho países en los que ya se encuentra ratificado el Convenio Budapest, como Chile, y crear un proyecto de ley en el cual se tipifiquen todos los delitos informáticos, tomando como referencia el catálogo de delitos redactado en el Convenio Budapest, y de esta manera convertir al articulado del código penal que habla sobre delitos informáticos en leyes penales en blanco y además, en el mismo, se regule la forma en la cooperación internacional?

Entrevistados:

Abogado David Vergara; Abogada María Belén Bernal; Abogado Christian Arregui Cueva; Abogada María Nicole Anzules; Abogada Margarita Cabrera Cevallos.

A continuación, se realiza el análisis de las preguntas que se realizaron en la entrevista para esto, se presenta una tabla que resume las respuestas:

Tabla 1. Resultados

Entrevistados _____ **Preguntas/ Respuestas**	**#1**	**#2**	**#3**	**#4**	**#5**
#1	Si	Si	Si	Si	Si
#2	No	No	No	No	Sí y No (Razones ambivalentes)
#3	Enfatiza medidas internas	Convenio adicional referente a delitos racistas y xenófobos	Desconoce convenios	No realiza propuesta	Propone capacitación sobre seguridad informática
#4	Si	No	Respuesta Ambigua	Respuesta parcial	No

#5	No	No	No	No	No
#6	Si	Si	No	Si	Ambivalente (Interesante, no necesario)

Cada abogado presenta una perspectiva única sobre la necesidad y la viabilidad de ratificar el Convenio Internacional Budapest y otros aspectos relacionados con la regulación de delitos electrónicos en Ecuador. Los puntos de vista varían desde la necesidad urgente de cooperación internacional hasta la importancia de la capacitación en ciberseguridad y la posible adecuación de las leyes nacionales a los estándares internacionales.

CAPÍTULO IV
PROPUESTA

Propuesta

La propuesta a la que se llegó tras realizar esta investigación es principalmente, la posibilidad de crear un proyecto de ley en el cual se logren concentrar todos los delitos de acuerdo a como se encuentran redactadas en el convenio internacional Budapest para de esta manera facilitar la ratificación del mismo y poder tener una normativa homogénea que en la cual se regulen únicamente estos delitos para así, tomando como ejemplo lo que ha hecho Chile en su normativa para poder ratificar el Convenio de Budapest.

Conclusión

Como conclusión luego de realizadas las entrevistas a los profesionales y realizar la comparación con las legislaciones extranjeras, es correcto decir que, como país, si bien es cierto contamos con una normativa que se podría establecer como suficiente, esta no refleja la situación en la que se encuentra el país, que cabe recalcar, organismos internacionales califican como crítica.

Entonces definitivamente poseer esta legislación no es suficiente, y como lo mencionan los profesionales entrevistados, es necesario que el país tome asunto de la importancia y la necesidad de tomar medidas que protejan a los ciudadanos de ataques cibernéticos, los cuales pueden ir desde poner en jaque a distribuidores de servicios de comunicación nacionales, o afectar a la economía por hackear la pagina web de un bando de influencia nacional.

Recomendaciones

Como recomendación, y basado en lo expuesto en la conclusión, es imperativo que se realicen capacitaciones a los agentes responsables de salvaguardar la seguridad de los ciudadanos, esto refiriéndose tanto a servidores

públicos que trabajen para órganos como la Fiscalía así como a los que dirigen y toman decisiones, y no únicamente a los representantes de estos, si no también a aquellos que se encargan de crear, aprobar y modificar las normas y los mecanismos que posee el estado para la constante lucha contra la delincuencia que, es indudable decir que siempre se va a encontrar a la vanguardia de los mecanismos para llevar acabo los actos punitivos que afectan a todos los miembros del país.

Además, es imperativo que se cree conciencia en la población en general y se promueva una cultura de ciberseguridad que pueda actuar como escudo ante estos delitos mundiales.

BIBLIOGRAFÍA

(n.d.).

Statista Research Department. (2023, julio 7). *Statista*. https://www.statista.com/statistics/210346/net-revenue-of-symantec/#:~:text=Its%20revenue%20in%20fiscal%20year%202022%20stood%20at%203.3%20billion%20U.S.%20dollars.

Asociación Ecuatoriana de Ciberseguridad . (2021). *Asociación Ecuatoriana de Ciberseguridad* . Asociación Ecuatoriana de Ciberseguridad : https://www.change.org/p/adhesi%C3%B3n-de-ecuador-al-convenio-de-budapest-contra-el-cibercrimen-lassoguillermo-asambleaecuador-cancilleriaec?utm_content=cl_sharecopy_29436874_es-419%3A3&recruiter=1211644598&utm_source=share_petition&utm_medium=copylink&ut

Azuero, Á. E. (2019). Significatividad del marco metodológico en el desarrollo de proyectos de investigación. *Revista Arbitrada Interdisciplinaria KOINONIA, IV*(8), 112.

Banco Central del Ecuador Subgerencia de Análisis de Productos y Servicios. (2020). *Camarón Ecuatoriano en el Mundo.*

Bastis Consultores. (2020, marzo 2). https://online-tesis.com/tecnicas-de-recoleccion-de-datos-para-realizar-un-trabajo-de-investigacion/

BBC. (2017, mayo 17). *BBC*. https://www.bbc.com/news/technology-39901382

Caeiro, R. E. (2021). *Documentación de impactos y el método Eslabones de Incidencia. Posibilidades de aplicación INTA.* Buenos Aires: Ediciones INTA; Estación Experimental Agropecuaria Catamarca. Retrieved mayo 30, 2022, from http://hdl.handle.net/20.500.12123/10324

Campos, N. O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, 100-111.

Carrasco, J. B. (2011). *Gestión de procesos (Alineados con la estrategia)*.

Casanoba, C. M. (1995). Los llamados delitos informáticos. *Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida.*

Castro, H. J., & Monteverde, A. S. (2018, mayo 30). *Revista ESPACIOS*. https://es.revistaespacios.com/a18v39n39/a18v39n39p31.pdf

CFN - Subg. De Análisis de Productos y Servicios. (2020). *EXPLOTACIÓN DE CRIADEROS, PREPARACIÓN Y CONSERVACIÓN, ELABORACIÓN DE PREPARADOS Y VENTAS AL POR MAYOR DE CAMARÓN Y LANGOSTINOS.* GUAYAQUIL.

Cloudflare. (2021). *Cloudflare*. https://www.cloudflare.com/es-es/learning/security/ransomware/wannacry-ransomware/

Congreso de la Nación Argentina. (1984). CODIGO PENAL DE LA NACION ARGENTINA. Buenos Aires, Argentina.

Congreso de la Republica de Perú. (2014, marzo 10). LEY DE DELITOS INFORMÁTICOS - LEY N° 30171. Perú.

Congreso Nacional Brasileño. (1996, julio 24). Ley no. 9.296. Brasil.

Congreso Nacional de Brasil. (1940, dicembre 7). Codigo Penal. Brasil.

Congreso Nacional de Chile. (1874, noviembre 12). Código Penal . Santiago, Chile.

Congreso Nacional de Chile. (2022, junio 20). Ley Núm. 21.459. Chile.

Consejo de Europa. (2001, noviembre 23). Convenio Sobre la Ciberdelincuencia. Budapest, Hungría.

Council of Europe. (1981, enero 28). Convenio Para La Protección De Las Personas Con Respecto Al Tratamiento Automatizado De Datos De Carácter Personal. Estrasburgo, Francia.

Cuatrecasas, L. (2017). *Ingeniería de Procesos y de Planta. Ingeniería Lean.* Barcelona: Profit Editorial I. S.L. .

El Comercio. (2022, julio 25). *El Comercio*. El Comercio: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

El Congreso de Colombia. (2009, enero 5). Ley 1273 de 2009. Colombia.

Equipo editorial, E. (2021, agosto 5). *Concepto*. Concepto: https://concepto.de/conclusion/

Fundación Fepropaz. (2023, Marzo 20). *Fundación Fepropaz*. La tecnología y las nuevas generaciones: https://fepropaz.com/la-tecnologia-y-las-nuevas-generaciones/#:~:text=Los%20baby%20boomers%20y%20la,uso%20de%20las%20herramientas%20digitales.

Galeano, J. (2011). El hombre y la tecnología: del hombre moderno al hombre moderno. *KubernÉtica*, 4-6. https://doi.org/https://www.kubernetica.com/documentos/articulos-academicos/el-hombre-y-la-tecnologia-del-hombre-moderno-al-hombreprimitivo.pdf

H., B. R. (2004). *Logística. Administración de la cadena de suministro.* . México: Pearson Educación.

Harán, J. M. (2023, agosto 31). *ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina*. welivesecurity: https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

Higueras, M. H. (1983). *ANTE LA RATIFICACIÓN DEL CONVENIO.* DA Notas.

International Telecommunication Union. (2020). *ITU Plublications.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

itahora. (2021, julio 6). *itahora.* itahora: https://itahora.com/2021/07/06/la-aeci-impulsa-la-participacion-de-ecuador-en-el-convenio-de-budapest/

La Asamblea Legislativa Plurinacional. (1972, Agosto 23). Ley No 1768 del Código Penal. *Ley No 1768 del Código Penal - Vigente y Actualizado 2022*. La Paz, Bolivia.

Marini, J. R., & Espíndola, E. A. (2016). Modelos de Investigación Cualitativa y Cuantitativa y su Aplicación en el Estudio del derecho. *Universita Ciencia, 5*(12), 13 - 24. https://doi.org/https://doi.org/10.5281/zenodo.7020101

Ministerio de Telecomunicaciones y Sociedad de la Información. (2022). ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. Ecuador.

Morgan, S. (2020, noviembre 13). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Observatorio del Principio 10. (2022). *Observatorio del Principio 10*. Observatorio del Principio 10: https://observatoriop10.cepal.org/es/countries/37/treaties

Onofa, M. (2022, junio 30). *Dialogo Americas*. Ataques cibernéticos amenazan seguridad en Ecuador: https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

Pérez Lindo, A. (1995). La esencia y el destino de la tecnología Nacional de Quilmes. *Repositorio Institucional Digital de Acceso Abierto de la Universidad, 02*(05), 168-174. https://doi.org/http://ridaa.unq.edu.ar/handle/20.500.11807/453

Ramirez, R. (2017, diciembre 27). *Policia Nacional del Ecuador* . Policia Nacional del Ecuador : https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Roberto Hernández Sampieri, Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la Investigación. In *Metodología de la investigación* (p. 91). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Rodríguez, A. M. (2020). *Manual de derecho informático.*

Sain, G. (2015, 11 14). Evolución histórica de los delitos informáticos. *Pensamiento Penal*. https://doi.org/https://www.pensamientopenal.com.ar/doctrina/40877-evolucion-historica-delitos-informaticos

Senado de la Republica de Colombia. (1890, octubre 19). Código Penal. Colombia.

Servicios, B. C. (2020).

Superintendencia de Compañias Subgerencia de Análisis y Productos y servicios. (2020). *Análisis Sectorial Camarón.*

Symantec Corporation. (2016). *Informe Norton sobre Ciberseguridad 2016.*

Temperini, M. G. (2014). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. *Simposio Argentino de Informática y Derecho, 14*, 129-139.

Torres-Torres, H. W. (2002). *Derecho Informático.* Medellín: Ediciones Jurídicas .

Valdés, J. T. (2008). *Derecho Informático.* McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE c.v.

W. Edwards Deming. (1982). *Out of the Crisis. Quality, productivity and Competitive Position.* Ediciones Díaz de Santos, S.A.

Zambrano-Mendieta, J. E., Dueñas-Zambrano, K. I., & Macías-Ordoñez, L. M. (2016). *Delito Informático. Procedimiento Penal en Ecuador* . Universidad Laica “Eloy Alfaro”.