UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADO

TEMA:

“Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la República del Ecuador, Colombia, Chile y Argentina**”**

AUTOR

Jimmy Paúl Cóndor Rosas

TUTOR

Dr. José Luis Romo Santana

AMBATO-ECUADOR

2024

TEMA:

SEGURIDAD CIBERNÉTICA: ESTUDIO COMPARATIVO DEL SISTEMA JURÍDICO DE LA REPÚBLICA DEL ECUADOR, COLOMBIA, CHILE Y ARGENTINA.

APROBACIÓN DE TUTOR

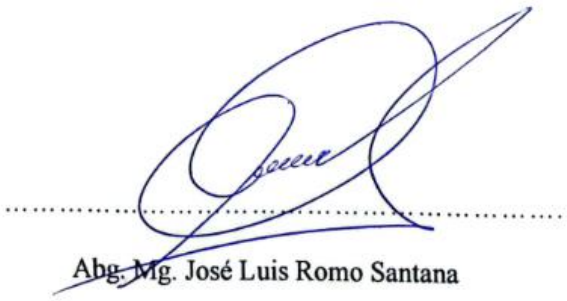
El suscrito Abg. Mg. José Luis Romo Santamaria, calidad de Tutor del Trabajo de Integración Curricular.

CERTIFICA:

Que el señor Jimmy Paúl Cóndor Rosas, portador de la Cédula de Ciudadanía: 180488502-6, habilitado para obtener el Título de Tercer Nivel; ha concluido su Trabajo de Integración Curricular, Modalidad PROYECTO DE INVESTIGACIÓN; sobre el Tema: "SEGURIDAD CIBERNÉTICA: ESTUDIO COMPARATIVO DEL SISTEMA JURÍDICO DE LA REPÚBLICA DEL ECUADOR, COLOMBIA, CHILE Y ARGENTINA". Previo a la obtención del título de Abogado; y al cumplir con los requisitos técnicos, científicos, reglamentarios, metodológicos y jurídicos, autorizo la presentación del mismo ante el Organismo pertinente, para que sea sometido a evaluación por parte de la Comisión calificadora designada por el H. Consejo Directivo

Ambato, 16 de enero de 2024

LO CERTIFICO



Abg. Mg. José Luis Romo Santana

TUTOR

AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jimmy Paúl Cóndor Rosas, manifiesto que el presente trabajo de titulación denominado: "SEGURIDAD CIBERNÉTICA: ESTUDIO COMPARATIVO DEL SISTEMA JURÍDICO DE LA REPÚBLICA DEL ECUADOR, COLOMBIA, CHILE Y ARGENTINA", es de mi propia y única autoría el cual constituye un trabajo original, que se basa en la aplicación de mis conocimientos previos adquiridos en mi formación académica a través de fuentes legales, doctrinales y bibliográficas. Además, se ha determinado diferentes ideas, conclusiones y recomendaciones que son responsabilidad del autor y de quienes las emitan.

Ambato, 16 de enero del 2024

SUSCRIBO

Jimmy Paúl Cóndor Rosas

C.I. 180488502-6

AUTOR

DERECHOS DE AUTOR

Doy mi autorización a la Universidad Técnica de Ambato para que utilice el presente trabajo de investigación como un documento accesible para consultas en los procedimientos de investigación, de acuerdo con las normativas internas de la institución. Transferiré completamente los derechos de autor de mi tesis con el propósito de investigación y difusión del conocimiento, y también autorizo la reproducción total o parcial siguiendo las regulaciones universitarias, siempre y cuando no se busque obtener beneficio económico y se realice con respeto a los derechos del autor.

Ambato, 16 de enero del 2024

SUSCRIBO

Jimmy Paúl Cóndor Rosas

C.I. 180488502-6

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

Los Miembros del Tribunal de Grado APRUEBAN el Trabajo de Investigación: "SEGURIDAD CIBERNÉTICA: ESTUDIO COMPARATIVO DEL SISTEMA JURÍDICO DE LA REPÚBLICA DEL ECUADOR, COLOMBIA, CHILE Y ARGENTINA", presentado por el señor Jimmy Paúl Cóndor Rosas, de conformidad con el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato. Autorizando su presentación ante los organismos correspondientes.

Ambato, ……2024

Para constancia firman:

……..

PRESIDENTE

…… ……

MIEMBRO MIEMBRO

DEDICATORIA

Este trabajo de investigación así como el tiempo y la constancia invertida se los dedico de todo corazón a mis padres, Jacqueline y Oscar, ya que desde pequeño me han enseñado el valor del trabajo, la dedicación y el amor por lo que hacemos; así también a mis hermanos Kevin y Mariangel, que a pesar de no vernos seguido han contribuido con su complicidad para culminar este trabajo, sintiéndose día a día parte del mismo y el proceso; finalmente quiero dedicarle gran parte de mi trabajo a una persona que siempre me ha cuidado, me enseñó a ser fuerte en la penumbra y humilde en el triunfo, a Laura mi abuelita, gracias por ser mi segunda madre y confiar en todo lo que hago, aunque a veces parezca perdido todo, su bendición siempre me ha sacado adelante.

Con todo mi amor.

Jimmy Paúl Cóndor Rosas

AGRADECIMIENTO

Agradezco en primer lugar a Dios y la virgen que siempre me han acompañado en los momentos difíciles, a mis padres por ser mi soporte y ayuda incondicional en esta etapa de mi vida académica; a mis hermanos por ser cómplices y amigos en los momentos que lo he necesitado; a mis amigos, que siempre han estado incondicionalmente dentro y fuera de las aulas, a los que estuvieron y a los que estarán muchas gracias por ser el motor de alegría dentro de la vida académica, a cada persona de la cual me llevo buenos recuerdos, muchas gracias de todo corazón.

Jimmy Paúl Cóndor Rosas

ÍNDICE GENERAL DE CONTENIDOS DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo de investigación se enfoca en evaluar la estructura legal de seguridad informática en Ecuador, contrastada con los marcos legales de Colombia, Chile y Argentina, a través de un análisis exhaustivo, se identificaron brechas y áreas de mejora en la legislación ecuatoriana, resaltando la necesidad de mayor claridad y especificidad en las regulaciones, así como una atención especial a las sanciones y medidas preventivas; se destaca la importancia de examinar y aprender de las leyes de otros países del mismo hemisferio para dar una mejor imagen a la legislación en Ecuador. Los objetivos específicos incluyeron analizar y comparar las leyes, regulaciones y políticas en el marco jurídico de seguridad cibernética de los países mencionados, evaluar la efectividad y aplicabilidad de las disposiciones legales, y proponer recomendaciones específicas para fortalecer el marco jurídico de seguridad cibernética en Ecuador; se subrayó la importancia de fortalecer y trabajar en conjunto para dar solución eficaz a los ciberdelitos, considerando compartir información con recursos mejorando así capacidades de respuesta y colaboración frente a los riesgos cibernéticos. Como resultado, se formularon recomendaciones específicas con el objetivo de aportar al entramado legal de seguridad cibernética en Ecuador, aunando a lo antes mencionado, se considerarán las prácticas más efectivas identificadas en Colombia, Chile y Argentina, estas sugerencias buscan abordar las deficiencias identificadas y ofrecer un marco legal más sólido y adaptable, mejorando la efectividad de las disposiciones legales en Ecuador; como síntesis, el estudio destaca la importancia de reforzar el marco legal de seguridad cibernética en Ecuador para potenciar la capacidad del país frente a los desafíos en este ámbito, considerando las experiencias y enfoques exitosos de otros países de la región.

Palabras Clave: ciberseguridad, análisis, cibernética, marco legal, colaboración.

ABSTRACT

The present research paper focuses on evaluating the legal structure of cybersecurity in Ecuador, contrasted with the legal frameworks of Colombia, Chile, and Argentina. Through an exhaustive analysis, gaps and areas for improvement were identified in Ecuadorian legislation, highlighting the need for greater clarity and specificity in regulations, as well as special attention to sanctions and preventive measures. The importance of examining and learning from the laws of other countries in the same hemisphere is highlighted to give a better picture to the legislation in Ecuador. Specific objectives included analyzing and comparing the laws, regulations, and policies in the cybersecurity legal framework of the aforementioned countries, evaluating the effectiveness and applicability of legal provisions, and proposing specific recommendations to strengthen the cybersecurity legal framework in Ecuador. The importance of strengthening and working together to provide an effective solution to cybercrimes was emphasized, considering sharing information with resources, thus improving response capabilities and collaboration in the face of cyber risks. As a result, specific recommendations were formulated with the aim of contributing to the legal framework of cybersecurity in Ecuador. In addition to the aforenoted, the most effective practices identified in Colombia, Chile, and Argentina will be considered. These suggestions seek to address the identified deficiencies and offer a more solid and adaptable legal framework, improving the effectiveness of legal provisions in Ecuador. In summary, the study highlights the importance of strengthening the cybersecurity legal framework in Ecuador to enhance the country's capacity in the face of challenges in this field, considering the experiences and successful approaches of other countries in the region.

Keywords: cybersecurity, analysis, cybernetics, legal framework, collaboration.

CAPITULO I

MARCO TEÓRICO

1.1.Antecedentes Investigativos

Varias hipótesis se han planteado sobre la seguridad cibernética en la actualidad, pero para RELASEDOR Y FLACSO (2017), en su Revista Latinoamericana de Estudios de Seguridad, titulada: "CIBERSEGURIDAD"; Dada la prevalencia de redes informáticas varias y el crecimiento de Internet, materia de ciberdefensa y ciberseguridad esenciales en los estudios estratégicos contemporáneos, esta transformación ha agregado una nueva dimensión a la guerra contemporánea, que tiene un impacto significativo en la vida cotidiana a nivel global; por lo tanto, es fundamental comprender estos conceptos cuando se formulan políticas de defensa a nivel nacional, en Ecuador, se ha discutido extensivamente sobre estos temas, pero la mayor parte del debate se ha centro en aspectos prácticos.

Dentro de los patrones de ciberdelitos en la sociedad latinoamericana, Rubio & Terán, (2023), en su proyecto de maestría titulado: "ANÁLISIS COMPARATIVO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR CON LA LEGISLACIÓN ARGENTINA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS"; establecen que, el objetivo a investigar en el documento es, la Ley Orgánica que se encarga de velar por los Datos Personal de Ecuador en comparación con Argentina, ambas con un lineamiento en la seguridad cibernética y los delitos informáticos; la evaluación se lleva a cabo de manera secuencial, en primer lugar, se destaca la importación creciente de la informática en la sociedad real y las vulnerabilidades que han surgido como resultado de los avances tecnológicos, también se identifican los ciberdelitos que más resaltan en los casos de Argentina y Ecuador .

En Latinoamérica la seguridad cibernética ha dado un giro drástico, el autor Serna Patiño, A. (2018) en su trabajo de investigación para la Maestría en Gestión Tecnológica, titulado: "ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD

PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN", establece que, el vertiginoso desarrollo de las TIC presenta desafíos significativos en la gestión, especialmente en ámbitos como la ciberseguridad y la infraestructura correspondiente, con el propósito de abordar la ciberseguridad, este estudio se enfoca en la óptima reacción a diversos conflictos y la salvaguarda de bases sociales en peligro en el ámbito tecnológico; se apoya en el modelo de evolución aplicable en ciberseguridad social es fanática de seguir modelos con Estándares y Tecnología.

El tema económico es una de las ramas con más ataques en lo que a ciberseguridad compete, para Gumucio Suarez, J. (2021), en su tesis de maestría titulada: "GUÍA DE IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ENTIDADES DE INTERMEDIACIÓN FINANCIERA"; la seguridad cibernética ha transformado la sociedad digital y su relación con los riesgos financieros, comparándola con los criterios puestos en contexto por los tratados de Basilea II, se destaca que en América Latina, las regulaciones relacionadas con la seguridad cibernética aún son generalizadas y carecen de detalles; por lo tanto, el NIST (Instituto Nacional de Estándares y Tecnología) proporciona un marco de referencia para una guía destinada a los responsables que provoquen riesgos en instituciones financieras para implementar la gestión de ciberseguridad.

Dentro del margen resolutivo de seguridad de la tecnología, Elizalde Castañeda, R. y otros, (2021), en su artículo científico publicado en la revista "Ius Comitiãlis", titulado: "LOS DELITOS CIBERNÉTICOS EN CHILE, MÉXICO Y COLOMBIA. UN ESTUDIO DE DERECHO COMPARADO"; establece que, los avances legislativos referentes a los ciberdelitos originados en Chile, México y Colombia, iniciaron hace décadas la tipificación de conductas asociadas a los delitos cibernéticos mediante leyes específicas para cada caso; a pesar de ello, persiste la incertidumbre sobre la amplitud de los avances en las reformas constitucionales y legales en esta esfera, se sugiere emplear el Convenio de Budapest, un acuerdo internacional establecido por el Consejo de Europa en 2001 para luchar contra esta nueva problemática digital, como un medio para conocer mejor la evolución de los delitos en Latinoamérica y a nivel mundial; el motivo de este acuerdo es establecer legislación penal aplicable a todos los

países que lo conforman, convirtiéndose en un marco crucial para el libre desarrollo del combate contra los ciberdelincuentes.

1.2.Seguridad Cibernética:

La seguridad cibernética, también reconocida como ciberseguridad o la ciberseguridad se enfoca en salvaguardar la vías de la informática y lo que está vinculado a ella, su principal objetivo es prevenir, detectar y responder a los ataques cibernéticos que pueden tener un impacto significativo en individuos, organizaciones, comunidades y naciones; estos ataques pueden derivar en pérdidas económicas, robo de datos personales, financieros o médicos, además de perjudicar la reputación y la seguridad de personas y entidades (Diaz Aparicio, 2023).

La ciberseguridad se ha vuelto de suma relevancia en el mundo actual, dado que la tecnología y la información desempeñan un papel esencial en la rutina diaria de individuos y entidades, su enfoque se centra en salvaguardar la infraestructura informática y sus componentes con el propósito de anticipar, identificar y gestionar las amenazas cibernéticas que pueden tener un impacto considerable en personas, organizaciones, comunidades y naciones en su conjunto.

En ese sentido, es menester traer a este análisis lo establecido por Serrano et al. (2021), quien manifiesta que, la seguridad cibernética abarca diversas categorías, como seguridad de la red, seguridad electrónica y seguridad de la tecnología de las comunicaciones, entre otras, un enfoque sólido de ciberseguridad incluye tecnología, procedimientos y políticas diseñados para salvaguardar elementos críticos del entorno de tecnología de la información, se establecen múltiples capas de protección en una estrategia de ciberseguridad sólida para defenderse de delitos cibernéticos que pueden implicar intentos de acceso no autorizado, alteración o destrucción de datos, extorsión, interrupción de operaciones comerciales normales, entre otros.

1.3.CIBERDELITOS

1.3.1. Evolución Histórica

1.3.1.1.Reseña Histórica de los ciberdelitos:

El ciberdelito tiene la característica de ser un una forma de delincuencia la cual en la actualidad se realiza por medio de los ordenadores, una vez que se da el surgimiento de la internet los mismos se dan a través de la red; los ciberdelitos en la última década han evolucionado para ser la red más activa en el mundo en base a su evolución y los medios empleados para su accionar; el origen de estos data desde finales de 1800, hasta la actualidad, hubo varios acontecimientos que han abierto precedentes a nivel mundial sobre los delitos cibernéticos, encontrando maneras de operación en función a los recursos, época y medios tecnológicos que facilitan el cometimiento de actividades ilícitas que están presentes en nuestro panorama cotidiano actual (Cordero Ruiz, 2021); a continuación se dividirá la historia por medio de reseñas y oleadas que según la época dan origen a los ciberdelitos conocidos en la actualidad, varios ya han desaparecido y otros aún mantienen su ideología y manera de operar dentro de la sociedad, aquí los más importantes de la historia.

1.3.1.2.Primer ciberdelito de la Historia:

El primer delito cibernético se remonta a la época en la cual no existían medios tecnológicos avanzados, no había una radio o una televisión, únicamente se encontraba en desarrollo la bombilla eléctrica pero con una distancia considerable a su primera comercialización; en Francia en la ciudad de Burdeos en el año 1834, los telégrafos ópticos eran propiedad del gobierno, llamado “el email Napoleónico”, siendo así que el acceso a estos tenían únicamente funcionarios y directores de cada red de conexión.

El “hackeo” de la época fue elaborado por dos banqueros los cuales crearon un “plan sin fisuras”, modificando los mensajes enviados por el telégrafo, el mercado de bonos en ese tiempo eran emitidos por este medio de mensajería, los banqueros se anticipaban 5 días a los inversionistas de los pueblos al interceptar información y usarla a su favor,

llegando a ganar en dos años más de 100.000 francos, suma de alta consideración para la época; el método que utilizaban era uy sencillo, sobornaban a un empleado de una de las torres de telégrafo con un sueldo para que este emita falsas señales y haciendo uso de los conocimientos de un ex empleado de estas se hacían con la información mucho antes que su competencia; demostrando así que la ineficacia en seguridad nunca es falla del sistema sino del humano como método de seguridad primitiva e ineficaz en la mayoría de un cibercrimen. (Rodriguez Garcia, 2018)

1.3.1.3.Primera Ola-Creación del Correo electrónico (1977):

Aunque al inicio el correo electrónico fue de uso académico exclusivamente por el Instituto Tecnológico de Massachusetts (MIT), tan pronto como fue posible trataron de integrar el servicio de mensajería para el público en general, es así que en 1971, Ray Tomlinson añade un formato web el cual es similar a las interfaces de correos electrónicos que conocemos actualmente, con buzones personales que podían almacenar y recibir mensajes, dando comunicación con una persona en específico que disponga un ordenador, este prototipo lo puso a prueba por primera vez la Agencia de Investigación Avanzada de Defensa de Estados Unidos (DARPA).

El primer auge del correo electrónico inicia de manera oficial entre 1973 hasta 1977, dado que este se estructura de la manera típica, tal como se lo conoce en la actualidad, agregándose la función de destinatario y remitente, abriendo la nueva opción de reenviar un mensaje como tal; sin embargo estas funciones traen consigo mensajes maliciosos que poco a poco se convierten en problemas dentro de esta interfaz, como estafas o malware que aparecen técnicamente en los correos visibles de la bandeja del internauta para causar ataques al equipo tecnológico una vez sean abiertos (Petrosyan, 2022).

1.3.1.4.Segunda Ola-Navegadores Web (1990):

En 1993, Marc Andreessen, otro científico informático, desarrolló el navegador Mosaic en la Universidad de Illinois, destacándose como el primer navegador web popular, precursor de Mozilla Firefox; Mosaic funcionaba en sistemas Windows y ofrecía un acceso sencillo a páginas web, salas de chat y bibliotecas de imágenes, un año después en la época de 1994, Andreessen fundó Netscape y lanzó Netscape Navigator a la sociedad, convirtiéndose en el primer navegador web comercial exitoso (Sintes Marco, 2023).

En 1995, Microsoft lanzó Internet Explorer, que eventualmente se transformó en el navegador número uno en todo el mundo, la rivalidad entre Microsoft y Netscape por el dominio del mercado de navegadores web se conoció como la "Guerra de Navegadores", esta competencia se centró en el control del mercado web de Windows, sin que ninguna otra empresa pudiera ofrecer una competencia significativa en ese momento. (López, 2017)

Con los navegadores web en auge, las páginas webs cuestionables se daban paso para vulnerar la internet, los delitos típicos eran la implementación de virus gusanos dentro de los servidores, para las personas de la época era novedosa la nueva web es así que no eran tan importante el peligro cibernético al cual se exponían, hecho que era aprovechado por los ciberdelincuentes de la época para malversar mails o crear propagandas que infectaban el dispositivo dentro del rango de peligro establecido por el delincuente con objetivo de obtener información personal o eliminar servidores importantes de empresas con fines de lucro; con el nacimiento de la WWW, también se dieron tres acontecimientos importantes que desencadenaron la llamada “Segunda Oleada” web, a continuación se da una breve reseña según la investigadora tecnológica (Peña, 2023).

- En el año de 1995, se origina el llamado “pishing”, que para la autora Mariana Leguizamón (2023), en su Trabajo Final de Grado en Criminología y Seguridad, titulado “El Pishing”, manifiesta que, el phishing se describe como el acto en el que una persona recibe notificaciones por cualquier medio electrónico de alguien que finge ser una entidad legítima, con el propósito de obtener información delicada, como cuentas bancarias, contraseñas y datos

personales, entre otros, posteriormente, esta información obtenida de manera engañosa se emplea para acceder a las cuentas personales de los afectados, lo que puede dar lugar a pérdidas financieras o usurpación de identidad.

Para esta época los ciberdelincuentes dieron a conocer el primer caso de phishing, el mismo se dio manifiesto con la táctica de enviar mensajes de correo electrónico fraudulentos, aparentando ser de una empresa auténtica, con el propósito de engañar a los usuarios y adquirir datos personales y financieros, este incidente se ejecutó utilizando el navegador web Netscape Navigator (Mr. Houston, 2021).

- En el año 1996, se iniciaron nuevos ataques a las redes que particularmente dependían de mecanismos más innovadores en el plan tecnológico, aquí se originó los ataques DDoS o DoS "Ataque de denegación de servicio distribuido", para los autores Martínez Lozano & Atencio Ortiz (2019), este delito se define como; El propósito de los ataques de denegación de servicio (DoS) es limitar o bloquear el acceso de los usuarios legítimos a los recursos de la red, computadora o servicio de la víctima.

  Si el ataque es iniciado por un solo *host*, se le llama ataque DoS, aunque es posible realizar un ataque DoS con un solo *host*, la mayoría de los ataques exitosos requieren un grupo de hosts maliciosos llamados *"bots"*, que inundan la red de la víctima con una gran cantidad de paquetes de ataque; de manera resumida, el evento implicó sobrecargar un servidor con un flujo de tráfico ficticio, lo que resultó en su incapacidad para atender las peticiones genuinas de personas reales y no los llamados "bots" que necesitaban desarrollar sus actividades, dando como resultado la invalidez de la página y sus servicios, es importante destacar que esta agresión se llevó a cabo utilizando el navegador web Netscape Navigator.

- En el año de 1999 los ataques con la internet más desarrollada se vuelven más complejos, pero con mayor beneficio para los ciberdelincuentes, los virus se originan, dentro del Blog sobre tecnología de España Business Insider México,

el autor Sarmiento A. (2021), comenta que el primer ciberataque conocido en el mundo fue el virus Melissa el cual se transmitía mediante emails propagándose por varias partes del mundo, el creador del virus fue David L. Smith, fue quien subió un archivo malicioso con el nombre list.doc, se propagaba en direcciones electrónicas, destruyendo archivos del computador infectado, causando pérdidas de 80 millones de dólares en empresas estadounidenses.

Durante la década de los 90, los navegadores web experimentaron un crecimiento y desarrollo, facilitando el acceso a la World Wide Web de una manera más sencilla y accesible para los usuarios, sin embargo, este período también presenció los primeros casos de ciberataques a través de los navegadores web, tales como el primer ataque de correo electrónico con el virus Melissa, el primer incidente de phishing y el primer ataque DDoS; estos ataques sentaron las bases para la evolución de los delitos cibernéticos y la necesidad de una colaboración internacional en su combate.

1.3.1.5.Tercera Ola-Redes Sociales (2000):

En la era actual, caracterizada por la tecnología y la información, las redes sociales son ahora una de las principales fuentes de comunicación y compartimos datos, sin embargo, este avance en las plataformas virtuales también ha generado una creciente preocupación, los ciberataques en redes sociales durante la década de 2000, los desafíos que surgieron han sido pioneros de las medidas implementadas para hacerles frente que se desarrollan en la actualidad.

Durante los años 2000, las redes sociales experimentaron un auge masivo, plataformas como MySpace, Hi5 y Facebook permitieron a las personas conectarse, compartir fotos, actualizar sus estados, y mucho más; sin embargo, esta era digital también conllevó una serie de amenazas cibernéticas, para los autores, Escobar Macías & Álvarez Galarza, (2022) dentro de su artículo de revista sobre análisis de ciberataques enfocado a la protección de datos, mencionan los acontecimientos más relevantes

como pioneros en redes sociales, en la década de 2000, se registraron algunos de los primeros incidentes de ciberataques en redes sociales.

En 2005, MySpace fue el escenario del primer ataque de phishing, en el cual se enviaban correos electrónicos fraudulentos que aparentaban ser de MySpace para engañar a los usuarios y obtener datos personales y financieros. Posteriormente, en 2006, se dio el primer ataque de spam en Facebook, donde se enviaban mensajes no solicitados a los usuarios de esta plataforma con fines promocionales. Un año después, en 2007, Facebook también sufrió el primer ataque de malware, en el que se enviaban mensajes infectados con malware a los internautas de red con el fin de de robar información personal y financiera.

Otro tipo común de ciberataque eran los virus y el malware, los usuarios descargaban archivos adjuntos o hacían clic en enlaces infectados, lo que permitía a los atacantes acceder a sus cuentas y propagar contenido malicioso; esto no solo afectaba a los usuarios de manera individual, sino que también tenía el potencial de propagarse rápidamente a través de las redes sociales, causando un impacto masivo.

Además de los ataques dirigidos a usuarios individuales, las redes sociales también se convirtieron en un objetivo de ataques a gran escala, en 2007 el que más marca el inicio de los ciberdelitos contra los datos personales y la integridad se dio con Facebook, esta red social fue víctima de un extenso ataque de phishing que afectó a millones de usuarios; este incidente marcó un punto de inflexión en la seguridad de las redes sociales, generando una mayor concienciación y la aplicación de sólidas medidas de protección.

Durante el 2000, los ciberataques en redes sociales representaron una amenaza importante para la seguridad y privacidad de los usuarios, los ataques de phishing y la propagación de virus y malware eran comunes, causando trastornos en la comunidad en línea, no obstante, estos desafíos también motivaron mejoras en las medidas de seguridad de las redes sociales, lo que ha llevado a un entorno más seguro y protegido en la actualidad; a medida que avanzamos hacia el futuro, es esencial mantener la

vigilancia y tomar precauciones adicionales para salvaguardar nuestra información en las redes sociales.

1.3.1.6.Cuarta Ola-Industria Criminal (1997):

La industria delictiva relacionada con los ciberdelitos ha experimentado una evolución significativa desde sus inicios en 1997; en la década de 1990, los ciberdelitos eran menos complejos y frecuentes que en la actualidad, aunque marcaron las bases para el desarrollo de la ciberdelincuencia y la importancia de la cooperación a nivel internacional en su combate.

Desde entonces, la industria delictiva en el ámbito de los ciberdelitos ha experimentado una evolución notable, los perpetradores de ciberdelitos emplean técnicas más avanzadas, como el phishing sofisticado, el malware de alta complejidad y tácticas de influencia social para dar un mal sabor de boca a los usuarios y acceder a información personal y financiera; de manera que, la industria de la ciberdelincuencia se ha vuelto más organizada y sofisticada, con grupos criminales que operan a nivel global y hacen uso de tecnología avanzada para cometer delitos (Torres Orozco et al., 2019).

Es importante destacar que la industria de los ciberdelitos es altamente lucrativa y sigue creciendo constantemente, los delincuentes cibernéticos pueden obtener considerables ganancias mediante la venta de información personal y financiera robada, la ejecución de ataques de ransomware y otras formas de ciberataques, de ahí que, esta industria delictiva también puede causar daños a la economía del mundo, ya que los ataques cibernéticos pueden ocasionar perjuicios económicos y dañar la reputación de empresas y organizaciones; estas estadísticas son resumidas por los militares del ejército Mexicano y US Army, Taylor & Esparza Diaz (2023), según su estudio realizado a nivel global se estima que los ataque cibernéticos suman casi la mitad de mil millones de dólares al año dentro de su actividad a nivel mundial.

En la actualidad, la evolución de la actividad delictiva en el ámbito de los ciberdelitos se mantiene en constante cambio, adaptándose a las nuevas tecnologías y tendencias. Los perpetradores de ciberdelitos emplean tácticas cada vez más avanzadas y riesgosas, como el deepfake, la inteligencia artificial y el internet de las cosas, para llevar a cabo sus acciones delictivas. No obstante, la pandemia de COVID-19 ha contribuido al aumento de la frecuencia de los ciberataques, ya que muchas personas ahora trabajan y estudian desde sus hogares, generando un incremento en el uso de la tecnología.

Por otra parte, la industria delictiva en el ámbito de los ciberdelitos el Doctor Acurio del Pino (2015), ha experimentado una evolución sustancial desde su origen en 1997, los ciberdelincuentes emplean tácticas más avanzadas y esta industria ha ganado en organización y sofisticación; es fundamental que los usuarios de Internet tomen formas para salvaguardar los datos de individuos y financieras, además que estén en pleno conocimiento del alto riesgo tecnológico, así mismo, es necesario que los gobiernos y organizaciones internacionales colaboren para combatir la ciberdelincuencia y proteger a los usuarios de Internet.

1.4.Concepto de Ciberdelito

El ciberdelito se refiere a actividades ilegales realizadas por medios tecnológicos con conexión a la web, aunque no existe una definición universalmente aceptada, generalmente se refiere a delitos cometidos utilizando tecnología digital, algunos ejemplos de ciberdelitos incluyen los fraudes en línea y accesos que no son autorizados a los mismos, el robo de información personal, el sabotaje de redes, el ciberacoso y la distribución de virus o malware; los ciberdelitos pueden tener como objetivo obtener beneficios económicos, atentar contra el buen nombre de instituciones o personas, o interferir con el funcionamiento de sistemas informáticos, es importante tener en cuenta que el ciberdelito puede tener implicaciones legales y puede ser perseguido con sanciones según las leyes regulatorias de cada país (Cavada Herrera, 2020).

Concomitantemente, los ciberdelitos se agrupan en modalidades las cuales son características de la informática siendo este el método en el cual se desarrollan, los equipos tecnológicos son los que más vulnerabilidades presentan dentro del ataque de

diversas mafias, sin embargo los datos de los usuarios que manejan equipos de cómputo se ven en riesgo de igual manera, siendo así las más cotizadas dentro del mercado de la internet oscura; es correcto entender el mecanismo del mercado negro de información para saber que el ciberdelito no solo trata de hurtar información sin consentimiento de la persona, sino que el campo va más allá siendo tema de discusión la estrategia que los ciberdelincuentes ocupan para obtener información de la víctima, con estafas, fraudes, suplantación de identidad de instituciones varias y clonación de carnets (bancarios, identidad o pasaportes).

En este sentido, el ciberdelito se define como la comisión de actividades delictivas realizadas mediante medios tecnológicos como Internet, ordenadores, teléfonos móviles, redes de comunicación 3G y 4G, fibras y demás, Pons Gamón (2017) comenta que Delincuentes cibernéticos dirigen sus ataques hacia individuos, compañías, una variedad de entidades institucionales y administraciones con distintos objetivos, como se ha destacado previamente, la perpetración de ciberdelitos implica la utilización de software malicioso creado con el propósito de eliminar, dañar, corromper, volver inaccesibles, modificar o suprimir información de una computadora sin autorización, ya sea con intenciones económicas o perjudiciales; estos individuos malintencionados pueden dirigir sus ataques hacia individuos, compañías y gobiernos. y pueden cometer delitos desde cualquier parte del mundo; el investigador de ciberdelitos Quevedo (2017).

El mismo, ofrece varias ventajas, algunas formas en que el ciberdelito puede llegar a los usuarios cotidianos de equipos y dispositivos móviles, para evitar la ciberdelincuencia, es crucial adoptar prácticas digitales sólidas, tales como emplear contraseñas robustas, abstenerse de abrir mensajes de correo electrónico que generen dudas, evitar compartir datos personales en plataformas en línea, y asegurarse de que el software de seguridad esté constantemente actualizado; se debe tener especial precaución en sitios web no seguros, redes sociales, vulnerabilidades de seguridad, contraseñas débiles en cuentas y dispositivos inteligentes, y, por encima de todo, en el manejo del correo electrónico.

Dentro de los ciberdelitos, los protagonistas son dos, el equipo tecnológico con sus características y el ciberdelincuente, en el primer caso la autonomía no es cien por ciento confiable ya que las diversas acciones son programadas por un tercero en cuestión, aunque cabe recalcar que las inteligencias artificiales (I.A.) son lo nuevo en la actualidad, sin embargo aún no consiguen el control total de sus acciones; pero para el ciberdelincuente esta autonomía de sus actos son relevantes ya que ellos actúan de maneras lógicas según el caso.

La ideología del ciberdelincuente según el sitio web de información diversa Forensic.notes (2021) se basa en cuatro aspectos marcados, la superación, cuando el individuo desea alcanzar o superar retos tecnológicos que desde un inicio constituyeron obstáculos dentro de su nivel de preparación; la ideología, como es de conocimiento público las redes sociales han constituido el lugar número uno para lograr un acercamiento claro y conciso a lo que modas, prototipos sociales y criterios liberales constituye, es así que estos personajes tratan de llegar con un mensaje de impacto ideológico a los individuos de un determinado grupo social o incluso poblacional según el delito accionado; el beneficio económico, dentro de este punto son dos las caras de la moneda, en un primer aspecto la vulneración de los sistemas informáticos abren un gran canal de posibilidades, el primer escenario se da cuando estas vulnerabilidades son explotadas de manera que nace la extorción buscando un lucro con el único fin de no dar a conocer este punto muerto de la entidad o institución atacada; el segundo escenario se da cuando al momento de encontrar la vulneración esta es tratada por el mismo atacante y así el lucro es legal ya que se ha prestado un servicio (identificación y solución).

Finalmente la venganza, al igual que los sicarios o ladrones a sueldo, los ciberdelincuentes en la mayoría de los casos documentados son contratados con el fin de dañar o atentar contra la reputación de una persona, entidad, institución o medio de comunicación digital, lucrando así a costa de la persona atacada; cada uno de estos aspectos se generalizan en función del entorno en el cual el individuo se haya desarrollado, llamándose Hacker cuando informa de problemas en un sistema informático y Ciberdelincuente cuando saca provecho de dichos fallos en beneficio propio o de su comunidad delictiva.

1.5.Tipos de delitos informáticos:

Dentro de la informática existen varios delitos cibernéticos, los cuales se han clasificado y han conceptualizado según los criterios de varios autores, Rubio & Terán (2023) mencionan los siguientes como aquellos delitos más sobresalientes dentro del mundo cibernético:

- **El Sabotaje Informático:** El sabotaje informático es un acto ilegal que implica la alteración, destrucción o deshabilitación de sistemas, redes o datos informáticos con la intención de causar daño o perjuicio a personas, empresas u organizaciones. Esta forma de delito puede ser perpetrada por individuos o grupos con motivaciones económicas, políticas o sociales, o simplemente por diversión o desafío (Equipo iNBest, 2012).

  Los métodos utilizados para llevar a cabo el sabotaje informático abarcan el manejo de virus, gusanos, bombas cibernéticas y cronológicas, ingreso sin autorización a redes informáticas, y la copia no sin consentimiento de información, entre otros, estos métodos pueden ser empleados para interrumpir el funcionamiento habitual de un sistema, sustraer datos confidenciales o incluso para extorsionar a la víctima solicitando un rescate; en Colombia, la Ley 21.459 establece sanciones para quienes cometan sabotaje informático, considerándolo como un delito, otros países, como Ecuador, también han incorporado delitos informáticos, incluyendo el sabotaje informático, en su Código Penal.

  El sabotaje informático puede acarrear serias consecuencias para las víctimas, como la pérdida de información valiosa, interrupción de servicios esenciales y la exposición de datos confidenciales; debido a esto es crucial que las instituciones y organizaciones implementen medidas de seguridad efectivas para resguardar sus sistemas y datos, y que los individuos adopten precauciones al utilizar dispositivos y servicios en línea.

- **El Acceso No Autorizado:** El acceso no autorizado, un delito informático, se refiere a la entrada no permitida a un sistema, red o dispositivo informático sin la debida autorización del propietario o administrador, este tipo de delito puede ser cometido por individuos o grupos con el propósito de obtener datos confidenciales, dañar el sistema o llevar a cabo actividades ilegales (Solís, 2018).

  Este acceso no autorizado puede lograrse mediante la explotación de vulnerabilidades en el sistema, para el autor argentino Roldan (2023) el uso de contraseñas sustraídas o a través de la ingeniería social; una vez que el perpetrador ha accedido al sistema, puede realizar acciones maliciosas, como modificar o borrar datos, instalar software perjudicial o acceder a información confidencial; en varios países, el acceso no autorizado se considera un delito y está sujeto a castigos legales, por ejemplo, en Ecuador, el Código Orgánico Integral Penal establece sanciones para quienes cometan este tipo de acceso no autorizado.

  Es crucial resaltar que el acceso no autorizado puede ocasionar serias consecuencias para las víctimas, incluyendo la pérdida de información valiosa, la interrupción de servicios esenciales y la exposición de datos confidenciales, por este motivo, es esencial que empresas y organizaciones apliquen medidas de seguridad apropiadas para proteger sus sistemas y datos, y que los individuos adopten precauciones al usar dispositivos y servicios en línea.

- **Los perjuicios a la información o software informático:** El daño intencional a la información o programas en computadoras se considera un delito de índole informática que involucra modificar, eliminar o inhabilitar datos o programas guardados en sistemas digitales, redes o dispositivos con el objetivo de perjudicar a individuos, empresas u organizaciones, este tipo de delito puede ser llevado a cabo por individuos o grupos con diversos propósitos, como obtener ganancias económicas, políticas o sociales, o simplemente por desafío o diversión (Acurio del Pino, 2023).

Este tipo de acto delictivo en el ámbito digital puede ocasionar repercusiones extremadamente perjudiciales, dado que la información y programas informáticos son cruciales para el desarrollo de actividades tanto en entornos organizativos como en la esfera personal en esta era digital, los perpetradores de ciberdelitos tienen a su disposición distintas estrategias para ejecutar este tipo de agresiones, entre las que se encuentran el malware, los virus y diversas tácticas de intrusión informática; la anticipación y la pronta detección de estos ataques son esenciales para reducir su impacto en la seguridad cibernética; legalmente, el sabotaje informático está tipificado como delito en varios países, como Colombia, Ecuador y Chile, por ejemplo, en Ecuador se ha debatido sobre la necesidad de ajustar los delitos informáticos, como el sabotaje informático.

Es esencial que tanto empresas, organizaciones como usuarios individuales tomen medidas de seguridad adecuadas para resguardar sus sistemas y datos contra el sabotaje informático, esto implica implementar software de seguridad, realizar copias de respaldo de manera regular y promover la conciencia sobre prácticas seguras en el uso de sistemas digitales y redes; dado que, resulta crucial contar con una legislación clara y actualizada que aborde los delitos informáticos, incluyendo el sabotaje informático, para garantizar la protección de sistemas y datos en el entorno digital.

- **Riesgo para la Sociedad:** Los delitos cibernéticos plantean una seria amenaza para la sociedad en diversos frentes, con riesgos de gran alcance, se ha reflexionado sobre el impacto de estos delitos, resaltando aspectos como la invasión a la privacidad al comprometer información confidencial, el impacto económico al causar pérdidas financieras a individuos, empresas y gobiernos, así como la amenaza a la seguridad nacional al comprometer infraestructuras críticas y sistemas de defensa (Wegener, 2013).

  Estos delitos también pueden afectar la seguridad pública al interrumpir servicios esenciales como energía, transporte y comunicación, generando

desconfianza en la tecnología y obstaculizando su avance, es crucial abordar los delitos cibernéticos con un enfoque integral que incluya medidas efectivas de seguridad, leyes actualizadas y políticas que salvaguarden los intereses tanto públicos como privados en el entorno digital; entender el impacto completo de estos delitos es fundamental para responder adecuadamente y mitigar los riesgos sociales.

- **El Espionaje Informático:** El espionaje informático consiste en acceder a sistemas digitales, redes o dispositivos sin autorización, con el propósito de obtener información confidencial, puede ser perpetrado por individuos, organizaciones o incluso gobiernos, con la finalidad de lucrar por este medio, políticos, militares, este delito puede implicar la interceptación de comunicaciones, robo de datos, obtención de contraseñas y vigilancia encubierta en línea, teniendo consecuencias graves como la exposición de información sensible y el compromiso de la seguridad nacional o empresarial López Díaz et al. (2018).

  Legalmente, está tipificado como delito en varios países, con leyes y tratados internacionales que lo abordan; por ejemplo, en Colombia, la Ley 1273 de 2009 establece sanciones para los delitos cibernéticos, incluyendo el espionaje informático; en Chile, la Ley 19.223 sobre delitos informáticos también considera el espionaje informático como un delito y establece sanciones (Bustamante Riaño, 2021).

  Es crucial que empresas, organizaciones y gobiernos tomen medidas de seguridad para resguardar sus sistemas y datos contra este tipo de espionaje, esto implica la incorporación de nuevas políticas de ciberseguridad, el cifrado de datos sensibles y la difusión de prácticas seguras en el uso de sistemas digitales, de manera que, se pueda mitigar dichos delitos con una pronta colaboración de las autoridades pertinentes dentro del entorno digital.

1.6.Reunión Global sobre la Sociedad de la Información de Ginebra (CMSI) y Convenio de Budapest.

Cumbre de Ginebra; en 2005 tuvo un impacto considerable en la cooperación internacional para hacer frente a los ciberdelitos a nivel mundial, durante la conferencia, se examinó la importancia de la seguridad digital y la confianza en el empleo de las Tecnologías de la Información y Comunicación (TIC) como fundamentos cruciales para el progreso mundial de la sociedad de la información. (Binder, 2019).

En relación con la participación de naciones latinoamericanas en este acuerdo, México desempeñó un papel destacado en las conversaciones sobre la comunidad informática, la segunda fase de dicha conferencia mundial, llevada a cabo en Túnez en 2005, fue un momento crucial para evaluar los progresos del Plan de Acción establecido durante la primera fase en Ginebra; en este contexto, México ha participado activamente en discusiones sobre la comunidad informática y ha contribuido a la evaluación de resultados y avances en este ámbito.

Esta cumbre fue de vital importancia para que países menos desarrollados conozcan los nuevos riesgos que la internet enfrenta y genera en la nueva era, como lo describen los investigadores Flores Pacheco et al. (2023), la colaboración en la CMSI ha posibilitado que países latinoamericanos, incluyendo México, participen en conversaciones y acuerdos internacionales, en la era de la información, la seguridad en línea y la combate contra actividades delictivas en el ciberespacio, estas iniciativas evidencian la necesidad de enfrentar los obstáculos vinculados a la seguridad digital y la salvaguarda de datos a nivel mundial, promoviendo la cooperación y la compartición de mejores prácticas entre países de distintas partes del globo.

Los resultados de esta cumbre sentaron las bases para la fase siguiente, celebrada en Túnez en 2005, sirviendo como plataforma para discutir la brecha digital, el manejo de las nuevas tecnologías y temas políticos como el control del Internet; la participación diversa y global de países en la Cumbre de Ginebra resaltó la importancia

de abordar colaborativa y equitativamente los retos y oportunidades de la sociedad de la información a nivel internacional.

Tratado de Budapest: representa un acuerdo internacional diseñado para combatir el cibercrimen y salvaguardar a individuos y empresas contra actividades delictivas en el ámbito informático. Aprobado por el Consejo de Europa en 2001 y en funcionamiento desde 2004, actualmente cuenta con la participación de 66 países, entre ellos diversos países latinoamericanos (Barrios Achavar & Vargas Cárdenas, 2018).

Argentina, Costa Rica, México, Panamá, Uruguay, Colombia y Chile; son algunas de las naciones latinoamericanas que han ratificado este tratado, comprometiéndose a implementar medidas para prevenir y combatir el cibercrimen; el Convenio de Budapest, además, establece una colaboración internacional entre sus miembros para la investigación y persecución de delitos informáticos (Secretaria del Senado de Colombia, 2020).

La inclusión de países latinoamericanos en este convenio es un gran logro en el combate contra el cibercrimen en la región. No obstante, aún es necesario realizar esfuerzos adicionales para mejorar la seguridad cibernética en estos países, esto implica reforzar las capacidades técnicas y legales de las autoridades encargadas de combatir el cibercrimen, así como informar a la población sobre riesgos y las medidas de seguridad en línea.

1.7.PORNOGRAFÍA INFANTIL

1.7.1. Definición:

"La pornografía infantil abarca la producción, distribución, posesión y consumo de material que muestra a menores de edad participando en actividades sexuales explícitas o sugerentes" (Colmenares-Guillén et al., 2021), este delito causa graves daños físicos y psicológicos en las víctimas, siendo crucial prevenirlo y sancionarlo para proteger los derechos humanos de los menores o infantes; aunque la definición varía según la legislación de cada país, en términos generales se refiere a cualquier material que implique a menores en actividades sexuales, es relevante analizar este

fenómeno desde diversas perspectivas, como la política criminal, el derecho comparado, la teoría psicoanalítica y la sociología.

1.7.2. Análisis sobre el ciberdelito "Pornografía infantil" (Maso, Meso, Micro):

Nivel mundial (maso)

El fenómeno global del ciberdelito de pornografía infantil ha provocado extensas discusiones en los ámbitos jurídico y social, existen variaciones en la definición de abuso y comercialización de material delicado varía según el país y sus leyes, generando críticas y desafíos en su conceptualización y regulación, a nivel internacional, se han adoptado diversas medidas para abordar este delito, como la colaboración entre países, la promoción y creación de personal especializado en combatir estos delitos cibernéticos y la aplicación de tecnologías para detectar y eliminar contenido ilegal en línea; a pesar de estos esfuerzos, el complejo problema y los pocos recursos en algunos países continúan siendo obstáculos para una prevención y sanción efectiva, es esencial continuar concientizando a la sociedad y desarrollar políticas públicas que posibiliten una respuesta coordinada a nivel global para enfrentar este grave problema (Bouyssou & Polaino Navarrete, 2015).

Latinoamérica (Meso)

La pornografía infantil es un problema grave en América Latina, ya que aproximadamente el 90% de su contenido disponible en Internet se produce en la región, esta situación tiene consecuencias serias para los niños y jóvenes, como la explotación, la generación de ingresos ilegales y la vulnerabilidad a fraudes con abusos hacia los menores; en los últimos tiempos, se ha intensificado el combate de este delito en la región a través de medidas legales y programas de concienciación, estos esfuerzos se enfocan en definir legalmente la pornografía infantil, abordar el estímulo para participar en actividades relacionadas y combatir la exposición a contenidos sexuales que involucren a menores; para enfrentar el ciberdelito de pornografía infantil, de manera general se sugiere mantener una estrecha vigilancia sobre los usuarios y

dispositivos conectados, implementar medidas adicionales de seguridad, promover programas de concienciación y prevención, así como apoyar a los proveedores de servicios para eliminar este tipo de contenido de sus sistemas (Barrio & Sarricouet, 2016).

Ecuador (Micro)

El ciberdelito de pornografía infantil en Ecuador muestra una magnitud preocupante que impacta de manera considerable en la sociedad, especialmente en niños y adolescentes, dentro de esta problemática Auquilla Diaz (2009), dentro de su investigación revela que en la ciudad de Cuenca, el 80% de los adolescentes ha estado expuesto a este contenido ilícito, y en el colegio Manuel J. Calle, el 60% de los entrevistados admite haber buscado o consumido pornografía infantil; la ausencia de una regulación (normativa o ley) específica en la legislación ecuatoriana agrava la problemática, ya que la normativa actual aborda la pornografía en general, pero no se centra específicamente en la trata y comercio de material sensible de infantes.

Así mismo, la falta de rigurosidad en la regulación de internet facilita la comercialización de este tipo de contenido; para hacer frente a este problema, se sugieren diversas medidas, como la sensibilización social, la presión para una regulación más rigurosa, la implementación de programas educativos y de apoyo a víctimas, y sus familias, la creación de mecanismos de denuncia en internet y la persecución con castigos rigurosos a los criminales para combatir la impunidad, técnicamente, aunque la situación es seria y compleja, la colaboración y la aplicación de acciones coordinadas en erradicar este problema (Campbell Suárez & Avendaño Iturralde, 2015).

1.7.3. La Salvaguarda del Interés Legal en el Contexto del Delito Cibernético de “Pornografía Infantil”

Dentro del derecho se da mención que el bien jurídico protegido es todo aquello que la normas respaldan, velan y aseguran se mantenga a buen recaudo dentro de los límites legales, se lo considera como de gran importancia para la sociedad, así como también es amparado por los derechos universales; sin embargo, para que el bien

jurídico sea reconocido como tal debe estar bajo la custodia de la ley, puesto que debe existir normativa que sancione las conductas que son contrarias a su protección (Zamora Jiménez, 2005).

El enfoque del objeto de protección contra el delito de material pornográfica en menores se centra en el desarrollo psicológico y sexual normal de los individuos menores de 18 años, para E. Crespo (2010), la participación de estos jóvenes en escenas de contenido sexual explícito puede tener graves consecuencias para su bienestar; la pornografía infantil es un desafío a nivel mundial que ha crecido con los avances tecnológicos, como Internet, que facilitan y simplifican la comisión de este comportamiento ilícito.

Dentro de la perspectiva del autor resaltan a continuación algunos aspectos importantes del bien jurídico protegido al igual que los criterios de Dupuy (2019), en el caso de penas y sanciones de esta actividad con menores:

1. **Integridad sexual y desarrollo independiente de la forma del ser:** por el hecho de que el material gráfico se queda de manera permanente en la red, asegura una perpetua distribución de esto, generando explotación y vulnerabilidad a la madurez de los menores en conflicto con este delito.
2. **Explotación de menores:** la pornografía infantil se constituye como un delito que utiliza menores de edad con fines sexuales y comerciales, vulnerando así sus derechos humanos, causándoles daños emocionales significativos seguidos de una serie de trastornos psicológicos a raíz de los abusos sufridos a lo largo de su experiencia.
3. **Derecho penal de las sociedades de riesgo:** se la constituye como un delito que puede poner en riesgo a individuos que son considerados vulnerables enfocada con el principio constitucional de cuidado de los infantes, generando un sinfín de daños en la juventud e infancia.
4. **Regulación Legal:** la trata de menores y reproducción audiovisual de contenido es un grabe delito que requiere fuertes regulaciones legales a nivel nacional e internacional, con leyes reforzadas con normativa optima y clara que castiguen las conductas contrarias a su promulgación.

En Argentina, la ley 26.388 del Código Penal especifica como un delito la introducción, distribución y posesión de material sensible con menores e infantes, mientras que por otro lado, la ley 25.763 confirma el "Protocolo Facultativo de la Convención sobre los Derechos del Niño sobre la venta de niños, la prostitución infantil y la pornografía infantil"; este protocolo amplía el concepto de lo que es pornografía infantil, abarcando tanto representaciones de menores participando en actividades con fin sexual como representaciones de los genitales de un niño con un propósito predominantemente sexual (Iglesias, 2023).

En cuanto a los ejemplos de intereses legítimos tutelados en materia de pornografía infantil, podemos mencionar:

- Protección de la existencia y la integridad física y psíquica de individuos menores de 18 años.
- Garantizar el derecho de individuos menores de 18 años a la intimidad personal y familiar.
- Garantizar la salvaguardia de los derechos de individuos menores de 18 años en el ámbito educativo y la protección en el entorno escolar.

1.7.4. La Definición del Principio del Interés Prioritario del Menor en la Legislación de Ecuador y América Latina en el Contexto del Delito de Pornografía Infantil:

El principio esencial en la legislación ecuatoriana con respecto al delito cibernético de pornografía infantil es el interés superior del niño. Este principio establece que, al tomar decisiones relacionadas con un niño, se debe considerar principalmente su bienestar y protección. En el contexto de la pornografía infantil, este principio se emplea con el propósito de resguardar a los niños, niñas y adolescentes de los posibles perjuicios físicos y psicológicos como víctimas de dicho delito. (Arrias Añez et al., 2021).

En diversas naciones latinoamericanas, el principio del interés superior del niño desempeña un papel clave en la legislación, especialmente en asuntos relacionados con la defensa de los derechos de los menores, como la pornografía infantil, según la revista jurídica IUSLatin.pe (2020), en México, la Ley General de los Derechos de Niñas, Niños y Adolescentes categoriza la producción y difusión de material pornográfico infantil como un acto violento, con consecuencias legales severas. En Colombia, la Ley 679 de 2001 prescribe penas de prisión y multas por el delito de trata de material sensible con menores; en términos generales, la legislación en la región reconoce la imperiosa necesidad de resguardar a los menores de abusos sexuales, resaltando la importancia crucial del principio de protección constitucional de los niños en la implementación de la ley y la protección de sus derechos.

1.8.Acoso Cibernético:

1.8.1. Definición:

"El acoso cibernético, también denominado ciberbullying, ocurre cuando una persona es objeto de molestias, amenazas, hostigamiento, humillación, vergüenza o abuso por parte de otro individuo a través de Internet o cualquier dispositivo de comunicación, como teléfonos móviles o tabletas" (Cowie, 2013, pp. 16-24); este fenómeno se caracteriza por el maltrato entre pares, es decir, menores de edad; este tipo de hostigamiento puede manifestarse de diversas maneras, como insultos, discriminación, bromas, usurpación de identidad, suplantación, divulgación de información o imágenes que causan vergüenza a la víctima, entre otras formas.

1.8.2. Análisis sobre el ciberdelito "Acoso Cibernético" (Maso, Meso y Micro):

Nivel mundial (Maso):

El ciberacoso, también conocido como acoso cibernético, constituye un delito con alcance global que conlleva consecuencias devastadoras, dentro del estudio de los factores sociales que originan el delito, Ramírez Vásquez (2022), comenta que dentro

de las causas incluyen el anonimato en línea, la facilidad de difusión de información y la falta de información sobre las consecuencias de las acciones en el espectro digital; las repercusiones del ciberacoso abarcan desde daños psicológicos hasta situaciones trágicas como el suicidio, y su impacto económico es considerable, proyectándose costos anuales de $10.5 billones para 2025; para hacer frente a este delito, se necesita una mayor colaboración entre gobiernos, fuerzas del orden y el sector privado, así como una mayor conciencia y educación sobre el uso responsable de la tecnología.

Latinoamérica (Meso):

Para estudios en Latinoamérica, México ocupa el noveno lugar mundial en cibercriminalidad, con 13 delitos por cada millón de habitantes en 2022, según un informe de Surfshark; el phishing, que utiliza correos electrónicos para el robo de información, destaca como un delito cibernético común en la región, afectando también a Brasil, Colombia, Perú y Chile; Terbeck (2023) redacta que el informe de LexisNexis Risk Solutions ha señalado un aumento del 20 % en la tasa global de ataques de fraude digital entre 2021 y 2022, subrayando la importancia de reforzar la ciberseguridad, el estudio Panorama del Ciberdelito en Latinoamérica revela que el fraude en el comercio electrónico se ha duplicado en la región; para abordar este problema, se recomienda implementar medidas de ciberseguridad a nivel individual y organizacional, realizar auditorías que promueven seguridad dentro de las comunidades.

Ecuador: (Micro):

El ciberdelito "Acoso Cibernético" preocupa a la sociedad ecuatoriana, generando consecuencias como ataques cibernéticos, desinformación y vigilancia gubernamental, dentro de una investigación sobre ciberdelincuencia en Ecuador, Bernabé Ron, et al. (2018) menciona que el gobierno de Ecuador busca abordar este problema mediante la implementación de leyes y políticas, incluyendo la Ley de Ciberseguridad, para prevenir y combatir amenazas cibernéticas; aunque se proponen soluciones como la elaboración de un sistema que pueda informar con anticipación y la capacitación en seguridad en línea, persisten desafíos en la protección de los derechos digitales; mejorar la infraestructura de ciberseguridad en línea y fortalecer la cooperación entre

gobierno, industria y sociedad civil son esenciales para afrontar de manera efectiva el ciberdelito en Ecuador.

1.8.3. El Bien Jurídico Protegido Dentro del Ciberdelito "Acoso Cibernético"

En América Latina, el ciberdelito de acoso cibernético busca vulnerar la integridad, intimidad y dignidad en el entorno digital, este fenómeno, implica intimidación, hostigamiento o difamación a por medios con conexión a internet, por lo general dadas en redes de comunidades cibernéticas y mensajes; es un problema creciente, especialmente entre los jóvenes, y los legisladores reconocen su gravedad, por ejemplo, en México, el Código Penal Federal penaliza el acoso cibernético, mientras que en Argentina, la Ley 26.485 lo considera violencia de género, estableciendo medidas de protección; en algunos países de Latinoamérica como se evidencia, toman medidas legales para prevenir y sancionar el acoso cibernético, reconociendo como afecta la sociedad y cuan esencial es resguardar la integridad en el mundo digital (Oliva León, 2017).

En la región latinoamericana, el blog jurídico Media Defence (2020) da a conocer que, dentro del tema de cibercrímenes de esta jurisdicción, se busca salvaguardar la integridad, intimidad y dignidad en el ámbito digital mediante la legislación contra el ciberdelito de acoso cibernético; los países pioneros con énfasis en la función estado y legislación, según los presentes estudios de campo mencionan lo siguiente:

- En México, está dentro del Código P. Federal, con sanciones para quienes intimiden, hostiguen o acosen a otros mediante medios electrónicos;
- Por otro lado, en Argentina, la Ley 26.485 de Protección Integral contra la Violencia hacia las Mujeres reconoce el acoso en línea como un tipo de violencia hacia persona de diferente género, estableciendo medidas de protección específicas para las víctimas;

Estos ejemplos ilustran la diversidad de enfoques incluidos ya dentro de los países de una misma región para abordar y prevenir el acoso cibernético; por otro lado Miró LLinares et al. (2023), hace un comentario sobre el bien jurídico protegido

en este ciberdelito, mismo que tiene como objetivo principal salvaguardar la integridad, intimidad y dignidad de individuos en el ámbito digital, se refiere al uso de tecnologías para acosar, humillar o difamar a otros a través de plataformas en línea, como ejemplos algunas de las claras vulneraciones son comportamientos que incluyen:

- El envío de mensajes de odio o amenazas por medio de redes sociales,
- La divulgación no autorizada de información personal y,
- La creación de perfiles falsos para hostigar a alguien en línea.

Estas acciones infringen la integridad emocional y psicológica delo individuos vulnerados en su privacidad y dignidad en el entorno digital.

1.9.Inteligencia Artificial:

1.9.1. Definición:

La inteligencia artificial se caracteriza como un campo en la informática que se enfoca en crear máquinas y programas que tienen la capacidad de emular la inteligencia humana, conforme a la descripción proporcionada por Andreas Kaplan y Michael Haenlein según se mencionó en (Lera, 2021), se refiere a "la habilidad de un sistema para interpretar de manera precisa datos externos, aprender de esta información y aplicar esos conocimientos para llevar a cabo tareas específicas y alcanzar metas mediante una adaptación flexible"; este campo abarca diversos subcampos, que incluyen campos de aplicación amplios, como propósitos generales, aprendizaje y percepción, abarcando disciplinas más específicas como la identificación de voz, el ajedrez, la demostración de teoremas matemáticos, la composición poética y el diagnóstico de enfermedades.

1.9.2. Evolución de la Inteligencia Artificial:

la inteligencia artificial (IA) representa un dominio en la informática focalizado en desarrollar máquinas con la capacidad de emular la inteligencia humana para ejecutar diversas tareas. Su origen se remonta a la posguerra con la introducción de la "prueba de Turing" y la acuñación del término en 1956 por John McCarthy, en la actualidad, la IA abarca una variedad de subcampos, desde propósitos generales hasta aplicaciones más específicas como el comando de identificación de voz, el arte, la poesía, la optimización de investigaciones breves, el diseño de espacios y en breves aprendizajes, que varían según la utilidad. Estos abarcan desde simples algoritmos hasta complejas redes de circuitos llamados neuronas que buscan replicar los circuitos y conexiones de neuronas del cerebro humano, utilizando modelos como el aprendizaje automático y profundo. (Salesforce Latam, 2023).

En los últimos años, López de Mántaras (2023) evidencia en su investigación que la inteligencia artificial (IA) ha experimentado notables avances tecnológicos, aunque aún se enfrenta a desafíos para consolidar su desarrollo completo, la investigación en IA se ha enfocado en la creación de inteligencias artificiales especializadas, destacando logros impresionantes en la última década, impulsados por la combinación de abundantes datos y poder de cómputo avanzado; a pesar de estos progresos, se sostiene que, incluso si las futuras inteligencias artificiales alcanzan un alto grado de inteligencia, incluyendo las de propósito general, nunca podrán igualar la singularidad y complejidad del desarrollo mental humano.

1.9.3. Que entidades se encargan de la protección en caso de ataques de Inteligencias Artificiales:

En América Latina y en Ecuador, según la OEA (2018), las instancias legislativas responsables de salvaguardar contra posibles amenazas de inteligencia artificial engloban diversas categorías:

- **Organismos gubernamentales:** en Argentina han establecido entidades gubernamentales con el propósito de regular y supervisar el empleo de inteligencia artificial, esto se manifiesta a través de legislaciones como la Ley

de Inteligencia Artificial, diseñada para abordar tanto los beneficios como los riesgos asociados con esta tecnología (Galceran-Vercher, 2023).

- **Autoridades financieras:** Las autoridades financieras, como la Superintendencia de Bancos del Ecuador, también pueden adoptar medidas para supervisar y regular el uso de inteligencia artificial en el sector financiero, su enfoque busca garantizar el anonimato para cuidar de los sistemas involucrados

- **Asociaciones y organizaciones:** Todas las instituciones gubernamentales, existen organismos como la Asociación Latinoamericana de Normalización (ALAN), cuya labor se centra en establecer estándares y regulaciones para la inteligencia artificial en la región.

Estas entidades legislativas y reguladoras se dedican a desarrollar y aplicar marcos normativos y legales con el objetivo de proteger contra posibles riesgos y amenazas asociadas con la inteligencia artificial, su meta es fomentar un uso seguro, ético y responsable de esta tecnología en América Latina y en Ecuador.

1.10. ESTUDIO COMPARATIVO

El método de estudio comparativo toma un papel crucial en la investigación científica y de mercados al involucrar la contrastación procesal, conjuntos de datos o elementos, utilizado en diversas disciplinas como la antropología y sociología, este enfoque ofrece una comprensión más profunda al analizar las estructuras organizativas y desvela conexiones entre fenómenos (Piovani & Krawczyk, 2017); sus objetivos abarcan desde mejorar la comprensión interna de una organización hasta aumentar la conciencia de sistemas y culturas distintas, así como identificar posiciones competitivas.

La aplicación del análisis comparativo se extiende a investigaciones cualitativas y cuantitativas, Tonon (2011) permitiendo la consideración de variables temporales y espaciales, así pues, se pueden distinguir tipos específicos de análisis comparativo,

como el individualizador, que resalta las particularidades individuales al comparar un número limitado de casos; en resumen, el análisis comparativo se presenta como una herramienta valiosa en las ciencias sociales para describir, explicar e interpretar la realidad mediante la comparación de diversos casos o fenómenos.

1.11. ECUADOR

1.11.1. La Ciberseguridad:

La preservación de la ciberseguridad en Ecuador se vuelve esencial para salvaguardar la diversa información y los prestadores de servicios críticos del país en el mundo digital, Ecuador ha experimentado avances significativos en la normativa y la organización de sus medidas de ciberseguridad a través de la implementación de leyes y políticas nacionales, como la Ley de Protección de Datos Personales y la Estrategia Nacional de Ciberseguridad; a pesar de estos avances, persisten desafíos, incluyendo limitaciones presupuestarias, la escasez de personal especializado y la importancia de dar conocimientos útiles a la sociedad sobre ciberseguridad (Vera, 2019).

En los últimos años Ecuador ha entrado en una crisis de ciberseguridad para lo cual el país ha adoptado patrones en los cuales se debe basar la ideología social y gubernamental del país, siendo así que Cuervo (2021) da una mención a la Política de Ciberseguridad del "Acuerdo Ministerial N° 006-2021" del 17 de mayo de 2021 haciendo mención que la estrategia de seguridad cibernética en Ecuador se basa en siete elementos esenciales, los cuales abarcan; la gobernanza en ciberseguridad, el manejo de sistemas informáticos e incidentes, protección de servicios e infraestructuras digitales críticas, la defensa y soberanía, la seguridad ciudadana y pública, la cooperación a nivel regional e internacional, así como la educación y concienciación; estos esfuerzos colectivos tienen como objetivo reforzar la posición del país frente a los retos cibernéticos y fomentar un entorno digital más seguro y consciente.

Ecuador ha instituido la Ley de Protección de Datos Personales para supervisar el flujo de información digital en empresas privadas y organismos públicos, a pesar de los avances en la elaboración de marcos legales para gestionar riesgos en infraestructuras

críticas, el país enfrenta desafíos en ciberseguridad, incluida la carencia de un presupuesto sostenible y la escasez de personal especializado; la consolidación de una cultura de ciberseguridad también se presenta como un desafío, complicando la implementación eficiente de políticas y estrategias; dada la vitalidad que tiene la seguridad cibernética en el desarrollo social, la economía y humano, Ecuador debe fortalecer constantemente sus capacidades y políticas en este campo, al mismo tiempo que fomenta una formación segura sobre delitos cibernéticos en la comunidad.

1.11.2. Los Ciberdelitos:

Dentro del Ecuador con la evolución tecnológica ha surgido varios tipos de delitos los cuales tomando el camino de la evolución y los medios cotidianos que más utiliza la población (tecnología), se han adaptado a un mundo digital dando como resultado en atracos de diferente tipo por medio de cajeros, llamadas, infiltraciones no autorizadas en empresas públicas o privas, robo de dispositivos móviles, clonación de tarjetas, extorciones por llamada, entre otros, que día con día se van haciendo más populares debido a la escases de conocimiento y cultura en temas de seguridad, tanto en lo social como dentro de las entidades que deben brindar protección a la ciudadanía.

En la actualidad existen varios tipos de ciberdelitos dentro del Ecuador, pero la viabilidad de esta investigación se concentra en los pioneros que se mantienen hasta hoy y han generado una evolución crítica en su modo operandi, estos son:

1. **El robo de información personal:** una de las investigaciones del Diario nacional El Comercio (2022), se destaca como uno de los ciberdelitos más prevalentes en Ecuador, siendo ejecutado principalmente mediante la técnica de *"phishing"*, en este método, los criminales envían correos electrónicos que simulan ofertas bancarias o descuentos en productos con el objetivo de obtener datos personales o contraseñas de las víctimas; la pandemia ha acentuado la vulnerabilidad de la sociedad con estos delitos, siendo así que las compras en línea son tendencia actualmente, por ende trasferencias y pagos con dinero plástico (tarjetas), para contrarrestar eficazmente esta amenaza, es imperativo reforzar las medidas de seguridad digital y fomentar la conciencia sobre los riesgos asociados a los ciberdelitos.

2. **Ataques informáticos a empresas y entidades públicas:** Los ciberataques a empresas y entidades públicas en Ecuador han experimentado un aumento, con 1,358 casos de acceso no autorizado reportados desde 2018 hasta la fecha, según información de la Fiscalía, la vulnerabilidad del sector público se acentúa debido a la falta de inversión en medidas preventivas, así como también se da por la falta de preparación del personal de seguridad que se debe encargar de la protección del estado en tema de seguridad cibernética, por otro lado el sector privado podría ser pionero en implementar estrategias de seguridad web de países desarrollados en el tema sean Norteamericanos o los más complejos como son los Europeos; resulta imperativo generar conciencia sobre seguridad digital, reforzar la respuesta gubernamental, impulsar la investigación y desarrollo de tecnologías de ciberseguridad, y establecer colaboraciones internacionales para abordar estos delitos (Vargas Borbúa et al., 2020).

3. **Pornografía Infantil:** la explotación infantil en contenido pornográfico, catalogada como un delito cibernético según el artículo 103 del Código Orgánico Integral Penal (COIP, 2014), en Ecuador, ha registrado un aumento tanto a nivel nacional como internacional en los últimos años, con una carencia de sanciones apropiadas para las víctimas, el COIP establece penas rigurosas, que van desde 13 hasta 26 años de prisión, para diversas conductas vinculadas con este crimen.

   Sin embargo, la Policía Nacional, a través de la Unidad Nacional de Ciberdelito, ha llevado a cabo operativos y detenciones, evidenciando su dedicación en la lucha contra este fenómeno, se han documentado casos de solicitudes de imágenes íntimas a adolescentes mediante perfiles falsos en plataformas de redes sociales, subrayando la importancia de la vigilancia y la acción policial para contrarrestar la pornografía infantil en el ámbito digital.

4. **Acoso Cibernético:** El ciberacoso, también denominado como cyberbullying, se caracteriza por ser una agresión intencional y repetitiva realizada a través de medios electrónicos dirigida hacia una víctima, en Ecuador, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) ha alertado sobre el uso inapropiado de las TIC con el propósito de causar daño, especialmente a niños, niñas y adolescentes, con consecuencias negativas que incluyen trastornos de estrés, ansiedad y alteraciones sustanciales en la vida digna de los individuos víctimas de estos atentados(MINTEL, 2023).

   Informes indican un aumento de los delitos informáticos, incluyendo el ciberacoso, en Ecuador, con un incremento en las denuncias de casos en años recientes, el COIP (2014) de Ecuador incorpora leyes que penalizan estos delitos, dentro de su *SECCIÓN QUINTA, PARÁGRAFOS PRIMERO (Delito de Discriminación), SEGUNDO (Delito de Odio),* de igual forma en la *SECCIÓN SEXTA (Delitos contra el derecho a la intimidad personal y familiar),* finalmente tenemos a la *SECCIÓN SÉPTIMA (Delito contra el derecho al honor y al buen nombre),* siendo así los más utilizados dentro del presente ciberdelito, el COIP sin embargo a ido imponiendo penas de prisión para los responsables.

1.11.3. Normativa:

Dentro de la legislación ecuatoriana, se destaca el orden superior o jerarquías de la aplicación de las normas, como se determina en el art. 425 de nuestra Constitución de la República del Ecuador, teniendo en cuenta este punto de ley, dentro del Ecuador las principales normas legales que son las encargadas en jurisdicción de combatir los ciberdelitos son:

- **Tratado de Delito Informático:** El Tratado de Delito Informático tiene como objetivo establecer una política penal dirigida al cibercrimen, mediante la implementación de legislación especializada y la promoción de la cooperación internacional, aborda aspectos procedimentales como la preservación ágil de datos, la revelación parcial de datos de tráfico y la interceptación de datos de

contenido; facilita el acceso sin necesidad de asistencia mutua a datos informáticos almacenados en el ámbito transfronterizo, fomentando una pronta colaboración entre las partes involucradas; en Ecuador y el resto de países de América Latina, desde la perspectiva legal, el delito informático comprende actividades punibles según las leyes convencionales como robos, hurtos, fraudes y estafas, los mismos dan apertura a dos enfoques conceptuales: uno convencional que aborda *comportamientos antijurídicos* con el uso de computadoras, y otro no convencional que define los delitos informáticos como *conductas ilícitas* en las cuales se utilizan computadoras como medio o fin para cometer actos delictivos (Zambrano-Mendieta et al., 2016).

- **Política Nacional de Ciberseguridad en Ecuador:** esta política en Ecuador tiene como objetivo establecer una estrategia integral para asegurar el Estado de Derecho y salvaguardar a los ciudadanos en el entorno digital, guiada por 7 pilares, el gobierno impulsa la cooperación entre el sector público, privado y la sociedad civil; a pesar de la implementación de acciones contra el cibercrimen, se subraya la necesidad de fortalecer la seguridad digital y concienciar sobre los ciberdelitos, en síntesis, la política refleja la importancia asignada a la protección en línea, buscando medidas eficaces para contrarrestar las amenazas cibernéticas en Ecuador (LISA Institute, 2023).

- **Legislación y medidas de otros países miembros de la OEA:** (Departamento Contra La Delincuencia Organizada Transnacional (DDTO) | OEA (2022); es recomendable gestionar normativa que se asemeje a los países más desarrollados de America Latina en temas de ciberseguridad, como un ejemplo claro es Argentina, los cuales ya integran a sus códigos penales términos modernos como es el "*Grooming*", creando programas que están normados como es la Ley 27.590 protegiendo la integridad de los niños, son ejemplos de buena gestión legal en términos de ciberseguridad anclados a la nueva realidad de la actualidad; en el caso de Ecuador el "*Acuerdo Ministerial N° 006-2021*" únicamente modifico ciertos aspectos legales de manera general como lo refleja el COIP en sus artículos *103-104-190-173-17-229-230-231-232-233-234*., sin determinar la evolución investigativa de las entidades encargadas de

velar por la sociedad, así como de los recursos para la investigación y sanciones de delitos de ciberseguridad, dando una imagen aún anticuada de normas para con la realidad moderna.

1.11.4. Jurisprudencia:

Tabla 1

Pornografía Infantil

SENTENCIA No. 456-20-JP/21
▪ **Caso No.** 456-20-JP/21 ▪ **Magistrado ponente:** Ramiro Ávila Santamaria ▪ **Tipo de sentencia:** Constitucional ▪ **Materia:** Acción de Protección ▪ **Decisión:** Si se acepta la acción de protección ▪ **Fecha de la sentencia:** 23 de noviembre del 2021 ▪ **Gaceta Judicial o Base de datos:** Página web de la Corte Constitucional del Ecuador
TEMA:
La justicia restaurativa y el derecho al debido proceso en contextos educativos /Sexting.
DERECHOS VULNERADOS:
En este caso, la Corte Constitucional determina que el Colegio Bilingüe Marie Clarac ha infringido los derechos de M.M. y su representante legal de la siguiente manera: fuente Constitución de la Republica del Ecuador.

- **Art. 76.** Se vulneró el **derecho al debido proceso**, que incluye las garantías de ser sancionado por una autoridad competente y con la debida observancia del trámite propio de cada procedimiento.
- **Art. 76. 7.a.** Se afectó el **derecho a la defensa** durante todas las etapas del procedimiento.
- **Art. 76.7.h.** Se menoscabó el **derecho a presentar argumentos**, replicar los de las otras partes, presentar pruebas y refutar las presentadas en su contra.
- **Art. 76.7.c** Se violó el **derecho a ser escuchado**, así como a que la opinión de la estudiante sea considerada al fundamentar la resolución.

PROBLEMA JURÍDICO

En la situación de una estudiante que, a través de su teléfono móvil, compartió imágenes privadas de una compañera de su escuela (acción conocida como sexting) y enfrentó medidas disciplinarias, que incluyeron la suspensión y la confiscación de su dispositivo electrónico, la Corte Constitucional está evaluando los procedimientos disciplinarios dentro del entorno educativo. La corte tiene en cuenta los principios de justicia restaurativa y el debido proceso con todas sus garantías. Como resultado de su análisis, la Corte determina que en este caso específico se han vulnerado estos principios y derechos.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

- Constitución de la república del ecuador
- Ley Orgánica de garantías Jurisdiccionales y Control Constitucional
- Código de la Niñez y Adolescencia
- Código orgánico de la función judicial

- Reglamento de Régimen Académico del Sistema Nacional de Educación Superior
- Ley Orgánica de Educación Superior
- Código de la Democracia
- Código Orgánico Integral Penal
- Código orgánico General de Procesos

HECHOS JURÍDICAMENTE RELEVANTES

1. La estudiante fue sancionada por el colegio por haber distribuido fotos íntimas de otra estudiante sin su consentimiento.

2. La estudiante presentó una acción de protección alegando que se vulneraron sus derechos al debido proceso y a la defensa.

3. El juez de primera instancia negó la acción de protección.

4. La estudiante apeló la decisión y la Corte Provincial de Pichincha confirmó la decisión del juez de primera instancia.

5. La Corte Constitucional aceptó la revisión de la acción de protección.

6. La Corte Constitucional determinó que se vulneraron los derechos de la estudiante al debido proceso y a la defensa.

7. La Corte Constitucional ordenó al colegio adecuar su código de convivencia y estableció medidas de reparación para la estudiante.

8. La Corte Constitucional estableció que la revisión de la acción de protección se limitaba al proceso disciplinario de la estudiante y no afectaba los derechos de la otra estudiante afectada por la distribución de las fotos.

DECISIÓN

La Corte Constitucional, administrando justicia constitucional conforme lo dispuesto en el artículo 436 (6) de la Constitución, artículo 25 de la LOGJCC, DECIDE:

1. Declarar que el Colegio Bilingüe Marie Clarac vulneró el derecho de M.M. y de su representante legal al debido proceso en las garantías de ser sancionado por autoridad competente y con observancia del trámite propio de cada procedimiento; a la garantía de no ser privado del derecho a la defensa en ninguna etapa del procedimiento; a la garantía de presentar argumentos y replicar los argumentos de las otras partes, presentar pruebas y contradecir las que presenten en su contra; y a la garantía de ser escuchado y que la opinión de la estudiante se tome en cuenta a la hora de motivar la resolución.
2. Aceptar la acción de protección presentada y revocar la decisión del juez de la Unidad Judicial Penal con sede en el Distrito Metropolitano de Quito, emitida el 23 de mayo de 2019, y la sentencia de la Sala Penal de la Corte Provincial de Pichincha, dictada el 5 de febrero de 2020.
3. Disponer, como medidas de reparación:
    a. La institución educativa tiene la responsabilidad de ajustar su código de convivencia de acuerdo con lo establecido en esta resolución y en las decisiones previas de la Corte respecto al debido proceso y al derecho de los menores de ser escuchados en cualquier proceso que afecte sus derechos. En un lapso de seis meses, el colegio debe

comunicar a la Corte los cambios realizados en su código de convivencia para cumplir con lo estipulado.

b. La institución educativa debe expresar disculpas por la manera en que abordó los acontecimientos de este caso. Además, en un plazo de un mes, se requiere que envíe a A.A. y M.M. una carta personal redactada y firmada por la directora del colegio con el siguiente contenido:

   "A nombre del Colegio "Unidad Educativa Particular Marie Clarac", y en cumplimiento de la sentencia emitida por la Corte Constitucional (456-20-JP/21), pido disculpas a [en la carta el colegio deberá poner los nombres correspondientes] por no haber generado un ambiente seguro que permita solucionar de forma adecuada y restaurativa el conflicto suscitado en un caso de circulación de fotos íntimas. Nos comprometemos a tomar las medidas pertinentes para que, hechos como los sucedidos, no se vuelvan a repetir."

c. Dentro de un mes a partir de la notificación de este fallo, la institución educativa debe compartir la sentencia con todos los integrantes de su comunidad educativa.

d. El MINEDUC tiene la responsabilidad de ajustar, emitir y comunicar las normativas, así como difundir tanto la legislación como esta resolución, de acuerdo con lo establecido en los párrafos 102 y 103 de esta decisión.

e. Dentro de un mes a partir de la notificación de este fallo, el Consejo de la Judicatura debe proceder a la difusión y publicación de esta sentencia dirigida a todos los jueces del país. **4.** Notifíquese, publíquese y cúmplase.
ANÁLISIS
Esta sentencia de la Corte Constitucional del Ecuador aborda de manera completa la salvaguarda de los derechos de los niños, niñas y adolescentes en el entorno educativo, estableciendo medidas correctivas y subrayando la relevancia del debido proceso y la justicia restaurativa; a través de un examen detallado, la sentencia busca asegurar la adecuada protección de los derechos constitucionales, estableciendo precedentes vinculantes para casos futuros de naturaleza similar, siendo de la misma manera se da a conocer la importancia de las leyes en defender los derechos constitucionales fundamentales dentro del ámbito educativo, contribuyendo de esta manera a la consolidación del sistema de justicia en el país.

Elaborado por: Autor, (2023)

Tabla 2

Acoso Cibernético

SENTENCIA No. 785-20-JP/22
▪ **Caso No.** 785-20-JP/22 ▪ **Magistrado ponente:** Hernán Salgado Pasantes ▪ **Tipo de sentencia:** Constitucional ▪ **Materia:** Acción de Protección

- **Decisión:** Si se acepta la acción de protección
- **Fecha de la sentencia:** 19 de enero del 2022
- **Gaceta Judicial o Base de datos:** Página web de la Corte Constitucional del Ecuador

TEMA:

Derecho a la libertad de expresión en el Internet y redes sociales en contextos educativos.

DERECHOS VULNERADOS:

En este caso, la Corte Constitucional determina identifica varios derechos vulnerados en el caso de R.S.A.E., entre ellos: fuente Constitución de la República del Ecuador.

- **Art. 76.** Se vulneró el **derecho al debido proceso,** fue vulnerado en relación con el interés superior de los niños, niñas y adolescentes en el proceso disciplinario iniciado en contra de R.S.A.E. y la presunción de inocencia; además no se permitió que ejerciera su derecho a la defensa por medio de sus padres.
- **Art. 66.6 Se afectó el derecho a la libertad de expresión,** se vio vulnerado debido a la sanción impuesta por una publicación considerada deshonrosa, sin un análisis adecuado y desde la perspectiva del adulto, a pesar de tratarse de un adolescente.
- **Art. 76.7.c** El **derecho a ser escuchado** y que su opinión sea seriamente considerada y evaluada durante el procedimiento administrativo.

- **Art. 77.8.** El principio de **No Autoincriminación,** al hacerle firmar dos cartas autoincriminatorias en las que aceptaba haber realizado memes ofensivos contra las autoridades de La Condamine.

PROBLEMA JURÍDICO

En esta decisión se analizan las sentencias derivadas de la acción legal presentada por el progenitor de un estudiante, quien enfrentó un proceso disciplinario por haber establecido una cuenta en la plataforma de redes sociales Instagram para compartir memes relacionados con la institución educativa. La Corte concluye que se han infringido los derechos al debido proceso, a las garantías de ser escuchado y que su opinión sea debidamente considerada, a la prohibición de autoincriminación, a la libertad de expresión y a la tutela judicial efectiva.

NORMAS JURÍDICAS RELEVANTES PARA EL CASO

- Constitución de la república del ecuador
- Reglamento de la Ley Orgánica de Educación Intercultural.
- Ley Orgánica de Educación Intercultural
- Código de Convivencia
- Reglamento Interno de la Institución Educativa
- Jurisprudencia de la Corte Constitucional del Ecuador
- Normativa relacionada con el uso responsable del internet y redes sociales por parte de niños, niñas y adolescentes.

HECHOS JURÍDICAMENTE RELEVANTES

1. La restricción del derecho a la libertad de expresión de R.S.A.E. se produjo a raíz de la imposición de una sanción por la difusión de un contenido considerado

deshonroso, sin una evaluación apropiada y desde la óptica de un adulto, a pesar de que se tratara de un individuo adolescente.

2. La violación del principio de no autoincriminación de R.S.A.E. se produjo al obligarlo a suscribir dos cartas autoincriminatorias en las cuales reconocía haber creado memes ofensivos dirigidos a las autoridades de La Condamine.

3. La ausencia de una evaluación detallada acerca de si la publicación realmente perjudicó la reputación, representa una violación al derecho a la libertad de expresión en general y en plataformas de redes sociales.

4. La negativa a permitir que R.S.A.E. hiciera uso de su derecho a la defensa a través de la intervención de sus padres, constituyó asimismo una infracción a su derecho al debido proceso.

5. Es esencial fortalecer la libertad de expresión en el entorno educativo, siempre y cuando se salvaguarden los derechos de los demás y se prevengan la discriminación y el maltrato.

6. La relevancia de asegurar el derecho a expresarse, comunicar y acceder a información, ideas, opiniones y otros aspectos relacionados con la esfera de vida que abarcan dichas instituciones.

7. Es imperativo llevar a cabo un análisis exhaustivo, considerando las circunstancias específicas de cada situación, con el propósito de verificar que cualquier restricción potencial a la libertad de expresión esté debidamente establecida por la ley, persiga un objetivo legítimo, y sea adecuada, necesaria y proporcionada para alcanzar dicho propósito.

DECISIÓN

Las decisiones tomadas en la Sentencia No. 785-20-JP/22 se basaron en el análisis de los hechos y la normativa aplicable, así como en la jurisprudencia de la Corte Constitucional del Ecuador.:

1. Establecer que el Colegio Unidad Educativa La Condamine infringió el derecho de R.S.A.E. al debido proceso, en lo que respecta a la garantía de ser escuchado y a la consideración de la opinión del estudiante al fundamentar la decisión, así como a la prohibición de autoincriminarse, en relación con el interés superior de los niños, niñas y adolescentes y el derecho a la libertad de expresión. Por otro lado, la Junta Distrital 17D05 de Resolución de Conflictos del Ministerio de Educación violó el derecho a la libertad de expresión.
2. Establecer que la Unidad Judicial de Tránsito de Pichincha ubicada en el Distrito Metropolitano de Quito y la Sala Penal de la Corte Provincial de Justicia de Pichincha infringieron el derecho a la tutela judicial efectiva de R.S.A.E., quien presentó una acción de protección a través de su padre.
3. Admitir la acción de protección presentada por Santiago Almeida, en calidad de representante legal de su hijo R.S.A.E., y anular las resoluciones fechadas el 14 de enero de 2020, emitida por la Unidad Judicial de Tránsito de Pichincha en el Distrito Metropolitano de Quito; y el 12 de mayo de 2020, proferida por la Sala Penal de la Corte Provincial de Justicia de Pichincha en el marco de la Acción de protección No. 17460-2019-06305.
4. Como medidas de reparación, se dispone:

i. El colegio deberá disculparse y enviar a R.S.A.E. y a sus padres, en un plazo de un (1) mes a partir de la notificación de esta resolución, una carta confidencial firmada por el Director General con el siguiente contenido:

"A nombre del Colegio 'Unidad Educativa La Condamine', y en cumplimiento de la sentencia emitida por la Corte Constitucional (785-20-JP/21), pido disculpas a [en la carta el colegio deberá poner los nombres correspondientes] por no haber respetado sus derechos al debido proceso y a la libertad de expresión, dentro del proceso disciplinario iniciado en contra del alumno por la creación de una cuenta en la red social Instagram ni haber generado un ambiente seguro para solucionar el conflicto. Nos comprometemos a tomar las medidas pertinentes para que, hechos como los sucedidos, no se vuelvan a repetir."

ii. La Junta Distrital tendrá la obligación de ofrecer disculpas y enviar a R.S.A.E. y a sus progenitores, en un plazo de un (1) mes desde la notificación de esta decisión, una carta de carácter confidencial suscrita por sus integrantes con el siguiente contenido:

"La Junta Distrital, en cumplimiento de la sentencia emitida por la Corte Constitucional (785-20-JP/21), pedimos disculpas a [en la carta se deberá poner los nombres correspondientes] por no haber respetado su derecho a la libertad de expresión, dentro del proceso disciplinario iniciado en contra del alumno por la creación de una cuenta en la red social Instagram. Nos comprometemos a tomar las medidas pertinentes para que, hechos como los sucedidos, no se vuelvan a repetir."

iii. El colegio deberá ajustar su Código de Convivencia conforme a lo establecido en esta resolución y en la jurisprudencia de la Corte

referente al debido proceso y la libertad de expresión. La institución educativa deberá comunicar a la Corte en un plazo de seis (6) meses, contados a partir de la notificación de este fallo, acerca de las modificaciones realizadas en su código de convivencia.

iv. El Ministerio de Educación está obligado a crear un documento que aborde el uso responsable de internet y redes sociales por parte de niños, niñas y adolescentes, con la finalidad de difundirlo y utilizarlo como material para posibles capacitaciones o talleres en este ámbito. Este documento deberá ser elaborado en un plazo de seis (6) meses a partir de la notificación de esta resolución.

v. El Ministerio de Educación tiene la obligación de establecer una directriz general para las instituciones educativas a su cargo, en la cual se adecuen sus procesos disciplinarios adoptando una perspectiva de justicia restaurativa, de acuerdo con la jurisprudencia emitida en este sentido por parte de la Corte Constitucional. Este ajuste deberá realizarse en un plazo de un (1) mes a partir de la notificación de esta resolución.

5. El Colegio, así como el Ministerio de Educación deberán informar a la Corte Constitucional el cumplimiento de las medidas dispuestas inmediatamente cumplidos los plazos determinados en el numeral anterior.
6. El acatamiento y supervisión de las medidas ordenadas al Ministerio de Educación deberán llevarse a cabo de manera conjunta con las indicadas en este sentido por la Sentencia No. 456-20-JP/21.
7. Notifíquese, publíquese y cúmplase.

ANÁLISIS

La Sentencia No. 785-20-JP/22 de la Corte Constitucional del Ecuador realiza un minucioso análisis sobre la violación del derecho al debido proceso y a la libertad de expresión en un caso de procedimiento disciplinario relacionado con la publicación de memes en redes sociales, se resalta la observación de la falta de aplicación del test tripartito y la omisión en la determinación del contenido de las expresiones difundidas, así como la importancia de examinar las medidas desde una perspectiva sistémica digital; el análisis se sustenta en la normativa nacional e internacional, así como en la jurisprudencia pertinente, con el propósito de salvaguardar los derechos del adolescente afectado y establecer las responsabilidades de las instituciones educativas, este enfoque demuestra el compromiso de la Corte Constitucional del Ecuador con la salvaguarda de derechos constitucionales fundamentales en el contexto de la era digital y educativa, sentando así un precedente significativo para futuros casos similares.

Elaborado por: Autor, 2023.

Estudio del Caso:

Tabla 3

Descripción del Tipo Penal "Pornografía Infantil"

Pornografía Infantil	
Tipo Penal	Pornografía Infantil
Bien Jurídico Protegido	➢ El derecho a la privacidad y a la propia imagen de los menores está respaldado por el artículo 66 de la Constitución de la República del Ecuador, este artículo

	asegura el derecho a la intimidad personal y familiar, así como la inviolabilidad del domicilio; además, garantiza el derecho a la propia imagen, a la identidad, al secreto de las comunicaciones y a la protección de datos personales. ➢ Derecho al desarrollo equilibrado del menor: Este derecho se encuentra protegido en el artículo 45 de la Constitución de la República del Ecuador, el cual establece que "se reconoce y garantiza a las personas el derecho al desarrollo integral a lo largo de su vida y al acceso a bienes y servicios de calidad, en especial en educación, salud, alimentación, seguridad social, agua, saneamiento, vivienda, ambiente sano y trabajo digno".
Procedimiento	Acción Pública
Pena o Sanción	➢ **Contenido sexual explicito sea extranjero o nacional:** Pena privativa de trece a dieciséis años. ➢ **Si la victima sufre algún tipo de discapacidad o enfermedad grave o incurable:** Pena privativa de libertad de dieciséis a diecinueve años. ➢ **Familiares directos, parientes hasta cuarto grado de consanguinidad o segundo de afinidad, entorno íntimo de la familia o maestros:** pena privativa de libertad de veintidós a veintiséis años. ➢ **Difusión de videos o contenido sexual explícito de menores, para uso personal o intercambio pornográfico:** Pena privativa de libertad de diez a trece años.

Fuente: Código Orgánico Integral Penal, (2014); Constitución de la República del Ecuador, (2008).

Elaborado por: Autor, 2023.

Tabla 4

Descripción del Tipo Penal "Acoso Cibernético"

Acoso Cibernético	
Tipo Penal	Acoso Cibernético
Bien Jurídico Protegido	➢ El derecho a la intimidad y privacidad está salvaguardado según lo dispuesto en el artículo 66 de la Constitución de la República del Ecuador, este artículo asegura el derecho a la intimidad personal y familiar, así como la inviolabilidad del domicilio, además, garantiza el derecho a la propia imagen, a la identidad, al secreto de las comunicaciones y a la protección de los datos personales. ➢ El derecho a la seguridad y protección está amparado por el artículo 66 de la Constitución de la República del Ecuador, este artículo asegura el derecho a la seguridad integral de las personas, entendida como la condición necesaria para el pleno ejercicio de los derechos y garantías constitucionales. ➢ El derecho a la igualdad y a no ser objeto de discriminación está respaldado por el artículo 11 de la Constitución de la República del Ecuador, este artículo sostiene que todas las personas son iguales y tendrán los mismos derechos, deberes y oportunidades sin sufrir discriminación alguna.
Procedimiento	Acción Pública
Pena o Sanción	➢ **SECCIÓN QUINTA. - Delitos contra el derecho a la igualdad: (Arts. 176-177) Art.177 COIP:** Actos de odio, pena privativa de libertad de uno a tres años. En caso de heridas, se sancionará la pena privativa de libertad para el delito de lesiones agravadas a un tercio. En caso de muerte de la víctima la pena privativa de libertad será de veintidós a veintiséis años.

	➢ **SECCIÓN SEXTA. – Delitos contra el derecho a la intimidad personal y familiar: (Arts. 178-181) Art-178 COIP:** violación a la intimidad, pena privativa de libertad de uno a tres años. (no aplica en grabaciones de audio y video en las que intervienen personalmente o información pública). Las penas privativas de este tipo van desde los 6 meses hasta los tres años como máximo. ➢ **SECCIÓN SÉPTIMA. - Delito contra el derecho al honor y buen nombre: Art. 182 COIP:** Calumnia (*Delito de Acción Privada art. 415*)**,** pena privativa de seis meses a dos años-

Fuente: Código Orgánico Integral Penal, (2014); Constitución de la República del Ecuador, (2008).

Elaborado por: Autor, (2023)

1.12. COLOMBIA

1.12.1. La Ciberseguridad:

En Colombia, la ciberseguridad se ha vuelto un tema de gran relevancia, destacándose el país por liderar la implementación de una planificación optima nacional en este ámbito, dicha estrategia implica la creación de inteligencia, establecimiento de un marco de comunicación y respuesta con actores clave, formación de grupos de inteligencia para analizar información, y diseño de pruebas similares que proporcionen retroalimentación a las entidades comprometidas con la seguridad cibernética; así mismo, se ha progresado en la creación de bitácoras informativas nacionales sobre la evolución la ciberseguridad en el sistema financiero, reflejando un enfoque integral y proactivo en la prevención de ciberdelitos (OEA, 2019).

Como se dio mención con anterioridad el Coronel de Ejército de Colombia Cáceres García, (2023) menciona que Colombia sobresale como líder en la región al poner en marcha una estrategia integral contra el cibercrimen, la cual se encuentra delineada en el CONPES 3701, la propuesta se centra en contrarrestar las amenazas cibernéticas y abordar el aumento del cibercrimen, demostrando una aproximación proactiva; dada la cifra anual global de US $ 575.000 millones asociada al cibercrimen, con alrededor de US $90.000 millones en la región, la adopción de esta estrategia nacional representa un paso crucial para salvaguardar el ciberespacio y resguardar a ciudadanos y empresas de posibles riesgos.

1.12.2. Los Ciberdelitos:

En Colombia, el ciberdelito se evidencia un aumento considerable en los últimos tiempos, agravado por la pandemia y el creciente uso de la tecnología, según un informe de 2022, el país se sitúa como el cuarto más afectado en la región, con un notorio incremento vinculado al teletrabajo y vulnerabilidades en los sistemas de información, las modalidades de ciberdelito abarcan desde el skimming hasta el ransomware, y se ha alertado sobre posibles incrementos durante eventos como el "Día sin IVA"; a pesar de los esfuerzos de las autoridades y el Ministerio de Defensa, la fragilidad en la ciberseguridad expone a numerosas personas y empresas, subrayando la necesidad de una evolución estratégica crucial para enfrentar estos desafíos en Colombia.

En Colombia, existen varios ciberdelitos los cuales se han estipulado en su órgano legal, sin embargo, para el foro Infobae, (2021), en colaboración con la Policía nacional de Colombia y el Centro Cibernético Policial, aquí se describen los más importantes:

1. **Acceso Abusivo a Sistemas Informáticos:** En Colombia, en el Artículo 269A del Código P., las penalizaciones son más acentuadas en casos que involucren redes estatales, la participación de un servidor público o la búsqueda de beneficios para el infractor o terceros, de acuerdo con informes del Centro Cibernético Policial Nacional, se ha observado un incremento en la incidencia de este delito durante los años 2020 y 2021, evidenciándose en intrusiones en

sistemas empresariales o gubernamentales, accesos no permitidos a correos y la manipulación de usuarios para obtener datos confidenciales; la prevención requiere la implementación de medidas como la restricción de accesos, la automatización de procesos, la formación del personal y la verificación de la autenticidad, siendo esencial para reducir su impacto y fortalecer la seguridad cibernética en Colombia.

2. **Violación de Datos Intimos:** La "Violación de Datos Personales" constituye un ciberdelito en Colombia que implica la adquisición, utilización o divulgación no autorizada de información personal, de acuerdo con la Superintendencia de Industria y Comercio (SIC), el país experimenta aproximadamente 79 casos diarios de violación de datos personales, manifestándose a través de diversas modalidades como la obtención mediante correos electrónicos, suplantación en plataformas sociales y comercialización en la dark web; la estrategia preventiva enfatiza la necesidad de implementar medidas de seguridad, restringir el acceso a información personal, capacitar al personal y verificar la autenticidad.

3. **Pornografía Infantil:** como se detalla en el CÓDIGO P. COLOMBIANO LEY 599 DE 2000, Articulo 218, la pornografía infantil en Colombia constituye una problemática social preocupante que ha suscitado atención desde sus inicios, la legislación colombiana aborda este delito al definirlo como la utilización de menores de 18 años en material pornográfico, imponiendo sanciones que oscilan entre 10 y 14 años de prisión, acompañadas de multas; además, Colombia ha ratificado el Convenio sobre la Ciberdelincuencia, que busca combatir los delitos informáticos, incluyendo la pornografía infantil, y establecer un marco legal para la seguridad de la información en el país (Murcia Gutiérrez , 2022).

4. **Acoso Cibernético:** Es un delito digital que daña a individuos sin excepción, se fundamenta en la difamación y humillación mediante plataformas digitales como mensajes, redes sociales y correos electrónicos, en el país, el acoso cibernético está en aumento y tiene vínculos con el acoso escolar y las

relaciones interpersonales; a pesar de los esfuerzos legislativos en Colombia, como la Ley 1273 de 2009 y la adhesión al Convenio sobre la Ciberdelincuencia, el acoso cibernético persiste como un desafío de importancia (Rojas Ramos, 2022).

1.12.3. Normativa:

En Colombia, se han establecido diversas normativas y regulaciones destinadas para prevenir así también sancionar los ciberdelitos, algunas de las principales disposiciones legales comprenden:

1. **La Ley 1273 de 2009,** que reforma el Código P., introduce una nueva categoría de protección legal (bien jurídico) llamada "de la protección de la información", esta legislación impone sanciones penales a quienes comprometan la seguridad de la información, abarcando acciones como el ingreso sin autorización a sistemas en línea de la información, el cambio de sistemas de resolución de nombres de dominio y la obtención de beneficio propio o ajeno Policía Nacional de Colombia (PONAL, 2017).

2. **La Ley 1928 de 2018,** ratifica la aprobación del Convenio sobre la Ciberdelincuencia, el cual busca combatir los crímenes informáticos y establecer una legislación para la salvaguarda de datos informáticos en el contexto colombiano, mismo que entró en vigor el 23 de noviembre de 2001, en Budapest (Mejía-Lobo et al., 2021).

3. **El Convenio sobre la Ciberdelincuencia**, que recibió aprobación en el año 2018, implementa una política integral de Ciberseguridad y Ciberdefensa en Colombia, complementando así la política previamente adoptada por el país en estas áreas en el año 2001 (El Congreso de la República de Colombia, 2001).

1.13. CHILE

1.13.1. La Ciberseguridad:

> Se ha podido evidenciar una evolución optima en los ciberdelitos en Chile, caracterizado por un incremento en su complejidad y su vínculo con actividades como el narcotráfico y la trata de personas, con el propósito de abordar este creciente problema, la Policía de Investigaciones estableció la Brigada Investigadora del Cibercrimen en los primeros años 2000; el phishing y el acceso ilícito han evolucionado hacia desafíos más avanzados, incluyendo los ataques de ransomware, en 2022, se introdujo una Política Nacional contra el Crímenes de mafias organizadas que se enfoca específicamente en la ciberdelincuencia, mientras que la Ley 21.459 actualizó la normativa sobre delitos informativos en Chile, estableciendo sanciones y reglas procesales (Lara Gálvez et al., 2014).

Como es evidente la evolución tecnológica ha traído evolución de los ciberdelitos para la prensa PDI Chile (2022), en Chile, la ciberseguridad ha experimentado avances mediante la introducción de mecanismos legales y tecnológicos, en 2017, se instituyó el Comité Interministerial de Ciberseguridad con el propósito de coordinar y fortalecer las políticas en este campo. Asimismo, se creó una unidad especializada en Tics para fortificar las defensas de Fuerzas Armadas; se han implementado medidas como sistemas de seguridad en la nube y programas antivirus para salvaguardar la infraestructura digital, este asunto abarca de manera general tanto al ámbito público como privado, impactando a la población en su conjunto.

1.13.2. Los Ciberdelitos:

La investigaciones evidencian que en chile crecen los ciberdelitos en la investigación de Cifuentes Fuentes (2023), se ha notificado un incremento en los ciberataques, con un aumento en el phishing y en los intentos de ataques mediante malware, la evolución de los ciberdelitos ha estado caracterizada por diversos modus operandi y estrategias que los delincuentes emplean para acceder a cuentas bancarias, suplantar identidades o cometer fraudes; sin embargo, se ha evidenciado un aumento en la complejidad del

cibercrimen, con un crecimiento en la cantidad de dispositivos electrónicos y un mayor empleo de ransomware y troyanos bancarios.

En la actualidad varios ciberdelitos son mitigados dentro de Chile, a continuación, se da mención de los delitos que más afluencia tienen según la Biblioteca del Congreso Nacional de Chile (2022):

1. **Ransomware:** hace referencia a un software malicioso que limita el acceso a archivos específicos o al sistema, exigiendo un pago como condición para levantar dicha restricción, aunque no se ofrece una cifra específica para Chile, este tipo de ciberdelito tiene importancia a escala mundial.
2. **Fuga de datos:** también conocida como filtración de datos, es conocida como la propagación de datos confidenciales, en el contexto de los ciberdelitos en Chile, la fuga de datos en las organizaciones representa un problema significativo.
3. **Pornografía Infantil:** En Chile, el ciberdelito de tarta de infantes con contenido muy explícito engloba la creación, almacenamiento, distribución con exhibición de contenido explícito que involucra a menores, un informe de la Policía de Investigaciones resalta la dedicación hacia la investigación de este delito, el cual forma parte de los delitos sexuales bajo escrutinio; a nivel mundial, la pornografía infantil es penalizada debido a su amenaza hacia los individuos más vulnerables, que comprenden desde bebés hasta los 18 años (Salguero Diaz, 2019).
4. **Acoso Cibernético:** En Chile, el acoso cibernético, que abarca hostigamiento, amenazas y difamación a través de medios tecnológicos, carece de una legislación penal específica, a pesar de la consideración de tecnología en las leyes sobre acoso en general, sexual, laboral y escolar, aunque se encuentra en proceso un proyecto de ley sobre violencia digital, aún no se ha establecido una normativa específica; a pesar de esta ausencia, el ciberacoso afecta a una amplia población y ha captado la atención de las autoridades (Díaz & Rivera, 2022).

1.13.3. Normativa:

Las leyes dentro de Chile son de uso exclusivo para enfrentar ciberdelitos, sino también como medio de colaboración en conjunto con entidades públicas y privadas

para obtener un control significativo de este tipo de delitos dentro del país, a continuación, se enlistan las más importantes:

1. **La Ley 21.459 de Delitos Informáticos**: divulgada en junio de 2022, presenta regulaciones concernientes a los delitos informáticos, esta legislación revoca la Ley 19.223 y realiza modificaciones en otras partes de la legislación con el propósito de ajustarlos al Convenio de Budapest; entre las infracciones penales abordadas se incluyen el acceso no autorizado, la intercepción indebida y la destrucción de un sistema de información en la red, entre otros (Figueroa, 2022).

2. **Convenio de Budapest:** a pesar de no formar parte de la legislación chilena, es importante destacar el Convenio de Budapest, ya que la Ley 21.459 se ajusta a este acuerdo, el cual es ampliamente empleado a nivel internacional para la creación de leyes destinadas a combatir el cibercrimen, la adhesión de Chile a este convenio ha impactado en la actualización de su normativa interna (Carrasco, 2022)

3. **Normativa Internacional:** La Biblioteca del Congreso Nacional de Chile (2015), da mención que es importante cuestionar que, junto con las leyes nacionales, Chile ha incorporado directrices internacionales, como las que se dan en los sistemas de legislación europea enfocado a la seguridad cibernética, en relación con los ciberdelitos, dando resultados que hasta la fecha un excelente manejo de la normativa legal en control de los ciberdelitos.

1.14. ARGENTINA

1.14.1. La Ciberseguridad:

En Argentina, se presentan desafíos en el ámbito de la ciberseguridad debido a la elevada frecuencia de delitos informáticos, tales como el phishing, fraudes en aplicaciones con dinero virtual o plástico y estafas piramidales, para mitigar estos desafíos, el país ha establecido la Dirección de Investigaciones del Ciberdelito y ha implementado el "Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos";

el propósito de estas iniciativas es salvaguardar a los ciudadanos, mitigar las amenazas y alertar acerca de nuevas estrategias empleadas por cibercriminales (Secretaría de Seguridad y Política Criminal, 2020).

A nivel nacional según la investigación de Castillo (2023), se han establecido políticas destinadas a resguardar las infraestructuras críticas de información y reforzar las capacidades en prevención, detección, respuesta y recuperación de problemas con la seguridad en redes informáticas, también se llevaron a cabo iniciativas de sensibilización mediante charlas tanto presenciales como en línea en instituciones educativas y organizaciones; el propósito es promover el desarrollo responsable dentro de redes de internet, así como proporcionar educación para los ciudadanos en el entorno digital, estas acciones buscan mitigar riesgos y asegurar una buena navegación, segura de los individuos en las redes.

1.14.2. Los Ciberdelitos:

El incremento de ciberdelitos ha llevado a una mayor regulación y colaboración de entes públicos, como también privados, en Argentina, se ha establecido el Protocolo de Actuación para las Fuerzas de Seguridad en Ciberdelitos, centrado en investigación, recuperación de pruebas y cadena de custodia digital; además, el CERT.ar emite informes anuales sobre incidentes de seguridad informática, subrayando dar fortaleza a las diversas capacidades de prevención, protección y resistencia en el ámbito de la ciberseguridad (Ministerio de Seguridad, 2016).

Varios ciberdelitos se han desarrollado en Argentina, pero según el Ministerio de Justicia Argentino (2020), nombra a continuación los ciberdelitos más importantes:

1. **Ataques a la navegación:** Redirigen a los usuarios hacia sitios web que resultan en infecciones con software malicioso, tales como virus, gusanos y troyanos, robando así varia información valiosa para el usuario, se destaca también el daño de archivos o sistemas operativos, en ocasiones sin fines de lucro.

2. **Fraudes Informáticos:** Estos actos ilícitos implican el control de sistemas informáticos para poder acceder a redes confidenciales o causar perjuicio a terceros, se brinda información que el usuario necesite o se ofrecen servicios en la web, que posteriormente son manipuladas con el fin de dañar los sistemas informáticos de las víctimas, e incluso extorsionar a los mismos por la devolución de dicha información

3. **Pornografía Infantil:** La comisión de actos delictivos relacionados con la pornografía infantil es un atentado contra la constitución de derechos de los infantes, presentándose en diversas formas como la explotación sexual infantil y el grooming, en Argentina, la Ley 26.388 establece sanciones para la producción de este material; de acuerdo con un informe emitido por el Ministerio Público de la provincia de Buenos Aires, se ha registrado un aumento del 30% en las instancias judiciales relacionadas con pornografía infantil en los últimos años (Barrio & Sarricouet, 2016 pp. 171-196).

4. **Acoso Cibernético:** El ciberacoso constituye un delito que abarca el hostigamiento, la intimidación o la humillación mediante medios electrónicos, siendo evidente en Argentina a través de mensajes amenazantes, difamatorios o con contenido sexual no deseado; la legislación argentina, en la Ley 26.904, define y penaliza este tipo de ciberdelito, un informe del Ministerio de Justicia y Derechos Humanos subraya que ha aumentado el ciberacoso, especialmente entre los adolescentes en Argentina.

1.14.3. Normativa:

Las leyes dentro de Argentina han tenido una evolución drástica las mismas que evidencian la gran laboral de los legisladores en conjunto con la influencia de países europeos y también los latinos mismos que integran convenios sobre ciberseguridad a nivel mundial los cuales dan latencia de ejemplo para que este país desarrolle sus leyes en bien la sociedad, a continuación, se resaltan las normativas más importantes descritas por la Jefatura de Gabinete de Ministro de Argentina, (2017):

1. **La Ley 26.388** es la más destacada en tema sobre Delitos Informáticos define consecuencias legales para aquellos que ejecuten, fomenten, faciliten, contribuyan, utilicen o se beneficien del uso inapropiado de programas de información.

2. **Ley 25.326** de Protección de la confidencialidad de datos de los individuos, garantiza esta ley el cuidado óptimo de datos confidenciales de la población en el ámbito de los ciberdelitos, describiendo una normativa que genere seguridad al uso de datos en la red común.

3. **El Decreto Reglamentario N° 2628/2002:** introduce cambios al Decreto Reglamentario N° 1558/2001, implementando medidas adicionales de seguridad para la información en entidades gubernamentales, trabajando en conjunto la legislación nacional, así como también las diversas entidades públicas encargadas de la defensa del país argentino.

4. **La Ley 26.904 sobre Grooming,** tiene como propósito enfrentar el grooming, una modalidad de delito cibernético que implica la manipulación psicológica de una persona con el fin de explotarla sexualmente.

1.15. ANALISIS DE JURISPRUDECIA DE COLOMBIA, CHILE Y ARGENTINA

Tabla 5

Jurisprudencia sobre "Pornografía infantil" en Colombia, Chile y Argentina

CIBERDELITO "PORNOGRAFÍA INFANTIL"		
COLOMBIA	**CHILE**	**ARGENTINA**
SENTENCIA DE TUTELA N.º 240/18 DE LA CORTE CONSTITUCIONAL DE COLOMBIA (26 de junio de 2018)	**SENTECIA N° ROL 1894 DE TRIBUNAL CONSTITUCIONAL DE CHILE (12 de julio de 2011)**	**CAUSA DE CASACIÓN N° 103.255 DEL TRIBUNAL DE CASACIÓN PENAL DE LA PRONVICIA DE BUENOS AIRES (24 de junio del 2021)**
El tema aborda la situación de un joven que fue expulsado de su instituto por difundir imágenes privadas de compañeras a través de plataformas en línea, la madre del adolescente interpuso una acción de tutela argumentando que se violaron los derechos fundamentales de su hijo durante el procedimiento disciplinario, la Corte Constitucional evaluó	La situación que examina el artículo está relacionada con una propuesta de legislación en Chile que abogaba por la identificación de usuarios de cibercafés, con la finalidad de abordar el acoso sexual a menores, la tenencia de material pornográfico y la representación virtual o simulada de la pornografía infantil; el Tribunal Constitucional de Chile emitió un	En esta ocasión, nos encontramos con un recurso de casación presentado por el Fiscal General en contra de la decisión de la Cámara de Apelación y Garantías del Departamento Judicial, el Fiscal sostiene que la Cámara realizó una valoración arbitraria de las pruebas recopiladas y una interpretación incorrecta y aplicación del artículo 128 del

si se respetaron las garantías procesales y si los derechos fundamentales del joven fueron vulnerados en este asunto.	fallo donde se ocupó de cuestiones debatidas y significativas, tales como la igualdad ante la ley, el derecho a la salvaguarda de la vida privada y el principio de reserva legal.	Código Penal, sin considerar adecuadamente el propósito y sentido de la norma; también expresó su descontento por el sobreseimiento de D., argumentando que aunque la imagen no mostraba los genitales de la niña, sí exhibía partes íntimas, constituyendo una representación de sus áreas genitales y una fotografía con contenido pornográfico infantil.
DERECHOS VULNERADOS	**DERECHOS VULNERADOS**	**DERECHOS VULNERADOS**
1. Derecho al debido proceso. **2. Derecho a la educación.** **3. Derecho al libre desarrollo de la personalidad.** **4. Derecho a la intimidad personal y familiar.** 5. Derecho al buen nombre y la honra.	1. Protección de la vida privada 2. Igualdad ante la ley	1. Protección de la integridad de los infantes ante delitos de pornografía o acoso infantil.

NORMATIVA UTILIZADA	NORMATIVA UTILIZADA	NORMATIVA UTILIZADA
1. Constitución Política de Colombia. **2. Ley 115 de 1994, por la cual se expide la Ley General de Educación.** **3. Decreto 1965 de 2013, por el cual se reglamenta la organización y funcionamiento de los Comités Escolares de Convivencia.** 4. Sentencias de la Corte Constitucional, como la T-323 de 1994, T-341 de 2003, T-459 de 1997, T-917 de 2006, entre otras**.**	1. Proyecto de ley sobre acoso sexual a menores, posesión de material pornográfico y Pornografía infantil virtual, sujeto a control constitucional 2. Código Penal Chileno art. 366 QUÁTER y QUINQUES (DEROGADO) 3. Constitución de la República de Chile, art. 77	1. Artículo 128 del Código Penal de la Provincia de Buenos Aires. 2. Artículo 18 de la Constitución Nacional. 3. Otros artículos del Código Penal y del Código Procesal Penal de la Provincia de Buenos Aires
PENA	**PENA**	**PENA**
• **Art. 218 Código Penal Colombiano:**10 a 20 años (multa de 150 a 1500 salarios mínimos) • Pena aumenta de una tercera parte a la mitad, cuando el responsable es miembro del núcleo familiar.	• **Art. 366 QUÁRTER Código Penal Chileno:** castigado con presidio menor en su grado medio o máximo (541 días a 5 años).	• **Art. 128 Código Penal Argentino:** Financiamiento, publicación, distribución de material (6 meses a 4 años)

		• Tener en su poder material P.I. (4 meses a 2 años) • Facilite acceso a espectáculos pornográficos o suministre material (1 mes a 3 años)
ANÁLISIS	**ANÁLISIS**	**ANÁLISIS**
La decisión judicial resalta la importancia de garantizar el trato adecuado de derechos constitucionales fundamentales de los estudiantes durante los procedimientos disciplinarios y de prevenir la divulgación de contenido íntimo a través de plataformas en línea, dicho de la misma forma, hace hincapié en la necesidad de que las instituciones educativas establezcan medidas eficaces para evitar y castigar este tipo de comportamientos	El Tribunal concluyó que la creación de un registro de usuarios de cibercafés (Ley n° 20.526) representaba una transgresión al derecho que asegura tener una vida privada. Razonaron que este registro posibilitaría la vigilancia de las acciones, preferencias y relaciones personales de los usuarios, aun en ausencia de una pesquisa específica o una orden judicial; el Tribunal resaltó la importancia de preservar los derechos de	La sentencia examinada se enfoca en determinar si la acción del acusado constituye un delito conforme a lo establecido en el artículo 128 del Código Penal de la Provincia de Buenos Aires. Luego de un análisis exhaustivo, la conclusión inicial es que la conducta en cuestión se ajusta prima facie a lo dispuesto en dicho artículo, en consecuencia, se valida el recurso de casación presentado por el Fiscal General, se anula la

	privacidad, incluso en combatir contra delitos graves.	decisión de la Cámara y se remite el caso a la instancia original para que continúe el procedimiento.

Fuente: SENTENCIA DE TUTELA Nº 240/18, (2018); SENTECIA N° ROL 1894, (2011); CAUSA DE CASACIÓN N° 103.255, (2021)

Elaborado por: Autor, (2023).

1.2. Objetivos:

1.2.1. Objetivo General:

Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.

1.2.2. Objetivos Específicos:

1. Analizar y comparar las leyes, regulaciones y políticas existentes en el marco jurídico de seguridad cibernética de Ecuador, Colombia, Chile y Argentina, identificando las principales brechas y diferencias entre ellos.

2. Evaluar la efectividad y aplicabilidad de las disposiciones legales y mecanismos de aplicación relacionados con la seguridad cibernética en Ecuador, a través de un análisis detallado de su implementación y resultados prácticos, contrastándolos con las experiencias de Colombia, Chile y Argentina.

3. Identificar y proponer recomendaciones específicas para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas y enfoques exitosos utilizados en Colombia, Chile y Argentina. Estas recomendaciones deben abordar las brechas identificadas y estar orientadas a mejorar la prevención, detección, respuesta y sanción de los delitos y amenazas cibernéticas en el país.

CAPÍTULO II

METODOLOGÍA.

2.1.Materiales

Recursos Humanos

El titular de este proyecto de investigación, es el señor Jimmy Paúl Cóndor Rosas, con cedula de ciudadanía número 180488502-6, de 27 años, con un estado civil soltero, estudiante de la carrera de Derecho matriculado en noveno semestre de la misma en la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato.

La persona encargada como tutor en este proyecto de investigación es el Dr. José Luis Romo Santana, docente de la Institución de Educación Superior en la cual se ha elaborado este proyecto de investigación.

Recursos Institucionales

El desarrollo de este proyecto de investigativo se tomó en consideración el apoyo de diversas instituciones, como fuente principal es la Universidad Técnica de Ambato, con sus instalaciones, siendo este el lugar de estudio del autor

Recursos Materiales

Los elementos materiales empleados en esta tesis abarcan equipos de cómputo, software especializado, libros, artículos científicos y suministros de oficina; estos recursos se utilizan con la intención de recopilar, analizar y presentar los datos útiles para el desarrollo de la tesis, el equipo de cómputo y códigos legales referentes al derecho penal nacional como internacional, mismos que desempeñarán un papel crucial en el análisis de datos, la redacción del documento y la creación de tablas que respalden los descubrimientos.

Por otro lado, los libros y artículos científicos proporcionarán la base teórica y contextual para la investigación, así también páginas como Lexis y vLex, donde la búsqueda de jurisprudencia es más sencilla, de igual forma, el material de oficina será útil para organizar pensamientos, apuntes necesarios y escritura de borradores.

2.2.Métodos

La seguridad cibernética es un tema fundamental en la presente sociedad, debido al constante avance de las Tics, debido a esto, el estudio comparativo del sistema jurídico en relación con la seguridad cibernética se presenta como una herramienta fundamental para comprender y analizar cómo diferentes países abordan esta problemática desde un enfoque legal, dando por evidencia que dentro del presente proyecto es importante indagar dentro de diversas fuentes bibliográficas las cuales darán apertura al proceso de investigación, mediante metodología que de estructura al mismo.

La estructura metodológica de una tesis resulta crucial al justificar y explicar cómo utilizando herramientas varias se puede tener resultados concretos, al aclarar los supuestos del estudio, facilita la comprensión del trabajo y posibilita la adaptación y progresión de la metodología, garantizando la coherencia y consistencia en la recopilación de datos; la elaboración de esta estructura también es fundamental para garantizar la calidad y fiabilidad de los hallazgos, respaldar la elección de la metodología utilizada y permitir que los lectores y expertos en el campo evalúen el trabajo (Rivas, 2022).

2.2.1. Tipos de Investigación

Conforme a lo describe la revista virtual Lifeder, se puede entender la metodología descriptiva como un enfoque cualitativo aplicado en investigaciones que buscan evaluar aspectos específicos de una población o variada situación (Lifeder, 2022); este proyecto tiene como meta principal llevar a cabo un análisis comparativo del marco

legal relacionado con la seguridad cibernética en la República del Ecuador, Colombia, Chile y Argentina, utilizando la metodología descriptiva, con este propósito, se llevará a cabo un examen minucioso de las leyes, regulaciones y jurisprudencia de cada uno de estos países en materia dentro del marco de seguridad cibernética; de la misma forma, se expondrán las particularidades de las diversas normativas con el fin de recabar información que permita la identificación semejanzas, discrepancias y vacíos entre las regulaciones de ciberseguridad.

2.2.2. Método de Investigación

La indagación científica de Fran Arellano sobre investigación cualitativa, se describe como un conjunto de métodos empleados para recolectar e interpretar información sobre el comportamiento, las experiencias y el significado de las personas, este método no sigue un enfoque cuantitativo y, por ende, no es medible, aunque permite una exploración detallada de las experiencias humanas o de temas específicos (Arellano, 2015); la perspectiva cualitativa inicia con la colección de criterios e información crucial no numérica, facilitando así una exploración minuciosa de cada sistema jurídico, en este contexto, se pueden emplear diversas fuentes de información, como textos legales, documentos oficiales, informes, estudios de casos, entrevistas con expertos en seguridad cibernética y análisis de jurisprudencia relevante.

2.2.3. Fuentes de Investigación

Los criterios dentro del portal web En "economipedia", y según Francisco Coll Morales las fuentes de investigación secundaria proporcionan información organizada, elaborada y analizada deliberadamente por terceros (Morales, 2021); se consideran herramientas útiles para abordar situaciones complejas y ofrecer soluciones viables, las fuentes secundarias de investigación abarcan materiales que recopilan, analizan y sintetizan información previa sobre el tema, como libros, revistas académicas, informes gubernamentales, documentos de organizaciones internacionales y artículos periodísticos, en el contexto de la seguridad cibernética en los países seleccionados.

El uso de estas fuentes tiene varias ventajas porque suelen proporcionar una panorámica más amplia y actualizada de la situación de la seguridad cibernética en cada nación, al investigar y recopilar información de diversas fuentes primarias, los expertos y académicos brinda una visión global y actualizada de los desarrollos legales y prácticos en este ámbito.

Así también podemos mencionar que, según lo analizado por el autor dentro de esta investigación, es de gran utilidad las fuentes primarias, al analizar normativa legal, convenios o tratados internacionales que hablen sobre el tema, pero de crucial importancia el uso de la Constitución de los diferentes países para anclar información dentro de la jurisprudencia vincula al proyecto de investigación.

2.2.4. Técnicas de Investigación

En el contexto de un proyecto de investigación Montagud Rubio (2020), menciona que las técnicas de investigación se consideran instrumentos para adquirir información y conocimiento; son seleccionadas en base al objeto de estudio y al proyecto específico, la selección apropiada resulta óptimo para dar viabilidad y coherencia a los resultados, siendo esencial llevar a cabo una evaluación crítica de las varias fuentes usadas para obtener información para el proyecto, siendo las siguientes:

- **Técnica de Observación:** para criterio de Sanjuán Nuñez (2019), en un proyecto de tesis, la observación tiene como objetivo principal la confirmación directa de fenómenos, evitando sesgos y errores; su enfoque se dirige hacia la comprensión de significados y valores atribuidos por los sujetos, adquiriendo información a través de la interacción directa, facilita la descripción y explicación de comportamientos, el establecimiento de relaciones con los sujetos u objetos de estudio, así como la recopilación sistemática de datos.

- **Técnica de Búsqueda Bibliográfica:** como argumentan Gómez-Luna et al. (2014), la búsqueda bibliográfica busca identificar, evaluar y resumir las evidencias existentes de otros investigadores para ampliar el conocimiento y comprender el estado actual de la temática, facilita la comprensión lectora, el

informe de tendencias y el establecimiento de conexiones con investigaciones previas, aportando enriquecimiento y legitimación al proyecto; de la misma manera, contribuye a fundamentar la importancia del tema, identificar posibles líneas de investigación y prevenir la repetición de estudios.

- **Técnica de Entrevista:** citando a Díaz-Bravo et al. (2013)**,** la técnica de las entrevistas tiene un solo propósito obtener información de manera oral y personalizada acerca de eventos, experiencias y opiniones vinculadas al tema de investigación, su utilidad se destaca en estudios descriptivos y etapas exploratorias, donde contribuye al diseño de herramientas para la recopilación de datos y a la elucidación de aspectos que pueden resultar ambiguos para el entrevistador.

2.2.5. Instrumento de Investigación

Dentro del criterio de Ortega (2021), los instrumentos de investigación son medios para recolectar y analizar datos en concordancia con las preguntas formuladas, estos pueden abarcar mediciones, confirmaciones, recopilación de información y verificación de situaciones; la selección de estos instrumentos como se los han descrito en el anterior párrafo se determina según el tipo de investigación, los objetivos y las preguntas específicas planteadas en la tesis, en este caso la entrevista constara de 8 preguntas las cuales arrojaran resultados complementarios para dar coherencia y extender la información actual del proyecto.

2.3.Población y Muestra

Población: para criterio de Díaz de León (2018), la población se define como el conjunto integral de elementos o individuos que comparten una característica o propiedad común y que son objeto de investigación. En otras palabras, constituye la totalidad del grupo que se está examinando y del cual se pueden obtener los descubrimientos deseados.

Muestra: fundamentado por Morrou Roldán et al., (2005), la muestra constituye una pequeña parte o subconjunto representativo extraído de una gran cantidad de individuos en su totalidad, en lugar de estudiar a todos los individuos en la población, se selecciona una muestra más pequeña que se considera representativa de la población en su conjunto, la muestra se utiliza para realizar inferencias y sacar conclusiones sobre la población completa.

Debido a como se ha desarrollado la investigación, aplicar la población y muestra no es pertinente en un estudio comparativo de seguridad cibernética que examina los marcos legales de Ecuador, Colombia, Chile y Argentina, en su lugar, se analizó de manera comparativa información varia de los sistemas legales y jurídicos de los cuatro países, evaluando sus leyes, regulaciones y políticas en relación con la seguridad cibernética; el propósito es proporcionar una visión detallada de los sistemas legales en cada país y ofrecer recomendaciones para mejorar las medidas de seguridad cibernética en cada uno de ellos.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1.Evaluación y argumentación derivadas de las entrevistas.

A continuación, se presentará la tabulación de información obtenido en encuestas realizadas a diversos profesionales del ámbito legal, estos datos resultarán esenciales para enriquecer y complementar la investigación en conjunto con información comparativa dentro del presente proyecto de investigación, dando un panorama más óptimo a la comparación legislativa, la manera de imponer sanciones, así como también las estrategias tomadas dentro de la ciberseguridad para combatir los delitos tecnológicos y concluir cual legislación es la más fuerte dentro de la investigación; se han tomado en consideración 5 entrevistados y su opiniones profesionales, mismas que se han recopilado en audio y posteriormente transcrito de manera digital en el formato de entrevistas correspondiente.

A continuación, se detalla la tabla de preguntas y respuestas, así como también los nombres correspondientes de los entrevistados:

Tabla 6

Análisis de Preguntas y Respuestas

PREGUNTAS / ENTREVISTADOS		Teniente Coronel Xavier Chango Llerena / *Unidad de Criminalística de la Policía Nacional*	Capitán Carlos Francisco Osorio Vega / *Jefatura Zonal de Criminalística del Distrito Metropolitano de Quito*	Dr. Jonathan Ramos / *Universidad Central del Ecuador*	Dr. Juan Francisco Pozo Torres / *Universidad San Francisco de Quito*	Dr. José Heriberto Garcia Peña / *Tecnológico de Monterrey (México)*
Pregunta 1:	**¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?**	La legislación en nuestro país es limitada y necesita actualizarse. A diferencia de Colombia, donde cuentan con centros y patrullajes cibernéticos regulados, en nuestro país carecemos de estas medidas, aunque tenemos normativas penales en el COIP, estas sancionan	Es esencial reformar el COIP para asegurar la obtención y presentación de evidencia digital en el marco jurídico, ya que las acciones actuales se realizan principalmente en entornos digitales. La reforma debería facultar la presentación de evidencia digital como	Ecuador cuenta con un marco jurídico de seguridad cibernética basado en la Constitución, la Ley de Protección de Datos y el Comité Nacional de Ciberseguridad. Aunque destaca por el reconocimiento constitucional y las estrategias implementadas,	En comparación con Colombia Chile y Argentina la legislación ecuatoriana no da respuesta la a ciberseguridad a pesar de poseer ciertas normas, las mismas no son especificas o referentes a la ciberseguridad, por lo	Ecuador está desarrollando su marco jurídico de seguridad cibernética, con énfasis en el cuidado de datos. Sin embargo, presenta carencias en la claridad de sanciones y medidas preventivas. Al compararse con otros países, Ecuador

		algunos delitos, pero no abarcan completamente los nuevos delitos surgidos con las nuevas tecnologías y desarrollos.	prueba válida en investigaciones ante la autoridad competente.	enfrenta la debilidad de la falta de conocimiento público sobre ciberseguridad, comparado con Colombia, Chile y Argentina, Ecuador muestra compromiso, pero enfrenta desafíos en la difusión de derechos y políticas de ciberseguridad.	cual hace falta un cuerpo normativo especifico que rija las mimas, por cual estamos muy atrás de los países mencionados.	muestra un rezago en madurez y especificidad de su marco legal en ciberseguridad. Colombia y Chile lideran con regulaciones avanzadas, mientras que Argentina ha avanzado significativamente en su marco jurídico
Pregunta 2:	**¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de**	Es crucial reducir la brecha tecnológica considerando las nuevas tecnologías en las políticas públicas,	Actualmente, los artículos se centran en el levantamiento de indicios en el territorio, que	Para superar las deficiencias en seguridad cibernética en Ecuador, se plantea la idea de priorizar	Se requiere una codificación, es decir unificar las normas que se encuentran en	La normativa de seguridad cibernética en Ecuador necesita mejoras concretas,

	seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?	abarcando tanto su uso por el Estado como por la ciudadanía. También es necesario abordar los nuevos delitos que puedan surgir con estos avances para evitar un aumento de la brecha, se destaca la importancia de un uso responsable y ético de las tecnologías, con sanciones para casos de mal uso.	antiguamente implicaba todo lo físico en el lugar de los hechos. Sin embargo, con la proliferación de dispositivos tecnológicos, se necesita una normativa que defina cómo recopilar y presentar como prueba los indicios de computadoras, dispositivos móviles y otros equipos tecnológicos.	la divulgación de derechos y políticas, adoptar medidas para proteger los datos y establecer una entidad reguladora, la sugerencia se basa en la Ley de Protección de Datos de Ecuador y las estrategias empleadas por otros países en la región.	diferentes códigos procesales, penales y más para formar un cuerpo normativo que permita el manejo de la legislación.	como aumentar la claridad en cuanto a las sanciones y medidas preventivas, incluir disposiciones más detalladas sobre ciberseguridad y contemplar la implementación de reglamentaciones más específicas. Comparar las experiencias de Colombia, Chile y Argentina podría ofrecer ideas valiosas para modernizar la legislación en Ecuador

Pregunta 3:	**¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?**	Se consideraría no emitir un concepto para evitar un sesgo.	La cibernética involucra la interacción entre humanos, dispositivos tecnológicos y sistemas. Se propone formalizar la digitalización, preservando las pruebas en formato digital en lugar de materializarlas físicamente para no perder su validez.	Las leyes de ciberseguridad en Ecuador, Colombia, Chile y Argentina comparten el reconocimiento constitucional del cuidado de información valiosa y la implementación crucial de estrategias. Sin embargo, difieren en la creación de entidades reguladoras y la divulgación de derechos, lo cual podría afectar la eficacia de los marcos legales, resaltando la importancia de una mayor conciencia pública para	Más que similitudes existen diferencias, puesto que los otros países tienen un marco jurídico más desarrollado y codificado, mientras que el de nuestro país tiene normas desperdigadas, que no permiten una respuesta clara para la regulación de la ciberseguridad, entonces esto si influye en la eficacia, al poseer un instrumento legal	Ecuador, Colombia, Chile y Argentina tienen enfoques comunes en la protección de información vital y la promoción de incidentes, pero con diferencias en el nivel de detalle y claridad. Ecuador necesita mejoras específicas en sanciones y medidas preventivas, mientras que Colombia y Chile tienen regulaciones avanzadas. Argentina

				mejorar la protección ciudadana.	más avanzado dan una respuesta más clara.	ha experimentado avances significativos en su marco legal.
Pregunta 4:	**¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?**	La problemática de los delitos modernos radica en su carácter transfronterizo en el ámbito digital, a diferencia de los delitos antiguos que tenían límites definidos, dada la falta de rostros y nombres, es esencial contar con legislación transfronteriza que permita enjuiciar estos delitos mediante normativas aplicables en diversos países.	Como se mencionó si es una prueba que se cometió a través de la cibernética y esta digitalizado, las pruebas no se deben materializar, se debería conservarse y garantizar la integridad y originalidad del contenido.	Se detectaron deficiencias en los marcos legales de ciberseguridad, incluyendo la falta de difusión de derechos, políticas públicas, medidas de protección de datos y reguladores. Estas brechas pueden afectar la seguridad cibernética en Latinoamérica, destacando la importancia de difundir derechos y políticas para fortalecer la protección	Las falencias especificas están en la evolución constante, en materia de Ciberseguridad se actualiza cada momento, aparecen nuevas formas de entender, nuevas tecnologías que regulan cosas o la interacción social y jurídica de la sociedad. Otra seria que no existen una revisión	Se han observado carencias específicas en los marcos jurídicos de seguridad cibernética, destacando la falta de claridad en sanciones y medidas preventivas en Ecuador, en contraste con Colombia y Chile que lideran en regulaciones avanzadas. Estas deficiencias pueden restringir la capacidad

				ciudadana y la estabilidad en el ciberespacio.	constante desde términos hasta nuevas tecnologías.	de responder a amenazas emergentes y complicar la colaboración regional, impactando la seguridad cibernética en América Latina al dificultar la coordinación de esfuerzos y la capacidad de abordar desafíos de manera conjunta.
Pregunta 5:	**¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en**	Aunque existen sanciones para los delitos cibernéticos en el país, la aplicación efectiva a veces falla	Se ha reflejado en que los delitos se están cometiendo en las redes sociales, correos	Ecuador muestra compromiso en ciberseguridad con políticas, el Comité	Por la falta de una respuesta clara, actualizada y codificada que regule la Cibercriminalidad.	Ecuador necesita mejorar su legislación de seguridad cibernética,

	comparación con Colombia, Chile y Argentina,	debido a la inadecuación de la legislación y a la falta de conocimiento y herramientas por parte del personal encargado de las investigaciones, los vacíos en la normativa y las herramientas necesitan ser mejorados para fortalecer el proceso de judicialización y sanción en este ámbito.	electrónicos, entre otras, se ha visto que existen diferentes delitos que concurren a obtener información y estafar a las personas, suplantar identidades y ocasionar daños.	Nacional y reconocimiento constitucional de protección de datos. Aunque ha avanzado, enfrenta desafíos en la difusión de derechos y políticas públicas en comparación con Colombia, Chile y Argentina. Necesita aumentar la conciencia para mejorar su efectividad en seguridad cibernética.		especialmente en sanciones y medidas preventivas, en comparación con Colombia, Chile y Argentina, que tienen regulaciones más avanzadas. La falta de detalles específicos en las leyes puede complicar la implementación efectiva y la capacidad de respuesta ante amenazas cibernéticas
Pregunta 6:	**¿cuáles son los principales desafíos identificados en su**	Es esencial establecer un centro cibernético para la	Los principales desafíos son contar con una	Ecuador se enfrenta a desafíos en ciberseguridad,	Los principales desafíos es que se debe tomar en	La legislación de seguridad cibernética

	implementación de las disposiciones legales de seguridad cibernética en Ecuador?	vigilancia y respuesta a ataques informáticos, especialmente porque Ecuador figura entre los países que sufren ataques no ampliamente conocidos. Esto requiere fomentar una cultura de seguridad ciudadana y asegurar que todas las instituciones involucradas estén preparadas, la implementación de patrullajes cibernéticos es fundamental para prevenir, investigar y sancionar los ataques cibernéticos.	tecnología forense adecuada, la cual permita garantizar su obtención del contenido digital para a través de Fiscalía poder presentar este tipo de pruebas, así como también garantizar la obtención del contenido digital.	como la divulgación de derechos y políticas públicas, un mejor trabajo en preparar a fuerzas de seguridad, la colaboración entre instituciones, el fortalecimiento de la infraestructura cibernética y la promoción de la ciberseguridad. Estos desafíos, compartidos en Latinoamérica, impactan la protección de datos y la estabilidad en el ciberespacio. A pesar del compromiso ecuatoriano, es crucial mejorar la	serio el tema de seguridad cibernética para llegar a instancias legislativas y permitan una codificación consensuada por los actores que se ven involucrados o afectados por los ataques cibernéticos o de la información de los ficheros de datos, es decir tener la voluntad de crear un cuerpo único y legal que responda a las necesidades.	en Ecuador necesita mejoras, especialmente en la claridad de sanciones y medidas preventivas, en concordancia con países regionales como Colombia, Chile y Argentina, que tienen regulaciones más avanzadas. La falta de detalles específicos en las leyes puede complicar la capacidad de respuesta ante amenazas cibernéticas

				difusión y comprensión de derechos y políticas públicas para optimizar la eficacia en seguridad cibernética.		
Pregunta 7:	**¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?**	A diferencia de Colombia, donde existen organismos que supervisan varios centros cibernéticos para anticipar amenazas, en el país actualmente no hay organismos ni colaboración entre entidades para lograr resultados efectivos en este ámbito.	Los aciertos es que el equipamiento tecnológico forense que ya existe y es actualizada, ya que a través de ella se implementa metodología, técnicas y capacitación para el aprovechamiento de herramientas.	Colombia mejora colaboración público-privada en ciberseguridad. Chile aplica estrategias nacionales; Argentina, normativas y concientización. Ecuador debe enfocarse en cooperación, estrategias nacionales y regulaciones educativas.	Los aciertos es que existe una legislación que se debería estudiar para poder implementar en el país de una forma que responda a lo que sucede con los temas de ciberdelitos que se dan o son los más frecuentes en el país.	Los logros en la implementación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina, evidenciados por la adopción de regulaciones avanzadas y enfoque progresivo, proporcionan valiosas lecciones para mejorar

						el buen trabajo de la legislación y normativas en Ecuador, tomar como ejemplo el éxito en la evolución de los marcos legales de estos países podría fortalecer la capacidad de respuesta y adaptabilidad de Ecuador frente a los desafíos cibernéticos
Pregunta 8:	**¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores**	Es crucial aprender de las experiencias de países vecinos, especialmente en delitos cibernéticos. Se deben aplicar estrategias	Se propone fortalecer la parte jurídica con artículos más centrados en el ámbito digital, ya que el marco legal actual	En el caso de Ecuador, sería aconsejable fortalecer la cooperación entre el sector público y privado, implementar estrategias	Crear un marco legal eficaz para la ciberseguridad con herramientas claras para su	Para fortalecer la seguridad cibernética en Ecuador, se propone mejorar la claridad normativa, adoptar

	prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?	adaptadas a las particularidades del país, fortaleciendo la legislación nacional y transnacional, además, es esencial dotar de equipos y mejorar los conocimientos del personal en esta área.	se enfoca principalmente en la escena física del delito. Es necesario que el marco jurídico se oriente hacia la evidencia digital para que sea una prueba válida ante la autoridad competente, evitando así la invalidación de pruebas y la nulidad de sentencias.	nacionales de ciberseguridad y promulgar regulaciones precisas con un enfoque educativo. Estas acciones podrían abordar las deficiencias identificadas al mejorar la coordinación, la preparación estratégica y la conciencia sobre seguridad cibernética en la nación.	implementación, abordando tanto la seguridad privada como la estatal. Se requiere normativa que establezca organismos especializados para cerrar la brecha con otros países.	regulaciones más detalladas inspiradas en las prácticas de Colombia y Chile, y seguir una aproximación progresiva, tomando como ejemplo la evolución exitosa en Argentina.

Elaborado por: Autor (2023).

Análisis comparativo de resultados

Primera pregunta ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Análisis de resultados

Los participantes dentro de la entrevista sobre Seguridad Cibernética en Ecuador y naciones cercanas concuerdan en que el marco jurídico relacionado con la seguridad cibernética en Ecuador está en fase de desarrollo y presenta algunas lagunas y debilidades en comparación con los sistemas legales de Colombia, Chile y Argentina.

Específicamente, se resalta la especial consideración dada a la protección de datos en la legislación ecuatoriana, aunque se señala la falta de claridad en las sanciones y medidas preventivas, además, se observa un rezago en la madurez y especificidad del marco legal de ciberseguridad en Ecuador en comparación con Colombia y Chile, que lideran con regulaciones avanzadas, y Argentina, que ha avanzado notablemente en su marco jurídico.

En líneas generales, los entrevistados sugieren la necesidad de mayor claridad y especificidad en la legislación ecuatoriana respecto a la seguridad cibernética, así como una mayor atención a las sanciones y medidas preventivas; de igual manera se destaca la importancia de examinar y aprender de las leyes de países más desarrollados mejorando así la legislación en Ecuador.

Segunda pregunta ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Análisis de resultados

Las acciones específicas propuestas para mejorar la legislación de seguridad cibernética en Ecuador, los entrevistados recomiendan la adopción de regulaciones más detalladas basadas en las prácticas de Colombia y Chile, de igual manera, sugieren mejorar la claridad normativa y seguir un enfoque progresivo, tomando como referencia el exitoso desarrollo observado en Argentina.

En términos generales, se enfatiza la importancia de fortalecer el marco legal de seguridad cibernética en Ecuador para potenciar la capacidad del país para hacer frente de manera efectiva a los desafíos en este ámbito; se plantea la idea de que las sugerencias presentadas podrían abordar las deficiencias identificadas al proporcionar un marco legal más sólido y adaptable.

Tercera pregunta ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Análisis de resultados

Los participantes resaltan las notables disparidades en las leyes y regulaciones de ciberseguridad en los países analizados, haciendo hincapié en que los demás países cuentan con marcos legales más desarrollados y detallados, se enfatiza que estas diferencias pueden afectar la eficacia de los marcos legales respectivos, ya que un marco legal más avanzado garantiza una respuesta más clara y efectiva en la regulación de la ciberseguridad.

En este contexto, se subraya la necesidad de que Ecuador refuerce y actualice su legislación para mejorar su eficacia en la protección contra riesgos cibernéticos, tomando como referencia los éxitos en la implementación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina; estos logros demuestran la adopción de regulaciones avanzadas, un enfoque progresivo y claridad en los detalles, ofreciendo valiosas lecciones de mejora legal del Ecuador frente a estos delitos.

Cuarta pregunta ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

Análisis de resultados

En el presente informe acerca de Seguridad Cibernética en Ecuador y naciones circundantes, los entrevistados señalan diversas deficiencias específicas en el marco

legal de seguridad cibernética de los países evaluados, estas deficiencias incluyen la falta de claridad en las sanciones y medidas preventivas en Ecuador, mientras que Colombia y Chile lideran en regulaciones más avanzadas; se da como evidencia necesaria contemplar integrar a la normativa vigente legislación transfronteriza que permita enjuiciar delitos mediante normativas aplicables en distintos países.

Los participantes sugieren que estas brechas podrían restringir la capacidad de reacción ante amenazas emergentes y dificultar la colaboración regional, afectando la seguridad cibernética en América Latina al impedir la armonización de esfuerzos y la capacidad de abordar desafíos de manera coordinada; por lo tanto, se enfatiza la importancia de fortalecer y actualizar el marco legal de seguridad cibernética en Ecuador y otros países afines para optimizar la capacidad de respuesta y colaboración en la lucha contra los riesgos cibernéticos.

Quinta pregunta ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina?

Análisis de resultados

En el documento acerca de Seguridad Cibernética en Ecuador y naciones cercanas, los participantes enfatizan que los delitos cibernéticos en Ecuador se han manifestado a través del uso de redes sociales, correos electrónicos y otros canales para llevar a cabo acciones delictivas como la obtención de información, estafas y suplantación de identidad; si embargo, indican que la efectividad de las leyes de seguridad cibernética en Ecuador ha sido limitada, evidenciándose casos en los cuales la legislación no resulta adecuada o el personal carece del conocimiento y herramientas necesarios para

llevar a cabo investigaciones apropiadas, generando vacíos en la normativa y las herramientas para mejorar el proceso de judicialización y aplicación de sanciones.

Estos descubrimientos resaltan la urgencia de fortalecer la legislación y proporcionar capacitación al personal para mejorar la eficacia de las normativas de ciberseguridad en el país; de la misma forma, se destaca el abordaje los delitos cibernéticos, teniendo en cuenta la el desarrollo que da la tecnología y como destruye la sociedad en la comisión de delitos en el ámbito digital.

Sexta pregunta ¿cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Análisis de resultados

En el informe acerca de Seguridad Cibernética en Ecuador y naciones circundantes, los participantes señalan diversos desafíos en la implementación de las disposiciones legales de seguridad cibernética en Ecuador; estos desafíos incluyen la carencia de claridad en sanciones y medidas preventivas, la necesidad de mejorar la especificidad y detallar las regulaciones, así como trabajar en el aprendizaje de las fuerzas públicas de seguridad al igual que los individuos civiles; de manera similar se menciona la importancia de fomentar la cooperación interinstitucional y fortalecer la infraestructura cibernética.

Estos resultados resaltan la urgencia de abordar de manera integral los desafíos en la implementación de las disposiciones legales de seguridad cibernética en Ecuador, teniendo en cuenta la necesidad de mejorar la capacitación de la sociedad en general, así como promover la cooperación interinstitucional y fortalecer la infraestructura

cibernética, de la misma forma, se destaca la importancia de mejorar la especificidad y detallar las regulaciones para asegurar una cobertura completa y actualizada en un entorno tecnológico en constante cambio.

Séptima pregunta ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

Análisis de resultados

En el informe acerca de Seguridad Cibernética en Ecuador y naciones circundantes, los participantes subrayan la relevancia de la ayuda internacional en la prevención de los ciberdelitos, indican que la colaboración entre instituciones y la cooperación entre países son esenciales para afrontar los desafíos en materia de seguridad cibernética en la región.

Estos resultados resaltan la necesidad de fortalecer los convenios para cooperación y aprendizaje internacional en la rama de tecnología delictiva, considerando la importancia de compartir información y recursos para mejorar la capacidad de respuesta y colaboración frente a los riesgos cibernéticos; además, enfatizan la importancia de establecer acuerdos y protocolos de cooperación para asegurar una respuesta efectiva y coordinada en caso de incidentes cibernéticos que trasciendan las fronteras.

Octava pregunta ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Análisis de resultados

En el documento acerca de Seguridad Cibernética en Ecuador y países circundantes, los participantes destacan la importancia de crear una legislación especial de ciberdelitos así como existen en Colombia, Chile y Argentina, se subraya la necesidad de mejorar la claridad normativa, adoptar regulaciones más detalladas inspiradas en las prácticas de otros países, y seguir una aproximación progresiva para fortalecer la capacidad de respuesta y adaptabilidad de Ecuador frente a los desafíos cibernéticos.

Estos resultados resaltan la importancia de implementar recomendaciones específicas para fortalecer el marco legal de seguridad cibernética en Ecuador, con el propósito de abordar las deficiencias identificadas y proporcionar un marco legal más sólido y adaptable; se enfatizan en promover una evolución digital de las disposiciones legales en Ecuador, tomando como ejemplo el éxito en la evolución de los marcos legales de Colombia, Chile y Argentina para mitigar eficientemente a los ciberdelincuentes.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1.Conclusiones

4.1.1. Conclusión respecto al objetivo general

Analizando las brechas de legalidad en los países investigados en el proyecto, evidencia brechas y áreas de mejora significativas, se señalan carencias importantes, como la falta de claridad en sanciones y medidas preventivas, la necesidad de mejorar la especificidad de las regulaciones, y la insuficiente capacitación de toda la sociedad; además, se destaca la ayuda internacional y fortalecer la infraestructura cibernética.

Estas deficiencias en el marco legal ecuatoriano son de suma importancia, ya que podrían restringir la capacidad del país para prevenir y enfrentar delitos cibernéticos. Por lo tanto, se sugiere adoptar regulaciones más detalladas basadas en las mejores prácticas de otros países, así como mejorar la capacitación de la sociedad. También se enfatiza la necesidad de fortalecer la cooperación interinstitucional y mejorar la infraestructura cibernética, haciendo hincapié en la especificidad y el detalle de las regulaciones para adaptarse a un entorno tecnológico en constante cambio.

Como breve análisis, la investigación identifica y propone acciones para abordar las deficiencias en el marco legal de seguridad cibernética en Ecuador en comparación con Colombia, Chile y Argentina, las recomendaciones apuntan a fortalecer la legislación y mejorar la capacidad del país para afrontar los desafíos cibernéticos.

4.1.2. Conclusiones con respecto a los objetivos específicos

Analizar y comparar las leyes, regulaciones y políticas existentes en el marco jurídico de seguridad cibernética de Ecuador, Colombia, Chile y Argentina,

identificando las principales brechas y diferencias entre ellos. La investigación ha logrado su objetivo específico al analizar y comparar las leyes, regulaciones y políticas vigentes en la legislación de espacios digitales de Ecuador, Colombia, Chile y Argentina, se destaca que Colombia y Chile lideran en regulaciones avanzadas, mientras que Argentina ha experimentado avances notables en su marco jurídico; por otro lado, se señala que el marco legal de seguridad cibernética en Ecuador está en proceso de desarrollo y presenta lagunas y debilidades en comparación con sus contrapartes en la región.

Dentro de las brechas y diferencias identificadas, se enfatiza la falta de claridad en las sanciones y medidas preventivas en Ecuador, la necesidad de mejorar la especificidad y el detalle de las regulaciones, así como la capacitación de la población civil y fuerzas del orden; además, resalta la importancia de promover la ayuda interinstitucional y fortalecer la infraestructura cibernética.

La comparación de los marcos jurídicos ha permitido identificar prácticas y enfoques exitosos en Colombia, Chile y Argentina, sugiriendo que Ecuador podría adoptar estas estrategias para fortalecer su marco jurídico de seguridad cibernética, en síntesis, la investigación proporciona información valiosa para comprender las brechas y oportunidades en el ámbito de la seguridad cibernética, junto con recomendaciones específicas para mejorar la posición legal de Ecuador en este ámbito.

Evaluar la efectividad y aplicabilidad de las disposiciones legales y mecanismos de aplicación relacionados con la seguridad cibernética en Ecuador, a través de un análisis detallado de su implementación y resultados prácticos, contrastándolos con las experiencias de Colombia, Chile y Argentina. El análisis resalta las carencias en la efectividad y aplicabilidad de las disposiciones legales y mecanismos de ciberseguridad en Ecuador en concordancia comparativa de casos como de Colombia, Chile y Argentina, se enfatiza la falta de claridad en las sanciones y medidas preventivas en Ecuador, junto con la necesidad de fortalecer su capacidad de respuesta y adaptabilidad frente a desafíos cibernéticos.

Colombia y Chile lideran con regulaciones más avanzadas, mientras que Argentina ha experimentado un avance notable en su marco jurídico de seguridad cibernética; estas experiencias diversas señalan áreas específicas donde Ecuador podría mejorar su implementación y resultados prácticos en seguridad cibernética.

Como análisis, se propone que Ecuador se inspire en las lecciones aprendidas de Colombia, Chile y Argentina para fortalecer su marco jurídico en esta materia, la optimización de la claridad normativa, la adopción de regulaciones más detalladas y la aplicación de un enfoque progresivo son medidas recomendadas para abordar las deficiencias identificadas en la investigación.

Identificar y proponer recomendaciones específicas para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas y enfoques exitosos utilizados en Colombia, Chile y Argentina. Estas recomendaciones deben abordar las brechas identificadas y estar orientadas a mejorar la prevención, detección, respuesta y sanción de los delitos y amenazas cibernéticas en el país. Dentro de la presente investigación se concluye en primer término, se destaca que el marco legal relacionado con la seguridad cibernética en Ecuador en fase prueba presentando ya vacíos en comparación con los sistemas legales de países vecinos como Colombia, Chile y Argentina, aunque la legislación ecuatoriana demuestra una atención especial a la protección de datos, se menciona la carencia de claridad en las sanciones y medidas preventivas, así como un rezago en la madurez del marco legal.

Las deficiencias identificadas comprenden la falta de claridad en las sanciones y medidas preventivas en Ecuador, en contraposición con Colombia y Chile, que lideran en regulaciones más avanzadas, se enfatiza la importancia de establecer legislación transfronteriza para procesar delitos mediante normativas aplicables en distintos países.

En cuanto a los retos en la implementación, se subraya la carencia de claridad en sanciones y medidas preventivas, la necesidad de mejorar la especificidad y

capacitación en regulaciones, así como la relevancia de fomentar la colaboración interinstitucional y fortalecer la infraestructura cibernética.

Se resaltan los logros en el combata de ciberseguridad en Colombia, Chile y Argentina, destacando la importancia de la ayuda necesaria a nivel internacional en la prevención de ciberdelitos y compartir información y recursos para mejorar la capacidad de respuesta y colaboración ante los riesgos cibernéticos.

Es de vital importancia resaltar implementación y recomendaciones específicas para fortalecer el marco legal de seguridad cibernética en Ecuador, tomando como referencia el éxito en la evolución de los marcos legales de otros países; estas recomendaciones deben abordar las deficiencias identificadas y ofrecer un marco legal más sólido y adaptable, mejorando la efectividad de las disposiciones legales en Ecuador.

4.2.Recomendaciones

En el marco de las recomendaciones, se sugiere que Ecuador considere la posibilidad de unirse al Convenio de Budapest sobre Ciberdelincuencia, un tratado internacional que busca establecer un marco legal armonizado para abordar delitos cibernéticos transfronterizos; al adherirse a este acuerdo, Ecuador podría fortalecer su marco jurídico de seguridad cibernética al adoptar estándares reconocidos internacionalmente y facilitar la cooperación global en la investigación y enjuiciamiento de delitos cibernéticos, proporcionando así una herramienta eficaz contra las amenazas en el ámbito digital.

Como parte del análisis detallado de la implementación y resultados prácticos de las disposiciones legales de seguridad cibernética en Ecuador, sería beneficioso revisar y mejorar el Acuerdo Ministerial N°006-2021 del país, dicha mejora podría fundamentarse en las normativas internacionales y en las lecciones aprendidas de Colombia, Chile y Argentina; al considerar las experiencias de estos países, Ecuador podría fortalecer su marco jurídico y mejorar la eficacia de sus las normativas en

ciberseguridad, además, se sugiere consultar a expertos en la materia y revisar casos prácticos para obtener una perspectiva más completa y aplicada a la realidad, este enfoque permitiría una revisión más integral del marco legal ecuatoriano y su alineación con las mejores prácticas internacionales en seguridad cibernética.

Las sugerencias deben focalizarse en abordar las lagunas identificadas y dirigirse hacia la mejora de la prevención, detección, respuesta y sanción de los delitos y amenazas cibernéticas en la nación; de la misma forma, es crucial considerar la importancia de fortalecer la colaboración entre instituciones y proporcionar capacitación necesaria tecnológica a la población en general.

MATERIALES DE REFERENCIA

1. Referencias Bibliográficas

1. Acurio del Pino, S. (2023). *Delitos Informáticos: Generalidades.* Oas.org: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
2. Arellano, F. (2015). *Método Cualitativo*. Significados: https://www.significados.com/
3. Barrio, F. J., & Sarricouet, M. C. (2016). El derecho penal y la pornografía infantil en el derecho comparado a nivel internacional, de Argentina, Estados Unidos y Europa. *SCRIPT-ed, 13*(2), 171-196. https://doi.org/10.2966/scrip.130216.171
4. Binder, I. (2019). Sociedad civil y agenda de género en la Cumbre Mundial de la Sociedad de la Información: una revisión bibliográfica. *Teknokultura, 16*(1), 127-142. https://doi.org/10.5209/tekn.63277
5. Bouyssou, N., & Polaino Navarrete, M. (2015). *Los delitos de corrupción de menores y pornografía infantil.* Universidad de Sevillo.
6. Bustamante Riaño, J. J. (2021). AVANCES DE LA INFORMÁTICA FORENSE EN COLOMBIA EN LOS ÚLTIMOS CUATRO AÑOS. *Ingeniería Investigación y Desarrollo, 20*(1), 69-78. https://doi.org/10.19053/1900771x.v20.n1.2020.13384
7. Campbell Suárez , N. I., & Avendaño Iturralde, V. H. (12 de 2015). *Penalización a la explotación sexual infantil realizada vía internet en el código orgánico integral penal ecuatoriano.* Repositorio Uniandaes.edu: http://dspace.uniandes.edu.ec/handle/123456789/1052

8. Cardenas Moreno, W. (2015). *Repositorio Universidad Piloto de Colombia.* CIBERDEFENSA Y CIBERSEGURIDAD EN EL SECTOR DEFENSA DE COLOMBIA: http://repository.unipiloto.edu.co/
9. Carrasco, C. (28 de Junio de 2022). *Ley 21459: nueva normativa sobre delitos informáticos en Chile*. Neuronet: https://neuronet.cl/nueva-ley-21459-sobre-delitos-informaticos-en-chile/
10. Cavada Herrera, J. P. (2020). Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera. *Biblioteca del Congreso Nacional de Chile / Asesoria Técnica Parlamentaria*(SUP: 126200), 1. https://doi.org/https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf
11. Cordero Ruiz, D. F. (2021). *La Ciberdelincuencia.* Repositorio Universidad de Alcalá: https://ebuah.uah.es/dspace/bitstream/handle/10017/49563/TFM_Cordero_Ruiz_2021.pdf?isAllowed=y&sequence=1
12. Díaz , F., & Rivera, V. (3 de Enero de 2022). Amenazas, estafas y pornografía infantil: ciberdelitos siguen sin dar tregua en el segundo año de la pandemia. *La Tercera*, págs. 15-18. https://www.latercera.com/nacional/noticia/amenazas-estafas-y-pornografia-infantil-ciberdelitos-siguen-sin-dar-tregua-en-el-segundo-ano-de-la-pandemia/P5KYAB2OKVDPPICJT2UPSQRIPE/
13. Diaz Aparicio, J. D. (2023). *Seguridad Cibernética.* Researchgate.net: https://www.researchgate.net/profile/Juan-Diaz-

Aparicio/publication/369790664_Seguridad_cibernetica/links/642cceab20f25554da0bd3eb/Seguridad-cibernetica.pdf

14. Díaz de León, N. (2018). *Población y Muestra.* Universidad Autonoma del Estado de México: https://core.ac.uk/download/pdf/80531608.pdf
15. Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica, 2*(7), 162-167. https://doi.org/https://www.scielo.org.mx/scielo.php?pid=S2007-50572013000300009&script=sci_arttext
16. El Congreso de la República de Colombia. (23 de Noviembre de 2001). *"POR MEDIO DE LA CUAL SE APRUEBA EL «CONVENIO SOBRE LA CIBERDELINCUENCIA», ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST.".* leyes.senado.gov.co: https://leyes.senado.gov.co/proyectos%20/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2017%20-%202018/PL%20058-17%20Convenio%20Ciberdelincuencia.pdf
17. Elizalde Castañeda , R., Flores Ramírez, H., & Castro Lorzo, E. (2021). Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado. *Ius Comitiãlis, 4*(8). https://doi.org/http://portal.amelica.org/ameli/journal/137/1372935014/
18. Equipo iNBest. (19 de Junio de 2012). *¿Qué es el sabotaje informático?* inbest.cloud: https://www.inbest.cloud/comunidad/que-es-el-sabotaje-informatico
19. Figueroa, A. (28 de Julio de 2022). *Lo que deberías saber sobre la Nueva Ley 21459 de Delitos Informáticos y cómo actualiza a Chile en torno a la*

Ciberseguridad . Diplomados en Ciberseguridad: https://diplomadociberseguridad.com/2022/07/28/nueva-ley-21459-de-delitos-informaticos-chile/

20. Galceran-Vercher, M. (febrero de 2023). *Inteligencia artificial y ciudades: la carrera global hacia la regulación de los algoritmos.* CIDOB | notes internacionals: https://www.cidob.org/es/publicaciones/serie_de_publicacion/notes_internacionals_cidob/286/inteligencia_artificial_y_ciudades_la_carrera_global_hacia_la_regulacion_de_los_algoritmos
21. Gómez-Luna, E., Fernando-Navas, D., Aponte-Mayorga, G., & Betancourt-Buitrago, L. A. (18 de febrero de 2014). *Cómo citar el artículo.* Redalyc.org: https://www.redalyc.org/pdf/496/49630405022.pdf
22. Gumucio Suarez, J. (2021). *Repositorio Universidad de Chile.* GUÍA DE IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ENTIDADES DE INTERMEDIACIÓN FINANCIERA: https://repositorio.uchile.cl/
23. Iglesias, G. (2023). *Bienes protegidos en el delito de pornografía infantil* . sedici.unlp.edu.ar: http://sedici.unlp.edu.ar/bitstream/handle/10915/23871/Documento_completo.pdf?isAllowed=y&sequence=1
24. Lera, C. (1 de Abril de 2021). *Inteligencia artificial, un valor añadido*. Harvard-deusto.com: https://www.harvard-deusto.com/inteligencia-artificial-un-valor-anadido
25. Lifeder. (2022). Método Descriptivo. *Revista Virtual Lifeder, 20,* 14-16.

26. LISA Institute. (2023). *Avances de la Ciberseguridad y el Cibercrimen desde la realidad de Ecuador [Parte 2/4]*. lisainstitute.com: https://www.lisainstitute.com/blogs/blog/avances-ciberseguridad-cibercrimen-ecuador
27. López, J. (22 de Agosto de 2017). *Historia de los navegadores: de Mosaic a Chrome*. Blogthinkbig.com: https://blogthinkbig.com/historia-de-los-navegadores-de-mosaic-a-chrome
28. Ministerio de Seguridad. (14 de Junio de 2016). *Primer protocolo de la historia argentina contra el ciberdelito*. argentina.gob: https://www.argentina.gob.ar/noticias/gprimer-protocolo-de-la-historia-argentina-contra-el-ciberdelito
29. Montagud Rubio, N. (05 de julio de 2020). *Los 12 tipos de técnicas de investigación: características y funciones*. pymOrganization: https://psicologiaymente.com/cultura/tipos-tecnicas-investigacion
30. Morales, F. C. (1 de Marzo de 2021). *Fuente secundaria*. economipedia: https://economipedia.com/
31. Morrou Roldán, A., Mejía Mejía, E., Delgado, K., Santana, G., & Pacheco Lay, G. (2005). *Técnicas e Instrumentos de Investigación.* Edu.mx: http://online.aliat.edu.mx/adistancia/InvCuantitativa/LecturasU6/tecnicas.pdf
32. Mozilla Firefox. (2023). *Historia de los navegadores: épicas luchas de poder que nos trajeron los navegadores modernos*. https://www.mozilla.org/es-ES/firefox/browsers/browser-history/
33. Mr. Houston. (21 de Octubre de 2021). *Los 10 ciberataques más importantes de la historia.* Mr. Houston Tech Solutions: https://mrhouston.net/noticias/los-10-ciberataques-mas-importantes-de-la-historia/

34. Murcia Gutiérrez , H. F. (28 de junio de 2022). *La explotación como elemento del tipo de pornografía infantil: Análisis del artículo 218 del Código Penal a la luz de la jurisprudencia colombiana.* Edu.co: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/fb3fac62-9f0b-412a-b486-e350299dfcae/content
35. Oliva León, R. (5 de julio de 2017). *Ciberdelitos y redes sociales.* algoritmolegal.com: https://www.algoritmolegal.com/entorno-juridico-internet/ciberdelitos-y-redes-sociales/
36. Ortega, C. (14 de mayo de 2021). *5 instrumentos para recopilar información*. QuestionPro: https://www.questionpro.com/blog/es/instrumentos-para-recopilar-informacion/
37. Peña, D. M. (2023). *EL ORIGEN Y LA EVOLUCIÓN DE LOS DELITOS CIBERNETICOS timeline*. Timetoast timelines: https://www.timetoast.com/timelines/delitos-informaticos-bd08b2ec-b416-4fb6-bb11-c094fe5bc8a1
38. Petrosyan, K. (1 de Febrero de 2022). *La Historia Del Correo Electrónico*. EasyDMARC: https://easydmarc.com/blog/es/la-historia-del-correo-electronico/
39. Piovani, J. I., & Krawczyk, N. (2017). Los Estudios Comparativos: algunas notas históricas, epistemológicas y metodológicas. *Educacao e realidade, 42*(3), 821-840. https://doi.org/10.1590/2175-623667609
40. Pozo, L. (2022). *Repositorio del INSTITUTO DE ALTOS ESTUDIOS NACIONALES UNIVERSIDAD DE POSGRADO DEL ESTADO.* “CIBERSEGURIDAD Y MEDIDAS DE PROTECCIÓN DE LA

INFORMACIÓN ADOPTADAS POR EL ESTADO ECUATORIANO": https://repositorio.iaen.edu.ec/

41. RELASEDOR Y FLACSO. (JUNIO de 2017). *Repositorio FLACSO.* Revista Latinoamericana de Estudios de Seguridad: https://repositorio.flacsoandes.edu.ec/
42. Rivas, A. (09 de septiembre de 2022). *Marco metodológico: ¿Cómo redactar y cuál es su estructura?* Normas APA: https://normasapa.in/marco-metodologico/
43. Rodriguez Garcia, E. (10 de Junio de 2018). *El primer hackeo fue hace 184 años, cuando ni siquiera existían los ordenadores*. El Español: https://www.elespanol.com/omicrono/software/20180610/primer-hackeo-hace-anos-siquiera-existian-ordenadores/313969318_0.html
44. Rodriguez, F. (2021). *Respositorio Universidad nacional de La Plata.* La Aplicacion De La Ley Nacional De Proteccion De Datos Personales En Argentina: http://sedici.unlp.edu.ar/bitstream/handle/10915/130245/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y
45. Rojas Ramos, Y. (2022). *Regulación del Ciberdelito en el Marco Legal de la Seguridad de la Información como Medida de Protección Preventiva de Seguridad Cooperativa Nacional e Internacional.* Edu.co: https://repository.unilibre.edu.co/bitstream/handle/10901/25997/Regulacio%CC%81n%20del%20Ciberdelito%20y%20Cooperacion%20internacional.pdf?isAllowed=y&sequence=2

46. Rubio, C., & Terán, D. (2023). *Repositorio Universidad Salesiana del Ecuador.* Posgrados Maestria en Seguridad de la Información: https://dspace.ups.edu.ec/
47. Salesforce Latam. (7 de Septiembre de 2023). *Inteligencia Artificial: ¿Qué es?* Salesforce: https://www.salesforce.com/mx/blog/que-es-la-inteligencia-artificial/
48. Salguero Diaz, A. (Junio de 2019). *Análisis y respuesta de las Fuerzas y Cuerpos de Seguridad del Estado en relación a la pornografía infantil en Internet.* Universidad de las Palmas de Gran canaria: https://accedacris.ulpgc.es/bitstream/10553/24768/4/0740277_00000_0000.pdf
49. Sanjuán Nuñez, L. (Febrero de 2019). *La observación participante.* Uoc.edu: https://openaccess.uoc.edu/bitstream/10609/147145/5/MetodosDeInvestigacionCualitativaEnElAmbitoLaboral_Modulo2_LaObservaconParticipante.pdf
50. Secretaría de Seguridad y Política Criminal. (22 de octubre de 2020). *Plan Federal de Prevención de delitos tecnológicos y ciberdelitos*. argentina.gob: https://www.argentina.gob.ar/seguridad/investigacion/ciberdelito
51. Serna Patiño, A. (2018). *Repositorio Universidad Pontificia Bolivariana, Medellin.* ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTEMATICA DESDE LA ORGANIZACIÓN: https://repository.upb.edu.co/
52. Sintes Marco, B. (26 de Septiembre de 2023). *Historia de la Web: los navegadores*. Mclibre.org: https://www.mclibre.org/consultar/htmlcss/otros/historia-navegadores.html

53. Solís, S. (13 de Abril de 2018). *Hacking y acceso no autorizado - Seguridad informática: Investigación y respuesta*. linkedin.com: https://es.linkedin.com/learning/seguridad-informatica-investigacion-y-respuesta/hacking-y-acceso-no-autorizado
54. Vera, S. (9 de Abril de 2019). *Ecuador culmina la primera fase para la elaboración de la Estrategia Nacional de Ciberseguridad - Gobierno Electrónico de Ecuador*. Gobierno Electrónico de Ecuador: https://www.gobiernoelectronico.gob.ec/ecuador-culmina-la-primera-fase-para-la-elaboracion-de-la-estrategia-nacional-de-ciberseguridad/
55. Wegener, H. (2013). El desarrollo de las amenazas. La nueva realidad económica de la inseguridad cibernetica. En H. Wegener, *LOS RIESGOS ECONÓMICOS DE LA CIBERGUERRA [CAPÍTULO V]* (pág. 191). Universidad de Rioja.
56. Zamora Jiménez, A. (2005). *BIEN JURÍDICO Y CONSENTIMIENTO EN DERECHO PENAL*. cuci.udg: https://cuci.udg.mx/sites/default/files/bien_juridico.pdf

ANEXOS

Entrevistas

Dr. Juan Francisco Pozo Torres

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Tema: Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la Republica del Ecuador, Colombia, Chile y Argentina.

Guía de entrevistas

Entrevistador: Sr. Jimmy Paúl Cóndor Rosas

Ocupación: Estudiante de noveno semestre de la carrera de Derecho

Entrevistado: Juan Francisco Pozo Torres

Ocupación: Abogado y Profesor de Derecho Penal

Estudios: Abogado, Master en Derecho Penal, Especialista en delincuencia económica en la Universidad de Salamanca

Objetivo: Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.:

Pregunta 1: ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

En comparación con Colombia Chile y Argentina la legislación ecuatoriana no da respuesta la a seguridad cibernética a pesar de poseer ciertas normas, las mismas no son especificas o referentes a la ciberseguridad, por lo cual hace falta un cuerpo normativo especifico que rija las mimas, por cual estamos muy atrás de los países mencionados.

Pregunta 2: ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Se requiere una codificación, es decir unificar las normas que se encuentran en diferentes códigos procesales, penales y más para formar un cuerpo normativo que permita el manejo de la legislación.

Pregunta 3: ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Más que similitudes existen diferencias, puesto que los otros países tienen un marco jurídico más desarrollado y codificado, mientras que el de nuestro país tiene normas desperdigadas, que

no permiten una respuesta clara para la regulación de la ciberseguridad, entonces esto si influye en la eficacia, al poseer un instrumento legal más avanzado dan una respuesta más clara.

Pregunta 4: ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

Las falencias especificas están en la evolución constante, en materia de Ciberseguridad se actualiza cada momento, aparecen nuevas formas de entender, nuevas tecnologías que regulan cosas o la interacción social y jurídica de la sociedad. Otra seria que no existen una revisión constante desde términos hasta nuevas tecnologías.

Pregunta 5: ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina,

Por la falta de una respuesta clara, actualizada y codificada que regule la Cibercriminalidad.

Pregunta 6: cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Los principales desafíos es que se debe tomar en serio el tema de seguridad cibernética para llegar a instancias legislativas y permitan una codificación consensuada por los actores que se ven involucrados o afectados por los ataques cibernéticos o de la información de los ficheros de datos , es decir tener la voluntad de crear un cuerpo único y legal que responda a las necesidades.

Pregunta 7: ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

Los aciertos es que existe una legislación que se debería estudiar para poder implementar en el país de una forma que responda a lo que sucede con los temas de ciberdelitos que se dan o son los más frecuentes en el país.

Pregunta 8: ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Es necesario crear un marco jurídico que sea eficaz, que contenga herramientas de cómo se va a realizar la ciberseguridad, no solo la regulación si no la realización y si se habla se seguridad cibernética privada o seguridad cibernética estatal de instituciones públicas. Por lo tanto, se

necesita una norma que cree órganos tecnificados en la matera para dar una respuesta y así poder llenar o acercar la brecha con los países mencionados

Entrevistados: JUAN FRANCISCO PÉREZ TORRES

Capitán Carlos Francisco Osorio

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Tema: Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la Republica del Ecuador, Colombia, Chile y Argentina.

Guía de entrevistas

Entrevistador: Sr. Jimmy Paúl Cóndor Rosas

Ocupación: Estudiante de noveno semestre de la carrera de Derecho

Entrevistado: Carlos Francisco Osorio Vega

Ocupación: Perito en Informática Forense

Estudios: Ingeniero en Informática y Ciencias de la Computación.

Objetivo: Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.:

Pregunta 1: ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Como marco jurídico debería existir la reforma en el COIP, el cual nos permita garantizar la obtención de contenido o evidencia digital, ya que ahora en la actualidad se maneja todo de manera digital, todas las acciones son a través de internet, entonces la reforma debería ir basada en que faculte para poder sustentar la prueba o evidencia digital como una prueba para investigación que sea factible presentar ante la autoridad competente.

Pregunta 2: ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Actualmente los artículos están basados en el tema de levantamiento de indicios en territorio, pero en su tiempo el territorio era todo lo que se levantaba físicamente del lugar de los hechos, ahora en el escenario nos encontramos que tenemos dispositivos de computación, dispositivos móviles de comunicación, y más tipos de equipos tecnológicos, para los cual debería existir una normativa que permita establecer de qué manera se deberían fijar o levantar este tipo de indicios, para poder presentar como prueba.

Pregunta 3: ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Se debería manejar que todo lo que es cibernética es la intervención entre el ser humano y los dispositivos tecnológicos y los sistemas, entonces a través de los sistemas esta implementado todas estas herramientas por las cuales accedemos para poder ser víctimas de cualquier delito, en este caso se debería formalizar el tema de la digitalización, que todo lo que es digital debería mantenerse la prueba digital, no materializarlo de manera física y así perdería du validez.

Pregunta 4: ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

Como se mencionó si es una prueba que se cometió a través de la cibernética y esta digitalizado, las pruebas no se deben materializar, se debería conservarse y garantizar la integridad y originalidad del contenido.

Pregunta 5: ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina,

Se ha reflejado en que los delitos se están cometiendo en las redes sociales, correos electrónicos, entre otras, se ha visto que existen diferentes delitos que concurren a obtener información y estafar a las personas, suplantar identidades y ocasionar daños.

Pregunta 6: cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Los principales desafíos son contar con una tecnología forense adecuada, la cual permita garantizar su obtención del contenido digital para a través de Fiscalía poder poder presentar este tipo de pruebas, así como también garantizar la obtención del contenido digital.

Pregunta 7: ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

Los aciertos es que el equipamiento tecnológico forense que ya existe y es actualizada, ya que a través de ella se implementa metodología, técnicas y capacitación para el aprovechamiento de herramientas.

Pregunta 8: ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Sería un fortalecimiento en la parte jurídica que existan artículos que estén más orientados en la parte digital, puesto que el marco jurídico está más orientado a la parten de la escena de delito,

el lugar de los hechos. Por lo cual en el tema digital hace falta que le marco jurídico se oriente a la evidencia digital y esta sea un prueba válida ante la autoridad competente y evitar el fallido de las pruebas y ocasione la nulidad de la sentencia.

Entrevistados:

Teniente Coronel Xavier Chango

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Tema: Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la Republica del Ecuador, Colombia, Chile y Argentina.

Guía de entrevistas

Entrevistador: Sr. Jimmy Paúl Cóndor Rosas

Ocupación: Estudiante de noveno semestre de la carrera de Derecho

Entrevistado: Teniente Coronel Xavier Chango Llerena

Ocupación: Subdirector Nacional de Investigación Técnico Científico de la Policía Nacional

Estudios: Magíster en Ciencias Penales y Criminalísticas, Abogado, Licenciado en Ciencias Sociales y Políticas.

Objetivo: Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.:

Pregunta 1: ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

La legislación en nuestro país todavía es escasa, débil, tiene que ser actualizada, mientras de lo que conozco en Colombia existe centros cibernéticos de análisis de información, patrullajes cibernéticos que se encuentran reguladas, cosa que no tenemos en nuestro país, si bien nosotros tenemos normativas existentes dentro de lo que es dentro del campo penal como es el COIP, que establece ciertas sanciones para ciertos delitos pero no abarcan la integralidad de los nuevos delitos que están surgiendo tanto con las nuevas tecnologías emergentes o con los nuevos desarrollos que existen.

Pregunta 2: ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Se requiere para reducir la brecha es que se empiece a tomar en consideración lo que son las nuevas tecnologías, que dentro de las políticas públicas se consideren tanto lo que es el uso de las nuevas tecnologías en las actividades que realiza tanto el Estado como la ciudadanía, como en la situación de los nuevos delitos que puedan existir, porque si no se toma en serio los nuevos desarrollos la brecha podría incrementase. Buscar un uso responsable, ético y la sanción en caso de un mal uso de las tecnologías.

Pregunta 3: ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Se consideraría no emitir un concepto para evitar un sesgo.

Pregunta 4: ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

La situación de los delitos modernos, los delitos antiguos tenían fronteras, se sabía cuál era los límites, pero actualmente el cometimiento de delitos dentro de los que es el ámbito digital no respeta fronteras, no hay rostros, no hay nombres, entonces ocurre que los delitos sean transfronterizos y se necesita legislación transfronteriza para poder juzgar el delito a través de normativas de aplicabilidad en diferentes países.

Pregunta 5: ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina,

En el país los delitos cibernéticos si han existido sanciones, también han existido casos que en los cuales no se ha aplicado de manera efectiva ya sea por la legislación no es la adecuada o el personal no tiene el conocimiento, ni las herramientas para una investigación correcta porque por una parte está el conocimiento y por otra la tecnología que le sirve para analizar la información, entonces tenemos vacíos dentro de la normativa, de las herramientas para mejorar el proceso de la judicialización y la sanción y se necesita fortalecer.

Pregunta 6: cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Primero crear un centro cibernético es decir centros de vigilancia y respuestas ante ataques cibernéticos, teniendo en cuenta que Ecuador está entre los principales países que reciben ataques informáticos, que no son conocidos o difundidos, entonces se necesita tener una cultura de seguridad ciudadana y por otra parte se necesita que todas las instituciones que intervengan estén adecuadas. Se realice patrullajes cibernéticos, para la prevención, la investigación y la sanción de ataques cibernéticos.

Pregunta 7: ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

En Colombia tienen diferentes organismos que regenta a diferentes centros cibernéticos para visualizar futuras amenazas, mientras que en el país actual mente no existe los organismos ni el trabajo articulado entre entidades para obtener los resultados adecuados.

Pregunta 8: ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Es importante aprender de las lecciones aprendidas de los países vecinos, para delinear estrategias y aplicarlas al país, si bien los delitos son diferentes hay características que se comparte al estar en la misma región, especialmente en los delitos cibernéticos. Es importante tomar estas buenas prácticas para ver que es necesario implementar y fortalecer con legislación nacional y transnacional. Ademad de la dotación de equipos y la mejora de conocimientos en el personal.

Entrevistados: _____

Dr. Jonathan Ramos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Tema: Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la Republica del Ecuador, Colombia, Chile y Argentina.

Guía de entrevistas

Entrevistador: Sr. Jimmy Paúl Cóndor Rosas

Ocupación: Estudiante de noveno semestre de la carrera de Derecho

Entrevistado: Dr. Jonathan Ramos

Ocupación: Docente de la Universidad Central del Ecuador

Estudios: Master en derecho penal y ciberseguridad

Objetivo: Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.:

Pregunta 1: ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

El marco jurídico de seguridad cibernética en Ecuador se basa en la Constitución de la República, la Ley Orgánica de Protección de Datos Personales y la creación del Comité Nacional de Ciberseguridad, sus principales fortalezas incluyen el reconocimiento constitucional del derecho a la protección de datos personales y la implementación de políticas y estrategias de ciberseguridad, sin embargo, una debilidad es la necesidad de mayor difusión y conocimiento de los derechos y políticas públicas relacionadas con la ciberseguridad entre la población, en comparación con Colombia, Chile y Argentina, Ecuador ha demostrado un notable compromiso con la ciberseguridad, pero aún enfrenta retos en la difusión de derechos y políticas públicas.

Pregunta 2: ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

Para mejorar y cerrar las brechas en seguridad cibernética, la legislación ecuatoriana podría enfocarse en la difusión de derechos y políticas públicas, la implementación de medidas de protección de datos personales y la creación de una entidad reguladora, tomando como referencia la Ley de Protección de Datos de Ecuador y las estrategias de otros países de la región.

Pregunta 3: ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Las principales similitudes en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina son el reconocimiento constitucional del derecho a la protección de datos personales y la implementación de políticas y estrategias de ciberseguridad. Las

diferencias incluyen la creación de entidades reguladoras y la difusión de derechos y políticas públicas. Estas discrepancias pueden influir en la eficacia de los marcos legales respectivos, ya que una mayor difusión y conocimiento de los derechos y políticas públicas relacionadas con la ciberseguridad puede mejorar la protección de los ciudadanos

Pregunta 4: ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

Se han identificado falencias en el marco jurídico de seguridad cibernética de los países analizados, como la necesidad de difusión de derechos y políticas públicas, la implementación de medidas de protección de datos personales y la creación de entidades reguladoras, estas brechas pueden tener implicaciones en la seguridad cibernética regional de Latinoamérica, ya que una mayor difusión y conocimiento de los derechos y políticas públicas relacionadas con la ciberseguridad puede mejorar la protección de los ciudadanos y la estabilidad en el ciberespacio

Pregunta 5: ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina,

Ecuador ha demostrado un notable compromiso con la ciberseguridad, ejemplificado en la implementación de políticas y estrategias, la creación del Comité Nacional de Ciberseguridad y el reconocimiento constitucional del derecho a la protección de datos personales; sin embargo, aún enfrenta retos en la difusión de derechos y políticas públicas relacionadas con la ciberseguridad, en comparación con Colombia, Chile y Argentina, Ecuador ha realizado esfuerzos significativos, pero aún necesita mayor difusión y conocimiento de los derechos y políticas públicas para mejorar su efectividad en seguridad cibernética

Pregunta 6: cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Los principales desafíos en la implementación de las disposiciones legales de seguridad cibernética en Ecuador incluyen la difusión de derechos y políticas públicas, la capacitación y formación de las fuerzas de seguridad y la población en general, la cooperación interinstitucional, el fortalecimiento de la infraestructura cibernética y la promoción de la ciberseguridad. Estos desafíos son comunes en toda Latinoamérica y pueden tener implicaciones en la protección de datos personales y la estabilidad del ciberespacio. Ecuador ha demostrado un

compromiso significativo con la ciberseguridad, pero aún necesita mejorar la difusión y conocimiento de los derechos y políticas públicas para mejorar su efectividad en seguridad cibernética.

Pregunta 7: ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

Colombia: Fortalecimiento de colaboración público-privada en ciberseguridad. Chile: Implementación de estrategias nacionales de ciberseguridad. Argentina: Desarrollo de normativas específicas y concientización. Lecciones para Ecuador: Fomentar cooperación público-privada, establecer estrategias nacionales y promover regulaciones claras con enfoque educativo.

Pregunta 8: ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Los principales desafíos en la implementación de las disposiciones legales de seguridad cibernética en Ecuador incluyen la difusión de derechos y políticas públicas, la capacitación y formación de las fuerzas de seguridad y la población en general, la cooperación interinstitucional, el fortalecimiento de la infraestructura cibernética y la promoción de la ciberseguridad. Estos desafíos son comunes en toda Latinoamérica y pueden tener implicaciones en la protección de datos personales y la estabilidad del ciberespacio. Ecuador ha demostrado un compromiso significativo con la ciberseguridad, pero aún necesita mejorar la difusión y conocimiento de los derechos y políticas públicas para mejorar su efectividad en seguridad cibernética.

Entrevistados:

Dr. José Heriberto Garcia Peña

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Tema: Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la Republica del Ecuador, Colombia, Chile y Argentina.

Guía de entrevistas

Entrevistador: Sr. Jimmy Paúl Cóndor Rosas

Ocupación: Estudiante de noveno semestre de la carrera de Derecho

Entrevistado: Dr. José Heriberto García Peña

Ocupación: Docente en Tecnológico de Monterrey

Estudios: Especialista en Inteligencia Artificial

Objetivo: Evaluar el marco jurídico actual de seguridad cibernética en Ecuador, identificando sus brechas y áreas de mejora en comparación con los sistemas jurídicos de Colombia, Chile y Argentina.:

Pregunta 1: ¿Cómo describiría el marco jurídico de seguridad cibernética en Ecuador y cuáles considera que son sus principales fortalezas y debilidades en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

En Ecuador, se encuentra en proceso de desarrollo el marco jurídico de seguridad cibernética, siendo notables la Ley Orgánica de Telecomunicaciones y la Ley de Datos Personales. Entre sus puntos fuertes se destaca la atención especial a la protección de datos, aunque presenta carencias en la claridad de las sanciones y medidas preventivas. Al compararse con Colombia, Chile y Argentina, Ecuador muestra un rezago en cuanto a la madurez y especificidad de su marco legal en ciberseguridad. Colombia y Chile lideran con regulaciones avanzadas, mientras que Argentina ha avanzado significativamente en su marco jurídico.

Pregunta 2: ¿Qué requiere la legislación ecuatoriana para mejorar y cerrar las brechas o falencias identificadas en tema de seguridad cibernética, en comparación con los sistemas jurídicos de Colombia, Chile y Argentina?

La legislación ecuatoriana en seguridad cibernética necesita mejoras específicas para cerrar las brechas identificadas. Se requiere una mayor claridad en las sanciones y medidas preventivas, así como la incorporación de disposiciones más detalladas sobre ciberseguridad. Se podría considerar la implementación de normativas más específicas que aborden las amenazas emergentes y tecnologías actuales. Observar las experiencias de Colombia y Chile, con regulaciones avanzadas, y la evolución de Argentina en su marco jurídico, podría proporcionar insights para fortalecer y actualizar la legislación en Ecuador.

Pregunta 3: ¿Cuáles son las principales similitudes y diferencias en las leyes y regulaciones de seguridad cibernética entre Ecuador, Colombia, Chile y Argentina, y cómo cree que estas discrepancias pueden influir en la eficacia de los marcos legales respectivos?

Las normativas de seguridad cibernética en Ecuador, Colombia, Chile y Argentina comparten enfoques comunes en la protección de datos y la gestión de incidentes, aunque presentan diferencias notables en cuanto al nivel de detalle y claridad. Es evidente que Ecuador necesita mejoras específicas, especialmente en lo referente a sanciones y medidas preventivas, mientras

que Colombia y Chile sobresalen por contar con regulaciones avanzadas. Argentina ha experimentado avances significativos en su marco legal. Estas disparidades pueden impactar la

eficacia de los marcos legales respectivos, limitando la capacidad de respuesta de Ecuador, fortaleciendo la capacidad de anticipación en Colombia y Chile, y resaltando la adaptabilidad en la legislación argentina.

Pregunta 4: ¿Qué falencias específicas se han identificado en el marco jurídico de seguridad cibernética de los países analizados, y cuáles son las posibles implicaciones de estas brechas en la seguridad cibernética regional Latino América?

Las falencias identificadas incluyen la falta de claridad en sanciones y medidas preventivas en Ecuador, mientras Colombia y Chile lideran en regulaciones avanzadas. Estas brechas podrían limitar la capacidad de respuesta ante amenazas emergentes y dificultar la colaboración regional, afectando la seguridad cibernética en América Latina al obstaculizar la armonización de esfuerzos y la capacidad de abordar desafíos de manera coordinada.

Pregunta 5: ¿Cómo se ha reflejado la efectividad de las disposiciones legales de seguridad cibernética en Ecuador, en comparación con Colombia, Chile y Argentina,

La efectividad de las disposiciones legales de seguridad cibernética en Ecuador se ha visto afectada por la falta de claridad en sanciones y medidas preventivas. En comparación con Colombia y Chile, que cuentan con regulaciones más avanzadas, y con Argentina, que ha avanzado significativamente en su marco jurídico, Ecuador muestra ciertas limitaciones. La falta de especificidad en las leyes puede dificultar la aplicación efectiva y la capacidad de respuesta frente a amenazas cibernéticas. La comparación con estos países destaca la necesidad de fortalecer y actualizar la legislación ecuatoriana para mejorar su eficacia en la protección contra riesgos cibernéticos.

Pregunta 6: cuáles son los principales desafíos identificados en su implementación de las disposiciones legales de seguridad cibernética en Ecuador?

Los desafíos principales en la implementación de las disposiciones legales de seguridad cibernética en Ecuador se centran en la falta de claridad en sanciones y medidas preventivas. Esta carencia puede complicar la aplicación efectiva de las leyes y la capacidad de respuesta

frente a amenazas cibernéticas. Asimismo, la necesidad de mejorar la especificidad y detallar las regulaciones representa un reto para asegurar una cobertura completa y actualizada en un entorno tecnológico en constante cambio. Estos desafíos subrayan la importancia de fortalecer y modernizar la legislación para enfrentar de manera eficiente los riesgos cibernéticos en Ecuador.

Pregunta 7: ¿Cuáles son los aciertos de la aplicación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina que podrían servir para mejorar la efectividad de las disposiciones legales en Ecuador?

Los logros en la implementación de mecanismos de seguridad cibernética en Colombia, Chile y Argentina, evidenciados por la adopción de regulaciones avanzadas, enfoque progresivo y claridad en detalles, proporcionan valiosas lecciones para mejorar la efectividad de las disposiciones legales en Ecuador. Tomar como ejemplo el éxito en la evolución de los marcos legales de estos países podría fortalecer la capacidad de respuesta y adaptabilidad de Ecuador frente a los desafíos cibernéticos.

Pregunta 8: ¿Cuáles sería su recomendación para fortalecer el marco jurídico de seguridad cibernética en Ecuador, considerando las mejores prácticas observadas en Colombia, Chile y Argentina? ¿Cómo cree que estas recomendaciones pueden abordar las brechas identificadas en el contexto ecuatoriano?

Para fortalecer el marco jurídico de seguridad cibernética en Ecuador, se propone mejorar la claridad normativa, adoptar regulaciones más detalladas inspiradas en las prácticas de Colombia y Chile, y seguir una aproximación progresiva, tomando como ejemplo la evolución exitosa en Argentina. Estas recomendaciones buscan abordar las deficiencias identificadas al proporcionar un marco legal más robusto y adaptable, con el objetivo de mejorar la capacidad de Ecuador para enfrentar eficazmente los desafíos de seguridad cibernética.

Entrevistados: Dr. José Heriberto García Peña