Universidad Tecnológica ECOTEC

Título del trabajo:

“Modificación normativa al Código Orgánico Integral Penal para disminuir la desproporcionalidad en las penas de los delitos hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador”

Línea de investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Proyecto de investigación

Nombre de la carrera:

Derecho y Gobernabilidad

Título a obtener:

Abogado

Autor (a):

Francisco Samuel Granizo Sánchez

Tutor (a):

Ab Fabián Orellana Mgrt.

Guayaquil – Ecuador

2023 - 2024

DEDICATORIA

Este trabajo de investigación va dedicado en primer lugar a mis padres, Segundo Francisco Granizo Villacrés y Maura Alexandra Sánchez Moscoso, quienes fueron los únicos que nunca me dejaron solo y me ayudaron de manera económica, motivacional, espiritual para no darme por vencido en el medio del camino, con tolerancia y paciencia para continuar en este largo camino y llegar, por fin, hasta el día de hoy con excito.

A mi hermana menor, Daniela, quien sigue esta hermosa carrera con gran sacrificio día a día para llegar hasta donde estoy ahora, luchando por nunca rendirse pese a las adversidades de la vida de ser mama primeriza.

A mi sobrina Lía Daniela, que llego a mi vida para ensenarme a ser por primera vez tío, por permitirme sentir el amor de verdad y estar presente en mi vida diaria para luchar por demostrarle que tiene un apoyo fundamental emocional y siempre podrá contar con su tío favorito.

A mis abuelitos, Segundo Granizo y Carmen Amelia Villacrés, José Medardo y Maura Mosco, quienes, sin duda alguna, son ese complemento que Dios me puso en mi vida, por ser un gran aporte y apoyo incondicional a lo largo de mi vida, por siempre ser bondadosos y tener ese amor hacia mí.

A mis tíos, primos y a resto de mi familia, que me vieron crecer y tuve la dicha de aprender de cada uno de ellos, siempre pensando en mi bienestar para llegar a ser un excelente profesional.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a Dios por siempre guiarme y nunca dejar que me rinda por lo difícil que ha sido durante todos estos años llegar hasta el final, por siempre bendecirme y cuidar cada paso de mi familia, por que, sin duda, nunca pude haberlo hecho sin su ayuda.

Agradezco a mi familia, por ser definitivamente el pilar de mi vida, mis padres, mi hermana, mi sobrina, mis abuelos, dándome ese apoyo emocional y motivacional para cada paso que doy en la toma de decisiones.

Además, quiero agradecer a mis amigos, Christian Ruiz, Oswaldo Ruiz, por ser capaces de demostrar estar cuando más se los necesita, a Jimmy Abad, por nunca rendirse por más difícil que sea el camino, siempre sale adelante y al resto del grupo de mis amigos por ser incondicionales conmigo.

A Karina Ruiz, quien durante varios años hemos compartido momentos inolvidables, creando una amistad sincera, agradezco profundamente a Allyson Touzard, mi enamorada, por haber formado parte de mi vida durante la carrera universitaria y siempre creer en que si podía lograrlo, apoyo en los momentos más difíciles, este logro es también para ella.

Agradezco a la Universidad Tecnológica Ecotec, docentes, directivos, al Decano Mgrt. Andrés Madero Poveda y entre ellos al que considero el mejor tutor, docente, Mgrt. David Vergara, quien me ayudó como estudiante a lo largo de mi carrera y aprender lo que hoy pongo en práctica en este proyecto.

ANEXO N°16

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

Samborondón, 05 de diciembre del 2023.

Magíster
Ab. Andrés Madero Mgtr.
Decano(a) de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **"Modificación normativa al Código Orgánico Integral Penal para disminuir la desproporcionalidad en las penas de los delitos hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador"** según su modalidad PROYECTO DE INVESTIGACIÓN, fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: FRANCISCO SAMUEL GRANIZO SÁNCHEZ, para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

FABIAN ERNESTO ORELLANA BATALLAS

Mgtr/ PhD.. Fabian Orellana Batallas

Tutor(a)

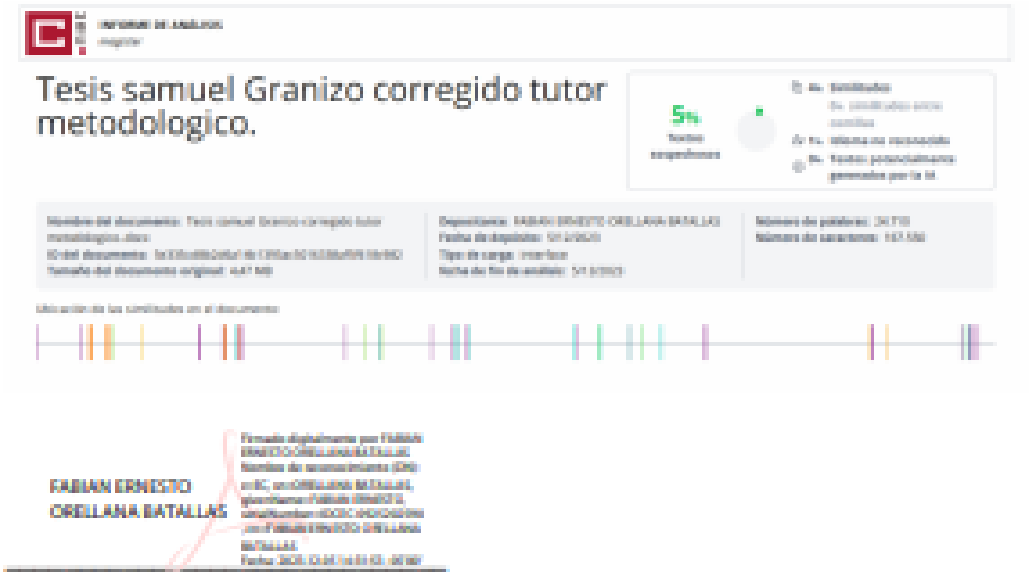
ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Fabian Orellana Batallas Mgtr., tutor del trabajo de titulación **"Modificación normativa al Código Orgánico Integral Penal para disminuir la desproporcionalidad en las penas de los delitos hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador"** elaborado por FRANCISCO SAMUEL GRANIZO SÁNCHEZ, con mi respectiva supervisión como requerimiento parcial para la obtención del título de ABOGADO.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias _ 5% _ mismo que se puede verificar en el siguiente link: https://app.compilatio.net/v5/login?nextUrl=%2Freport%2F3563dbaebe81aef878611da11d4c63ea0fbb508f%2Fsummary.

Adicional se adjunta print de pantalla de dicho resultado.



FABIAN ERNESTO ORELLANA BATALLAS

AB. FABIAN ORELLANA BATALLAS Mgrt.

RESUMEN

La investigación destaca la creciente amenaza de los delitos informáticos, especialmente el hacking, a nivel mundial y en Ecuador. Se enfatiza la importancia de establecer normativas para garantizar la seguridad y concientizar a los usuarios sobre los riesgos. La legislación ecuatoriana sobre delitos informáticos se centra en la Ley Orgánica de Telecomunicaciones, abordando aspectos como el acceso no autorizado, la intercepción de datos, el daño a sistemas y el fraude informático. El problema central identificado es la falta de proporcionalidad en las penas para los delitos de hacking y acceso no consentido en Ecuador. Se destaca la limitada doctrina legal sobre delitos informáticos y se plantea la necesidad de reformas para abordar las modalidades de estos delitos. La pregunta problema indaga sobre las razones detrás de la inaplicabilidad del principio de proporcionalidad y su impacto en el sistema legal y la seguridad de las redes en Ecuador. El periodo y lugar de la investigación se especifican en el Consejo de la Judicatura en Guayaquil, durante octubre y noviembre de 2023, con una población de estudio de 5 abogados sin cálculo de muestra debido a la cantidad limitada de participantes. La elección se justifica por la viabilidad de abordar directamente a toda la población de estudio debido a su tamaño reducido. Las entrevistas subrayan la complejidad y urgencia de abordar los delitos informáticos en Ecuador, desde la definición legal hasta la implementación de sanciones proporcionales y la mejora de la capacidad de investigación. La colaboración entre actores públicos y privados, la actualización constante de la legislación y la conciencia ciudadana son fundamentales en esta lucha en evolución contra la ciberdelincuencia.

Palabras claves: Delitos informáticos, Hacking, Legislación, Proporcionalidad en penas, Ciberseguridad

ABSTRACT

The research highlights the growing threat of cybercrimes, especially hacking, globally and in Ecuador. The importance of establishing regulations to ensure security and raise awareness among users about the risks is emphasized. Ecuadorian legislation on cybercrimes focuses on the Organic Telecommunications Law, addressing aspects such as unauthorized access, data interception, system damage, and computer fraud. The identified central problem is the lack of proportionality in penalties for hacking and unauthorized access crimes in Ecuador. The limited legal doctrine on cybercrimes is underscored, and the need for reforms to address the modalities of these crimes is raised. The research question investigates the reasons behind the inapplicability of the principle of proportionality and its impact on the legal system and network security in Ecuador. The period and location of the research are specified at the Judiciary Council in Guayaquil, during October and November 2023, with a study population of 5 lawyers without a sample calculation due to the limited number of participants. The choice is justified by the feasibility of directly addressing the entire study population due to its small size. The interviews underscore the complexity and urgency of addressing cybercrimes in Ecuador, from legal definition to the implementation of proportional sanctions and the improvement of investigative capabilities. Collaboration between public and private stakeholders, continuous updating of legislation, and public awareness are crucial in this evolving fight against cybercrime.

Keywords: Cybercrimes, Hacking, Legislation, Proportionality in penalties, Cybersecurity

.

ÍNDICE DE CONTENIDO

ÌNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La palabra “hacking” es un anglicismo que tomó su acepción del verbo “to hack” que significa “hachar” que se refiere a la acción ejercida con fuerza sobre la forma no autorizada a sistemas informáticos, programas, base de datos, computadores personales, móviles, etc. El “hacking” se puede definir como el acto de hackeo, irrupción no autorizada en sistemas informáticos o electrónicos que no pertenecen al sujeto que la ejecuta. Delito que tiene como resultado la prueba material de una evidencia de haber efectivamente realizado la intervención a los sistemas informáticos.

El mundo entero y Ecuador no es la excepción, ha crecido enormemente el campo de la tecnología y con ello los peligros inminentes de que los sistemas informáticos sean violentados para el cometimiento de delitos; es por ello que se considera necesario abordar este tema y contribuir para fortalecer con normativas que den mayor seguridad y fundamentalmente concientizar a los diferentes usuarios del peligro que día a día se corre.

En Ecuador, la legislación relacionada con delitos informáticos se encuentra principalmente en la Ley Orgánica de Telecomunicaciones, que fue reformada en 2013 para abordar temas de seguridad en el ámbito de las tecnologías de la información y las comunicaciones. Algunos de los puntos más relevantes incluyen:

Acceso no consentido: La ley prohíbe el acceso no autorizado a sistemas informáticos, redes, bases de datos o cualquier otro recurso informático.

Intercepción de datos: También se prohíbe la interceptación de datos sin autorización, lo que incluye el acceso a información privada o confidencial sin el debido consentimiento.

Daño a sistemas: Cualquier intento de dañar, alterar o destruir datos o sistemas informáticos sin permiso se considera un delito.

Robo de información: La apropiación indebida de información o la obtención ilegal de datos personales o comerciales también está penada por la ley.

Fraude informático: El uso de técnicas de hacking para cometer fraudes o estafas en línea se encuentra prohibido y es sancionado legalmente.

Las sanciones por delitos informáticos en Ecuador pueden variar, dependiendo de la gravedad del delito y otros factores, pero pueden incluir multas y penas de prisión. Es importante tener en cuenta que la seguridad informática y el respeto a la privacidad en línea son responsabilidades compartidas entre usuarios, empresas y el gobierno. Utilizar software y hardware actualizado, contraseñas seguras, y estar consciente de prácticas seguras en línea son formas de protegerse contra el acceso no consentido a sistemas informáticos.

En Ecuador, el marco legal relacionado con delitos informáticos, incluido el hacking y el acceso no autorizado a sistemas informáticos de telecomunicaciones, se encuentra principalmente en la Ley Orgánica de Telecomunicaciones, Ley Orgánica de Comunicación y otras leyes que abordan temas relacionados con la seguridad informática y la privacidad de datos.

El hacking no está contemplado como delito específico en la legislación ecuatoriana, sin embargo, los cuatro tipos penales que existen: revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial y ataque a la integridad de sistemas informáticos, así como los que se ejecutan contra el patrimonio público como: delito contra la información pública y acceso no consentido a un sistema informático de telecomunicaciones; constituyen en sí una modalidad de hacking; de estos delitos mencionados se analizó el ataque cibernético como el más ajustado a la conducta del hacker.

Es importante este trabajo de investigación porque el hacking es una actividad que ha ido en aumento en los últimos años, y con el avance de la tecnología, se ha convertido en una amenaza cada vez más grande para la seguridad informática. En muchos casos, los hackers realizan estas actividades con fines maliciosos, como robar información personal o financiera, o incluso para causar daño a sistemas y redes.

La pertinencia sobre este tema se radica justamente en el tipo penal del acceso no consentido a un sistema informático, en muchos casos, los delitos

informáticos pueden tener consecuencias graves y duraderas para las víctimas, como la pérdida de datos o la exposición de información personal y es La pena impuesta por un delito informático debe ser proporcional a la gravedad del delito y a las consecuencias que este haya tenido para las víctimas y la sociedad en general, asimismo, se deben considerar las circunstancias del caso, como la intencionalidad del delincuente y su historial delictivo" (COIP, 2014).

El panorama descrito en el contexto de Ecuador refleja la creciente preocupación global por los delitos informáticos y cómo estos afectan la seguridad y privacidad de la información en la era digital. La evolución constante de la tecnología ha creado un terreno fértil para la proliferación de actividades delictivas en línea, como el hacking y el acceso no autorizado a sistemas informáticos.

Planteamiento del problema

Es fundamental destacar que, en el presente contexto, la doctrina referente a los delitos informáticos en el país es limitada. Sin embargo, resulta alentador observar cómo diversos programas académicos en universidades están tomando la iniciativa de abordar estos aspectos, contribuyendo a la generación de conocimiento en el campo del derecho penal informático. Un desafío primordial que enfrenta el sistema judicial ecuatoriano en relación con los delitos informáticos radica en la búsqueda de la proporcionalidad de las penas. No obstante, la falta de conocimiento y comprensión acerca de estos delitos puede resultar en la imposición de penas menos rigurosas en comparación con delitos convencionales.

En este contexto de investigación, surge la necesidad imperante de enfocarse en la reforma e implementación de un tipo penal específico que aborde las modalidades y acciones de desarrollo y comercialización, siendo el delito de acceso no consentido uno de los ejemplos abordados previamente.

Respecto a esta situación, el autor Ramos señala: "El delito de interceptación en su último numeral contempla tal situación, aunque de forma más concisa que el de ataque. Además, una situación similar de atipicidad se presenta en los casos de venta de programas destinados a la comisión de delitos de transferencia

electrónica de activos patrimoniales, acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, y violaciones de información pública legalmente reservada. Estas situaciones tampoco han sido previstas en su totalidad en su contenido. Por consiguiente, se vuelve esencial tipificar un nuevo tipo penal bajo la denominación de 'abuso de dispositivos'." (Ramos, 2020, p. 103).

Además, en el transcurso de esta investigación, los resultados obtenidos resaltarán la naturaleza global de Internet y los desafíos inherentes para rastrear a los infractores, lo cual puede dificultar la aplicación de la ley y la imposición de sanciones adecuadas. Este escenario plantea un reto para la justicia en cuanto a cómo balancear la necesidad de sancionar a los delincuentes informáticos con la garantía de penas proporcionales y justas.

Para llevar a cabo esta investigación, se empleará una metodología basada en elementos cualitativos, descriptivos y explicativos. A través de la recopilación de información, material documental, literatura doctrinal y jurídica, se abordará en profundidad el tema en cuestión, abarcando conductas que en su mayoría no están contempladas en el Código Orgánico Integral Penal en relación con el acceso no consentido a sistemas informáticos.

En el contexto actual, la evolución tecnológica ha dado lugar a un incremento alarmante de los delitos informáticos, generando desafíos tanto a nivel nacional como global en cuanto a la legislación y sanciones adecuadas para abordar esta problemática. En el caso específico de Ecuador, a pesar de la creciente importancia de los delitos informáticos, la doctrina legal referente a esta materia se presenta como un terreno limitado y poco explorado.

Resulta alentador observar que diversos programas académicos en universidades ecuatorianas están comenzando a abordar aspectos relacionados con los delitos informáticos, contribuyendo a la generación de conocimiento en el campo del derecho penal informático. No obstante, este avance académico contrasta con un desafío primordial que enfrenta el sistema judicial del país en relación con los delitos informáticos: la búsqueda de la proporcionalidad de las penas. La falta de comprensión y conocimiento profundo sobre la naturaleza y

gravedad de estos delitos puede conllevar a la imposición de penas menos rigurosas en comparación con los delitos convencionales.

La urgente necesidad de abordar esta problemática se manifiesta en la carencia de un tipo penal específico que enfoque las modalidades y acciones de desarrollo y comercialización en delitos informáticos, destacándose el caso del acceso no consentido a sistemas como ejemplo paradigmático. A pesar de que existen disposiciones legales que tratan ciertos aspectos de estos delitos, como la interceptación ilegal de datos, la transferencia electrónica de activos patrimoniales y el ataque a la integridad de sistemas informáticos, se evidencia la ausencia de una normativa integral que aborde de manera adecuada y exhaustiva el espectro de conductas informáticas ilícitas.

Un análisis detenido de esta problemática se refleja en la reflexión del autor Ramos, quien destaca las deficiencias en la tipificación de ciertas conductas relacionadas con la venta de programas y dispositivos destinados a la comisión de delitos informáticos. Este vacío normativo plantea la necesidad imperante de reformar el sistema legal ecuatoriano, incorporando un nuevo tipo penal bajo la denominación de "abuso de dispositivos", que abarque estas modalidades y acciones, así como las vulnerabilidades que explotan los delincuentes informáticos.

Asimismo, la naturaleza global de Internet y la inherente dificultad de rastrear a los infractores representan desafíos adicionales para la aplicación efectiva de la ley y la imposición de sanciones proporcionales. La tecnología de rápida evolución y la capacidad de cometer delitos informáticos desde ubicaciones remotas plantean un dilema para la justicia, que debe equilibrar la necesidad de castigar a los delincuentes con la garantía de penas justas y proporcionales.

En vista de estas circunstancias, esta investigación tiene como objetivo principal explorar y analizar en profundidad la problemática de los delitos informáticos en Ecuador, enfocándose en la ausencia de una tipificación integral y la necesidad de reforma legislativa. Se empleará una metodología que involucra elementos cualitativos, descriptivos y explicativos, a través de la recopilación y análisis de información, material documental, literatura doctrinal y jurídica. Esta

investigación se propone contribuir al desarrollo de una legislación más sólida y efectiva para enfrentar los desafíos emergentes en el ámbito de los delitos informáticos en Ecuador.

Pregunta problema

¿Cómo puede lograrse una modificación normativa efectiva en el Código Orgánico Integral Penal para reducir la desproporcionalidad en las penas de los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador?

Objetivos

Objetivo general

Promover una modificación normativa al Código Orgánico Integral Penal en Ecuador que permita disminuir la desproporcionalidad en las penas asociadas a los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones

Objetivos específicos

- Examinar la legislación vigente en Ecuador relacionada con los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones, así como las penas establecidas en dicha legislación.
- Identificar los criterios utilizados por el sistema legal ecuatoriano para determinar las penas en casos de delitos informáticos, enfocándose en la ausencia o limitada aplicación del principio de proporcionalidad.
- Evaluar las posibles razones detrás de la aplicabilidad del principio de proporcionalidad en las penas impuestas en los delitos de hacking y acceso no autorizado a sistemas informáticos, considerando factores como la falta de precedentes, la falta de conocimiento técnico-jurídico y la rapidez de evolución tecnológica.

Justificación

La inaplicabilidad del principio de proporcionalidad en las penas de los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador es un problema que requiere una atención urgente. La ciberdelincuencia es un fenómeno en constante crecimiento en el mundo digital, y Ecuador no es una excepción. A medida que la sociedad se vuelve cada vez más dependiente de la tecnología, la seguridad informática se convierte en un tema crucial para proteger la integridad de los sistemas y la privacidad de los usuarios.

Abordar esta situación es fundamental debido a varias razones:

Desincentivar la comisión de delitos informáticos: La falta de penas proporcionales puede generar un ambiente propicio para que los hackers y ciberdelincuentes actúen sin temor a enfrentar consecuencias significativas. Al establecer sanciones adecuadas y disuasorias, se busca desalentar la realización de estos delitos y proteger a los ciudadanos y empresas de posibles ataques.

Fomentar la confianza en el entorno digital: Una legislación eficaz en materia de ciberseguridad y penas justas ayuda a generar confianza en el uso de tecnologías de la información y las comunicaciones. Si los ciudadanos y las empresas perciben que existe un marco legal robusto que protege sus datos y sistemas, se sentirán más seguros al utilizar servicios en línea y participar en la economía digital.

Mejorar la efectividad de la justicia: La inaplicabilidad del principio de proporcionalidad en las penas puede llevar a una percepción de impunidad frente a los delitos informáticos. Al establecer sanciones proporcionales y adecuadas, se contribuye a una administración de justicia más efectiva y justa, lo que aumenta la confianza en el sistema legal.

Fortalecer la ciberseguridad nacional: Una legislación actualizada y sanciones proporcionales permite a las autoridades y fuerzas de seguridad combatir más

eficientemente los delitos informáticos y proteger la infraestructura crítica del país frente a posibles amenazas cibernéticas.

Beneficios de los resultados propuestos:

Mayor protección para individuos y empresas: Con penas proporcionales, los ciudadanos y las empresas obtendrían una mayor protección frente a posibles ataques informáticos y robos de datos. Esto contribuiría a salvaguardar su privacidad y evitar posibles daños financieros o reputacionales.

Reducción de la ciberdelincuencia: Una legislación efectiva y penas justas actuarían como un elemento disuasorio para los delincuentes cibernéticos, lo que podría reducir la incidencia de delitos informáticos y mejorar la seguridad digital en el país.

Mayor confianza en el uso de la tecnología: Una regulación clara y sanciones proporcionales brindarían a los ciudadanos y empresas una sensación de seguridad al utilizar servicios en línea y participar en actividades digitales, lo que fomentaría el desarrollo del comercio electrónico y la economía digital.

Impulso al desarrollo tecnológico y la innovación: Un marco legal sólido y proporcional podría atraer inversiones y estimular el crecimiento del sector tecnológico en Ecuador, ya que las empresas verían un entorno más seguro y favorable para desarrollar nuevas soluciones digitales.

Abordar la inaplicabilidad del principio de proporcionalidad en las penas de los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador es esencial para proteger a los ciudadanos y empresas, fortalecer la ciberseguridad nacional, generar confianza en el entorno digital y promover un desarrollo tecnológico sostenible. Las mejoras concretas en términos de seguridad, confianza y crecimiento económico que se lograrían como resultado de una legislación más efectiva en esta área serían de gran beneficio para el país y sus ciudadanos.

Idea a defender

Se argumenta que la falta de penas proporcionales puede generar un ambiente propicio para que los hackers y ciberdelincuentes actúen sin temor a enfrentar consecuencias significativas. Al establecer sanciones adecuadas y disuasorias, se busca desalentar la realización de estos delitos y proteger a los ciudadanos y empresas de posibles ataques.

CAPITULO I

Marco Teórico

Delito de acceso no consentido

El delito de acceso no consentido, también conocido como intrusión informática o hacking no autorizado, se refiere a la acción ilegal de acceder a sistemas informáticos, redes o dispositivos electrónicos sin el permiso o consentimiento del propietario o administrador de dichos sistemas. Este acto constituye una violación de la privacidad y la seguridad de la información, y puede tener graves implicaciones legales (Atienza & Fernández, 2020).

En este tipo de delito, un individuo, comúnmente conocido como hacker, utiliza diversas técnicas y herramientas para eludir medidas de seguridad y obtener acceso a sistemas informáticos con fines fraudulentos, maliciosos o de robo de datos. Estos fines pueden incluir la obtención de información confidencial, la alteración o destrucción de datos, el robo de identidades o el sabotaje de sistemas.

El delito de acceso no consentido es considerado ilegal en la mayoría de las jurisdicciones y puede conllevar sanciones legales significativas, como multas, penas de prisión u otras medidas punitivas, dependiendo de la gravedad y el alcance del acceso no autorizado. Además, este tipo de actividades puede tener repercusiones graves para las víctimas, desde la pérdida de datos y la vulneración de la privacidad hasta daños financieros y reputacionales. Por lo tanto, es esencial tomar medidas adecuadas para proteger la seguridad cibernética y prevenir este tipo de delitos (Rúa, 2023).

En Ecuador, el acceso no consentido a sistemas informáticos o hacking no autorizado está tipificado como un delito y se encuentra regulado por la Ley Orgánica de Comunicación, que establece disposiciones relacionadas con la seguridad informática. Además, se aplican otras leyes y disposiciones

específicas relacionadas con delitos cibernéticos. Algunos puntos clave sobre cómo se maneja este delito en Ecuador son:

1. Ley Orgánica de Comunicación: La Ley Orgánica de Comunicación de Ecuador establece disposiciones relacionadas con la seguridad informática y la protección de datos personales. Esta ley prohíbe el acceso no autorizado a sistemas informáticos y redes, así como la difusión de información privada sin consentimiento.

2. Código Penal: El Código Penal ecuatoriano también contempla disposiciones relacionadas con delitos informáticos. Los artículos 230 y siguientes se refieren a la protección de sistemas y datos informáticos, y establecen sanciones para quienes cometan acceso no consentido o daño a sistemas informáticos.

3. Unidad de Investigación de Delitos Informáticos (UIDI): En Ecuador, existe la Unidad de Investigación de Delitos Informáticos (UIDI) de la Policía Nacional, encargada de investigar y combatir los delitos cibernéticos, incluyendo el acceso no consentido a sistemas informáticos.

4. Sanciones: Las sanciones para quienes cometan acceso no consentido a sistemas informáticos pueden variar según la gravedad del delito y el daño causado. Pueden incluir multas, penas de prisión y otras medidas punitivas, dependiendo de las circunstancias específicas del caso.

5. Cooperación Internacional: Ecuador también coopera con organizaciones internacionales y otros países para investigar y combatir delitos cibernéticos que trascienden las fronteras nacionales.

Es importante destacar que la legislación y las medidas para abordar los delitos informáticos, incluyendo el acceso no consentido, pueden evolucionar con el tiempo. Por lo tanto, es fundamental consultar a las autoridades competentes y a profesionales legales actualizados para obtener información precisa sobre cómo se maneja este tipo de delito en Ecuador en un momento dado. Además,

se recomienda que las organizaciones y los individuos tomen medidas proactivas para proteger sus sistemas y datos contra posibles ataques informáticos.

Principio de proporcionalidad de las penas en los delitos de hacking

El principio de proporcionalidad de las penas se origina en la filosofía y teoría del derecho penal, y tiene raíces históricas en la evolución de los sistemas de justicia penal a lo largo de los siglos. No tiene un origen específico en un lugar o momento determinado, sino que se ha desarrollado gradualmente como parte de la filosofía legal y la jurisprudencia a nivel global (Sinchiguano J. , 2022).

Algunos de los antecedentes históricos del principio de proporcionalidad de las penas pueden encontrarse en las obras de destacados filósofos y pensadores legales, como Cesare Beccaria, autor de "Dei delitti e delle pene" (De los delitos y las penas) en el siglo XVIII, quien abogaba por penas proporcionales y racionales en lugar de castigos crueles e inhumanos. La Ilustración europea influyó en gran medida en la promoción de ideas legales basadas en la razón y la justicia.

A lo largo del tiempo, este principio se ha incorporado en las leyes y sistemas legales de numerosos países y ha sido reconocido por diversas convenciones y tratados internacionales que abordan los derechos humanos y las normas de justicia penal. Su aplicación es fundamental para garantizar que las penas sean equitativas y no excesivamente severas, lo que contribuye a la protección de los derechos individuales y a la justicia en general.

El principio de proporcionalidad de las penas en los delitos de hacking es un concepto fundamental en el sistema de justicia penal que busca garantizar que las sanciones impuestas a los infractores sean proporcionales a la gravedad del delito y a las circunstancias individuales de cada caso. En el contexto de los delitos de hacking, este principio implica que las penas deben ajustarse de manera justa y equitativa al daño causado, el alcance de la intrusión informática y otros factores relevantes (Rodríguez J. , 2020).

En muchos sistemas legales, la proporcionalidad de las penas se evalúa teniendo en cuenta varios elementos, como la intención del infractor, el valor de la información o los datos robados, el impacto en las víctimas y la reiteración del delito. Por ejemplo, un hacking que resulta en la pérdida masiva de datos sensibles o la interrupción de servicios críticos puede considerarse más grave que un acceso no consentido a un sistema que no causa un daño significativo.

El objetivo principal de este principio es garantizar que las penas no sean excesivamente severas ni inadecuadas en relación con la naturaleza del delito. Además, busca promover la equidad y la justicia en el proceso legal, teniendo en cuenta la individualización de las penas para cada caso particular. La proporcionalidad de las penas también puede ser un factor importante en la prevención de delitos de hacking, ya que las penas apropiadas pueden disuadir a los posibles infractores.

Principio de Proporcionalidad en el Derecho Penal

El principio de proporcionalidad es un concepto fundamental en el derecho penal que se refiere a la idea de que las penas impuestas a los infractores deben ser proporcionales a la gravedad del delito cometido. Este principio tiene varias dimensiones y componentes clave que se exploran en el marco teórico del derecho penal (Sinchiguano, 2022). Montserrat (2018), menciona algunos temas específicos relacionados con el principio de proporcionalidad en el derecho penal:

1. **Origen y Fundamentos del Principio de Proporcionalidad:** Examina la historia y las bases filosóficas del principio de proporcionalidad en el derecho penal. ¿De dónde proviene este concepto y cuáles son sus raíces filosóficas?

2. **Dimensiones del Principio de Proporcionalidad:** Desglosa las dimensiones del principio de proporcionalidad, que suelen incluir la proporcionalidad en sentido estricto (la pena debe ser proporcionada al delito), la necesidad (la pena debe ser necesaria para lograr un fin

legítimo) y la idoneidad (la pena debe ser adecuada para el infractor y el delito).

3. **Derechos Humanos y Principio de Proporcionalidad:** Analiza cómo el principio de proporcionalidad se relaciona con los derechos humanos, especialmente en lo que respecta a la prohibición de tratos crueles, inhumanos o degradantes.

4. **Comparación Internacional:** Estudia cómo diferentes jurisdicciones aplican el principio de proporcionalidad en sus sistemas de justicia penal. Compara las leyes y sentencias de diferentes países para destacar similitudes y diferencias.

5. **Caso de Estudio:** Selecciona un caso de estudio relevante en el que se haya aplicado o cuestionado el principio de proporcionalidad en un proceso penal. Analiza los detalles del caso y su impacto en la jurisprudencia.

6. **Críticas al Principio de Proporcionalidad:** Explora las críticas y desafíos que el principio de proporcionalidad enfrenta en la práctica. Esto podría incluir debates sobre si las penas mínimas obligatorias son proporcionales o si la discreción judicial cumple con este principio.

7. **Reformas Legislativas:** Investiga si ha habido reformas legislativas que hayan afectado la aplicación del principio de proporcionalidad en el derecho penal de tu jurisdicción o en otros lugares.

8. **Delitos Específicos:** Examina cómo se aplica el principio de proporcionalidad en casos de delitos específicos, como homicidio, robo, narcotráfico u otros delitos graves.

9. **Jurisprudencia Internacional:** Revisa las decisiones de cortes internacionales, como la Corte Internacional de Justicia o la Corte Penal Internacional, para entender cómo aplican el principio de proporcionalidad en casos de crímenes internacionales.

10. **Recomendaciones y Perspectivas Futuras:** Considera las recomendaciones y perspectivas futuras en torno al principio de proporcionalidad en el derecho penal. ¿Cómo podría evolucionar este principio en respuesta a los cambios sociales y legales?

El principio de proporcionalidad en el derecho penal es un concepto fundamental que establece que las penas impuestas a los infractores deben ser proporcionales a la gravedad del delito cometido. Este principio se basa en una serie de componentes clave que guían la toma de decisiones en el sistema de justicia penal.

La primera dimensión del principio de proporcionalidad es la proporcionalidad en sentido estricto. Esto significa que la pena debe ser directamente proporcional a la gravedad del delito. En otras palabras, un delito menor no debe castigarse con una pena excesivamente severa, y un delito grave debe llevar consigo una pena acorde con su gravedad. La proporcionalidad en sentido estricto busca evitar que se impongan penas desmedidas o excesivas, lo que sería contrario a los principios de justicia y equidad (Ramos, 2019).

La segunda dimensión del principio de proporcionalidad es la necesidad. Esto implica que la pena debe ser necesaria para lograr un fin legítimo, como la prevención del delito, la rehabilitación del infractor o la protección de la sociedad. En otras palabras, no se debe imponer una pena si existen alternativas más apropiadas o menos restrictivas que puedan lograr el mismo objetivo. La necesidad asegura que las penas en el derecho penal sean justificadas y no se utilicen de manera arbitraria (Couso, 2018).

La tercera dimensión del principio de proporcionalidad es la idoneidad. Esta dimensión se refiere a que la pena debe ser adecuada tanto para el infractor como para el delito en cuestión. Esto significa que la pena debe ser proporcionada no solo a la gravedad del delito, sino también a las circunstancias personales del infractor. Por ejemplo, se debe considerar la edad, la salud mental y otros factores relevantes para determinar la idoneidad de la pena. La idoneidad garantiza que las penas sean justas y apropiadas para cada caso individual (Vaca, 2019).

El principio de proporcionalidad en el derecho penal se basa en tres dimensiones esenciales: la proporcionalidad en sentido estricto, la necesidad y la idoneidad. Estas dimensiones trabajan juntas para asegurar que las penas impuestas sean justas, proporcionales a la gravedad del delito y adecuadas tanto para el infractor como para la sociedad en general. El respeto y la aplicación adecuada de este principio son fundamentales para el funcionamiento equitativo del sistema de justicia penal.

Delitos Informáticos en Ecuador

Los delitos informáticos en Ecuador han adquirido una creciente relevancia en un mundo cada vez más digitalizado. En este contexto, es esencial explorar la legislación y las regulaciones relacionadas con los delitos informáticos en Ecuador. Esto incluye analizar los tipos de delitos que abarcan, como el hacking y el acceso no consentido a sistemas informáticos de telecomunicaciones. Estudiar la legislación específica que aborda estos delitos proporciona una base sólida para comprender las sanciones penales asociadas y cómo se aplican en la práctica (Branca, 2023).

Es fundamental considerar cómo se definen y clasifican estos delitos en el marco legal ecuatoriano, así como los elementos clave necesarios para establecer la culpabilidad. Esto podría incluir cuestiones como la intención maliciosa, la invasión de sistemas protegidos y el acceso no autorizado a datos confidenciales. La interpretación precisa de estos elementos es esencial para garantizar una aplicación coherente de la ley.

Un aspecto relevante de los delitos informáticos en Ecuador es la cuestión de las penas asociadas. Esto incluye el análisis de la gravedad de las sanciones y cómo se determina la proporcionalidad entre la pena y la gravedad del delito. En este contexto, se pueden abordar preguntas sobre si las penas actuales son adecuadas para disuadir eficazmente a los infractores y si se aplican de manera coherente.

Además de la legislación, es importante considerar cómo los tribunales ecuatorianos han interpretado y aplicado la ley en casos de delitos informáticos.

Esto implica examinar sentencias judiciales relevantes y casos de estudio para comprender la jurisprudencia y cómo se resuelven los casos en la práctica. Identificar tendencias y desafíos en la aplicación de la ley puede proporcionar información valiosa sobre la efectividad de las políticas actuales en la lucha contra los delitos informáticos en Ecuador (Cuenca, 2022).

El estudio de los delitos informáticos en Ecuador implica una exploración profunda de la legislación, la interpretación judicial y las sanciones penales asociadas. Esta investigación es esencial para comprender cómo el sistema legal ecuatoriano aborda estos delitos en un entorno digital en constante evolución y cómo se protegen los derechos de las partes involucradas.

Además de los aspectos legales y penales, hay varios puntos relevantes que se pueden abordar al explorar el tema de los delitos informáticos en Ecuador. El crecimiento de los delitos informáticos es un punto crítico. Es importante investigar y analizar cómo ha evolucionado la incidencia de los delitos informáticos en Ecuador en los últimos años, incluyendo el aumento de la ciberdelincuencia y su impacto en diversos sectores, como empresas, individuos y el gobierno.

Otro aspecto crucial es la rápida evolución de la tecnología y cómo esta ha influido en la naturaleza y sofisticación de los delitos informáticos. Puedes explorar cómo los delincuentes aprovechan las últimas tendencias tecnológicas y cómo las leyes se adaptan para abordar estas amenazas emergentes.

La cooperación internacional es esencial en el contexto de los delitos informáticos, que a menudo son transfronterizos. Ecuador puede estar involucrado en investigaciones y cooperación internacional en este ámbito, lo que hace relevante investigar los tratados y acuerdos de cooperación con otros países en la lucha contra la ciberdelincuencia (García, 2022).

Analizar los efectos socioeconómicos de los delitos informáticos en Ecuador es importante. Esto incluye cómo estos delitos pueden afectar la economía, la confianza del público en la tecnología y la seguridad de los datos.

Los delitos informáticos a menudo involucran la violación de la privacidad y la seguridad de los datos personales. Investigar las medidas de protección de datos y privacidad en Ecuador y cómo se aplican en casos de ciberdelincuencia es relevante.

Explorar los esfuerzos educativos y de sensibilización que se realizan en Ecuador para prevenir los delitos informáticos también es crucial. Esto incluye programas de concienciación dirigidos a individuos y empresas sobre prácticas de seguridad en línea.

Investigar cómo se fomenta la colaboración entre el sector público y privado en la detección y prevención de delitos informáticos es importante. Esto puede incluir la participación de empresas de tecnología, bancos y otras instituciones en la lucha contra la ciberdelincuencia.

Identificar los desafíos legales y jurídicos específicos que enfrenta Ecuador en la persecución de los delitos informáticos, como la extradición de delincuentes cibernéticos o la adquisición de pruebas electrónicas en investigaciones, es esencial.

Por último, analizar cuestiones éticas relacionadas con la ciberdelincuencia, como la responsabilidad de las empresas en la protección de datos y la ética en la piratería informática, también es relevante. Al abordar estos aspectos, se puede obtener una comprensión más completa de la situación de los delitos informáticos en Ecuador, sus implicaciones y los esfuerzos para combatirlos. Esto puede servir como base sólida para investigaciones más profundas o para el desarrollo de políticas y estrategias efectivas en la prevención y persecución de la ciberdelincuencia en el país.

Los delitos hacking y acceso no consentido

Los delitos de hacking y acceso no consentido a sistemas informáticos son cuestiones críticas en el ámbito de la ciberseguridad y la ley. Saraguro (2021), presenta algunas opiniones y perspectivas relevantes de expertos y stakeholders sobre estos delitos:

1. **Defensores de la Ciberseguridad**: Expertos en ciberseguridad y organizaciones dedicadas a la protección de sistemas informáticos a menudo argumentan que los delitos de hacking y acceso no consentido representan una seria amenaza para la seguridad en línea. Abogan por leyes y medidas de seguridad robustas para prevenir y sancionar estos delitos, ya que pueden resultar en la filtración de datos sensibles, el robo de información financiera o la interrupción de servicios críticos.

2. **Comunidad de Hacking Ético**: Existe una comunidad de hackers éticos que aboga por el uso responsable de las habilidades de hacking para identificar vulnerabilidades en sistemas y ayudar a las organizaciones a mejorar su seguridad. Argumentan que la distinción entre hackers éticos y criminales es fundamental y que se deben promover programas de recompensa por encontrar vulnerabilidades en lugar de criminalizar a todos los hackers.

3. **Gobiernos y Aplicación de la Ley**: Las agencias gubernamentales y las fuerzas del orden a menudo se esfuerzan por combatir los delitos de hacking y acceso no consentido. Argumentan que estos delitos pueden tener implicaciones graves para la seguridad nacional y económica, y buscan la extradición y el enjuiciamiento de los perpetradores.

4. **Legisladores y Reguladores**: Los legisladores y reguladores tienen la responsabilidad de definir las leyes y regulaciones que rigen estos delitos. Su enfoque puede variar, desde imponer sanciones severas hasta desarrollar políticas que fomenten la educación y la concienciación sobre la ciberseguridad.

5. **Empresas y Protección de Datos**: Las empresas y organizaciones suelen ser víctimas de delitos de hacking y acceso no consentido. Abogan por medidas de seguridad más sólidas y a menudo están sujetas a regulaciones de notificación de violaciones de datos. También desempeñan un papel importante en la promoción de la educación en ciberseguridad y la adopción de prácticas de seguridad sólidas.

6. **Ética en la Ciberseguridad**: La ética en la ciberseguridad es un tema importante, y algunos expertos abogan por la responsabilidad ética en la industria de la ciberseguridad. Argumentan que la seguridad cibernética no debe utilizarse para fines maliciosos y que los profesionales de la ciberseguridad deben adherirse a un código de conducta ético.

En conjunto, estas perspectivas ilustran la complejidad de los delitos de hacking y acceso no consentido, y cómo la sociedad y las partes interesadas están tratando de abordarlos desde diversas perspectivas, incluyendo la ciberseguridad, la ética y la aplicación de la ley. El equilibrio entre la lucha contra el cibercrimen y la protección de los derechos y la privacidad en línea es un desafío constante en la era digital.

El tratamiento y análisis legal de los delitos de hacking y acceso no consentido a sistemas informáticos requiere una serie de consideraciones fundamentales para garantizar la protección de los sistemas y la privacidad de los usuarios.

En primer lugar, es esencial contar con definiciones legales claras y precisas que describan de manera detallada las acciones que constituyen estos delitos. Esto incluye especificar qué se entiende por acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones o la distribución de software malicioso. Estas definiciones claras son cruciales para que los tribunales y las autoridades puedan aplicar las leyes de manera efectiva (Martínez, 2022).

En segundo lugar, las penalidades establecidas en las leyes deben ser proporcionales a la gravedad de los delitos. Esto significa que las sanciones penales, multas y otras medidas punitivas deben reflejar adecuadamente la magnitud del daño causado o el potencial de daño. Las penalidades deben ser lo suficientemente disuasorias para desalentar la comisión de estos delitos, pero también deben garantizar un enfoque justo y equitativo en la persecución de los delincuentes (Atienza & Fernández, 2020).

Además, es fundamental que las leyes diferencien de manera clara y precisa entre actividades legales y delictivas en el ámbito de la seguridad informática. Por ejemplo, las pruebas de penetración llevadas a cabo por profesionales de la

seguridad cibernética con el consentimiento de los propietarios de sistemas no deben considerarse delictivas. Estas actividades legítimas deben estar protegidas por la ley y no deben ser objeto de persecución penal.

Por último, el enfoque legal debe ser flexible y adaptable a medida que evoluciona la tecnología y cambian las amenazas cibernéticas. Las leyes deben estar en constante actualización para abordar nuevos métodos y técnicas utilizados por los delincuentes cibernéticos, y deben ser diseñadas para garantizar la protección de la seguridad informática y la privacidad en línea sin socavar las libertades individuales. En conjunto, un enfoque legal integral y actualizado es esencial para abordar eficazmente los delitos de hacking y acceso no consentido en la era digital (Soler, 2023).

En Ecuador, los delitos de hacking y acceso no consentido a sistemas informáticos son tratados en virtud de la legislación penal y de ciberseguridad del país. La legislación ecuatoriana ha evolucionado para abordar estas cuestiones en el contexto de la creciente digitalización de la sociedad.

En primer lugar, el Código Orgánico Integral Penal (COIP) de Ecuador incluye disposiciones que tipifican y sancionan los delitos informáticos, incluidos los relacionados con el acceso no autorizado a sistemas informáticos y la interceptación de datos electrónicos. Estos delitos pueden conllevar sanciones penales, multas y otras medidas coercitivas, dependiendo de la gravedad del delito.

Además, Ecuador ha desarrollado leyes específicas relacionadas con la ciberseguridad y la protección de datos, como la Ley Orgánica de Comunicación y la Ley Orgánica de Protección de Datos Personales. Estas leyes establecen obligaciones y responsabilidades tanto para las entidades públicas como privadas en lo que respecta a la seguridad de la información y la privacidad de los datos personales.

El país también ha creado instituciones y unidades especializadas, como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL),

encargada de supervisar y regular el sector de las telecomunicaciones y la tecnología de la información en Ecuador.

Sin embargo, como en muchos otros países, el tratamiento legal de estos delitos plantea desafíos continuos relacionados con la adaptación a la evolución tecnológica y las amenazas cibernéticas en constante cambio. La cooperación internacional y la capacitación de profesionales en ciberseguridad son áreas que continúan siendo cruciales para abordar eficazmente los delitos informáticos en Ecuador y en todo el mundo.

Jurisprudencia Internacional.

La jurisprudencia internacional es un componente esencial del derecho y desempeña un papel fundamental en la formación de políticas y la toma de decisiones legales en todo el mundo. Al explorar la jurisprudencia internacional, es necesario considerar una serie de aspectos clave.

Primero, es importante destacar cómo los tribunales internacionales, como la Corte Internacional de Justicia (CIJ) o la Corte Penal Internacional (CPI), han abordado casos relacionados con el derecho internacional. Esto incluye la interpretación de tratados, la resolución de disputas entre Estados y la persecución de crímenes internacionales (Sanmartín, 2021).

La jurisprudencia internacional también puede proporcionar información valiosa sobre la evolución del derecho internacional en áreas específicas, como los derechos humanos, el derecho humanitario, el derecho comercial y el derecho ambiental. Los fallos de estos tribunales pueden influir en la interpretación y aplicación de las leyes internacionales en diferentes jurisdicciones.

Además, es importante considerar cómo las decisiones de tribunales internacionales pueden afectar las relaciones entre Estados y cómo se implementan en la práctica. Esto puede incluir la ejecución de sentencias y la cooperación entre Estados para hacer cumplir el derecho internacional.

La jurisprudencia internacional también puede servir como referencia y orientación para los tribunales nacionales al resolver casos que involucran

cuestiones de derecho internacional. Los tribunales nacionales a menudo se basan en decisiones de tribunales internacionales para fundamentar sus propias decisiones (Guamán, 2023).

Por último, es relevante examinar cómo los Estados y las organizaciones internacionales utilizan la jurisprudencia internacional en la formulación de políticas y en la promoción del estado de derecho a nivel internacional. Esto puede incluir la defensa de posiciones políticas basadas en fallos de tribunales internacionales y la promoción de la cooperación y la paz en el ámbito global.

La jurisprudencia internacional desempeña un papel central en la interpretación y aplicación del derecho internacional. Su estudio es fundamental para comprender cómo se resuelven las disputas entre Estados, cómo evoluciona el derecho internacional y cómo influye en las políticas y decisiones legales en el ámbito internacional.

La jurisprudencia internacional es un campo esencial en el ámbito del derecho internacional y abarca una serie de aspectos fundamentales. Una de las características notables es la diversidad de fuentes que contribuyen a la jurisprudencia internacional, que incluye sentencias de cortes internacionales, decisiones de tribunales nacionales que aplican el derecho internacional, dictámenes consultivos de la Corte Internacional de Justicia y decisiones de órganos de tratados internacionales. Estas diversas fuentes se combinan para formar un cuerpo de jurisprudencia que orienta la interpretación y aplicación del derecho internacional (Burgos & Medina, 2022).

Un ámbito de especial importancia en la jurisprudencia internacional es su impacto en la protección de los derechos humanos a nivel global. Las decisiones de cortes como la Corte Interamericana de Derechos Humanos y la Corte Europea de Derechos Humanos establecen estándares significativos para la defensa de los derechos fundamentales. Estos precedentes influyen en la promoción y protección de los derechos humanos en todo el mundo.

Además, los tribunales internacionales desempeñan un papel crucial en la resolución de conflictos internacionales. La jurisprudencia derivada de casos de

disputas territoriales, comerciales u otros tipos contribuye a la resolución y aclaración de conflictos entre Estados.

La jurisprudencia internacional también contribuye al desarrollo y evolución del derecho internacional. Las decisiones de los tribunales internacionales pueden influir en la creación de nuevas normas y prácticas internacionales, así como en la consolidación de normas de derecho consuetudinario.

La interacción entre jurisdicciones nacionales e internacionales es un tema importante que aborda la jurisprudencia internacional. Los Estados deben encontrar un equilibrio entre sus obligaciones bajo el derecho internacional y su soberanía nacional, y la jurisprudencia internacional a menudo ofrece orientación sobre cómo resolver conflictos entre estas jurisdicciones.

La jurisprudencia internacional también ha sido fundamental en la promoción de áreas cruciales del derecho internacional, como el derecho ambiental y humanitario. Los casos relacionados con la protección del medio ambiente y la regulación de conflictos armados han establecido estándares esenciales para la comunidad internacional.

Finalmente, los tribunales internacionales, como el Tribunal Penal Internacional (TPI), desempeñan un papel fundamental en la persecución de crímenes internacionales y en la búsqueda de justicia en situaciones de conflicto y graves violaciones de derechos humanos. La jurisprudencia de estos tribunales aborda cuestiones relacionadas con la responsabilidad penal individual y la reparación a las víctimas (Rúa, 2023).

La jurisprudencia internacional es un campo en constante evolución que ejerce un impacto significativo en la promoción de valores, derechos y responsabilidades en el ámbito internacional, y su influencia abarca diversos aspectos del derecho internacional y la gobernanza global.

Comparación de leyes internacionales

España

En España, las leyes relacionadas con delitos informáticos, incluyendo el hacking y el acceso no consentido a sistemas informáticos de telecomunicaciones, están contempladas principalmente en el Código Penal. La aplicación del principio de proporcionalidad en las penas se basa en la gravedad del delito, las circunstancias específicas de cada caso y las leyes vigentes en el momento del juicio.

El Código Penal español contempla diversos tipos de delitos relacionados con la informática y las telecomunicaciones. Por ejemplo, el artículo 197 bis se refiere al acceso no autorizado a sistemas informáticos, y el artículo 278 trata sobre la interceptación de las comunicaciones.

En términos generales, la proporcionalidad en las penas significa que la sanción impuesta debe ser proporcionada a la gravedad del delito. Las leyes penales suelen establecer rangos de penas para diferentes delitos, y los tribunales tienen la facultad de determinar la pena exacta dentro de esos límites, teniendo en cuenta factores como la intencionalidad del acusado, el daño causado y otras circunstancias relevantes.

En España, las penas por delitos relacionados con el hacking y el acceso no consentido a sistemas informáticos están contempladas en el Código Penal. Por ejemplo, el artículo 197 bis del Código Penal español establece la pena de prisión de seis meses a dos años para aquellos que, sin estar debidamente autorizados, accedan o se mantengan en un sistema o en parte del mismo.

Inglaterra

En el Reino Unido, las leyes relacionadas con el hacking y el acceso no autorizado a sistemas informáticos se encuentran principalmente en la Ley de Delitos Informáticos de 1990 y otras disposiciones legales.

La proporcionalidad en las penas generalmente se rige por el principio de que la pena debe ser proporcional a la gravedad del delito. En el contexto de los delitos informáticos, las penas pueden variar según la naturaleza y la gravedad del delito, así como otros factores atenuantes o agravantes.

En el Reino Unido, el Acta de Delitos Informáticos de 1990 (Computer Misuse Act 1990) establece diversas disposiciones para penalizar el acceso no autorizado a sistemas informáticos. Por ejemplo, la sección 1 de la ley trata sobre el acceso no autorizado a programas o datos, y la sección 3 se refiere a la creación y distribución de software malicioso.

Las penas asociadas con estas disposiciones pueden incluir multas y penas de prisión, y la duración de estas penas puede variar según la gravedad del delito y otros factores. En casos graves, como el acceso no autorizado con intenciones maliciosas o la interferencia con sistemas críticos, las penas pueden ser más severas.

Brasil

En Brasil, los delitos informáticos están regulados por la Ley N.º 12.737/2012, conocida como la "Ley Carolina Dieckmann", y por disposiciones del Código Penal Brasileño. La ley aborda diversas formas de delitos informáticos, incluyendo el acceso no autorizado a sistemas y la interceptación indebida de comunicaciones electrónicas.

En términos generales, el principio de proporcionalidad en las penas establece que la sanción impuesta debe ser proporcional a la gravedad del delito. La legislación brasileña prevé penas específicas para los delitos informáticos, y la duración de las penas puede variar según la gravedad del delito, la presencia de agravantes o atenuantes, y otros factores.

La pena para delitos de acceso no autorizado a sistemas informáticos en Brasil puede incluir multas y penas de prisión, dependiendo de la gravedad y las circunstancias del delito. Además, en casos específicos, la legislación brasileña

también puede considerar la indemnización a la víctima como parte de las sanciones.

Argentina

En Argentina, los delitos informáticos, incluyendo el hacking y el acceso no consentido a sistemas informáticos, están regulados principalmente por la Ley N.º 26.388, conocida como la Ley de Delitos Informáticos. Esta ley tipifica y sanciona diversas conductas relacionadas con el uso indebido de sistemas informáticos y datos.

En términos generales, la proporcionalidad en las penas implica que las sanciones deben ser proporcionales a la gravedad del delito. Las penalidades por delitos informáticos en Argentina pueden incluir multas y penas de prisión, dependiendo de la naturaleza y la gravedad de la infracción.

Ecuador

En Ecuador, los delitos relacionados con hacking y acceso no consentido a sistemas informáticos se encuentran regulados en el Código Orgánico Integral Penal (COIP). El COIP aborda una variedad de conductas ilegales, incluyendo aquellas relacionadas con el acceso no autorizado a sistemas informáticos y la interceptación de datos.

El principio de proporcionalidad en las penas es un concepto general en derecho penal que establece que la gravedad de la pena debe ser proporcional a la gravedad del delito. Las leyes ecuatorianas suelen seguir este principio, y las penalidades por delitos informáticos pueden incluir sanciones como multas y penas de prisión.

Evolución de la Legislación en Delitos Informáticos

La evolución de la legislación en delitos informáticos ha sido una respuesta necesaria a la creciente digitalización de la sociedad y la proliferación de actividades delictivas en línea. A medida que la tecnología avanzaba, las autoridades y los legisladores se dieron cuenta de la importancia de establecer

un marco legal que abordara adecuadamente estas amenazas. En las primeras etapas de la informática, las leyes existentes resultaban insuficientes para abordar los delitos informáticos de manera efectiva (Saltos, 2022).

A finales del siglo XX y principios del siglo XXI, muchos países comenzaron a promulgar leyes específicas para abordar los delitos informáticos. Estas leyes tipificaban una variedad de acciones delictivas, como el acceso no autorizado a sistemas, el fraude en línea, el robo de datos y la difusión de malware. La legislación también incluyó disposiciones relacionadas con la responsabilidad de las empresas y la protección de datos personales (Cabezas, 2019).

A medida que las amenazas cibernéticas evolucionaban, la legislación tuvo que adaptarse para mantenerse al día. Esto implicaba la revisión y enmienda constante de las leyes existentes para abordar nuevas técnicas y tácticas utilizadas por los delincuentes cibernéticos. Además, la cooperación internacional se volvió esencial, ya que los delincuentes operan a menudo más allá de las fronteras nacionales. Los acuerdos y tratados internacionales también se desarrollaron para facilitar la persecución de los delitos informáticos a nivel global.

La legislación en delitos informáticos no solo se centró en la persecución, sino también en la prevención y la educación. Se establecieron programas de concienciación y capacitación para informar al público y a las empresas sobre las mejores prácticas de seguridad cibernética. Las empresas también se vieron obligadas a implementar medidas de seguridad más estrictas y a notificar a las autoridades y a los afectados en caso de violaciones de datos.

La evolución de la legislación en delitos informáticos refleja la creciente importancia de abordar las amenazas cibernéticas en la sociedad moderna. Ha habido un esfuerzo constante por parte de los legisladores para mantenerse al día con la tecnología y las tácticas de los delincuentes cibernéticos, y se ha promovido la cooperación internacional para combatir eficazmente estos delitos en un entorno digital en constante cambio. La legislación no solo busca castigar a los infractores, sino también proteger y concienciar al público sobre los riesgos y las mejores prácticas en línea.

Impacto Social y Tecnológico

El impacto social y tecnológico de los delitos informáticos es profundo y se extiende a todos los aspectos de la sociedad moderna. En primer lugar, a nivel social, los delitos informáticos han alterado la forma en que las personas interactúan en línea y han generado preocupaciones significativas sobre la seguridad y la privacidad en el ciberespacio. La percepción de la seguridad en línea ha disminuido debido a la amenaza constante de ataques informáticos, lo que ha llevado a un aumento en la desconfianza en la tecnología y en la forma en que se manejan los datos personales. Esto ha llevado a una mayor conciencia sobre la importancia de la ciberseguridad tanto para los individuos como para las organizaciones (Flores, 2019).

En un nivel tecnológico, los delitos informáticos han impulsado la innovación en ciberseguridad. La aparición de amenazas cibernéticas sofisticadas ha impulsado el desarrollo de soluciones de seguridad avanzadas. Empresas y gobiernos han invertido significativamente en la investigación y desarrollo de tecnologías de defensa cibernética, como firewalls, sistemas de detección de intrusiones y análisis de comportamiento de amenazas. Esto ha creado una industria en crecimiento en torno a la ciberseguridad, generando empleo y oportunidades económicas.

Además, el impacto de los delitos informáticos se extiende a la economía en general. Las empresas se han visto afectadas por la pérdida de datos, el robo de propiedad intelectual y los costos asociados con la recuperación de ataques cibernéticos. Esto ha impulsado la necesidad de inversiones adicionales en seguridad de la información y ha llevado a una mayor concienciación sobre los riesgos cibernéticos entre las empresas y sus clientes.

En el ámbito legal, los delitos informáticos han generado desafíos significativos para los sistemas judiciales. La complejidad de rastrear y enjuiciar a los delincuentes cibernéticos, que a menudo operan a nivel internacional, ha requerido una cooperación legal y policial transfronteriza más sólida. Se han establecido tratados y acuerdos internacionales para abordar la extradición de

delincuentes cibernéticos y facilitar la colaboración en la investigación y persecución de estos delitos (Salvadori, 2019).

El impacto social y tecnológico de los delitos informáticos es considerable. Ha generado preocupaciones sobre la seguridad y la privacidad en línea, ha impulsado la innovación en ciberseguridad, ha afectado a la economía y ha planteado desafíos legales significativos. En un mundo cada vez más conectado digitalmente, la gestión efectiva de los delitos informáticos se ha convertido en una prioridad crítica para individuos, empresas y gobiernos en todo el mundo.

Comparación con Otros Delitos en Ecuador

La comparación entre los delitos informáticos y otros tipos de delitos en Ecuador muestra diferencias y similitudes importantes en términos de su naturaleza, impacto y manejo legal. Alanya (2022), presentan algunas de las principales distinciones y semejanzas:

1. **Naturaleza de los Delitos**:
    - **Delitos Informáticos**: Los delitos informáticos implican el uso de tecnología y sistemas informáticos para cometer actos ilegales, como el acceso no autorizado, el fraude en línea o la difusión de malware.
    - **Otros Delitos**: Otros delitos pueden abarcar una amplia gama de actividades, desde delitos violentos hasta delitos financieros tradicionales, como el robo o la estafa.
2. **Impacto**:
    - **Delitos Informáticos**: Los delitos informáticos pueden tener un impacto significativo en la privacidad, la seguridad de los datos y la confianza en línea. Pueden afectar tanto a individuos como a empresas y entidades gubernamentales.
    - **Otros Delitos**: Otros delitos pueden tener un impacto variado en las víctimas, dependiendo de su naturaleza. Pueden causar daño

físico, emocional o financiero, y pueden tener un alcance limitado o más generalizado.

3. **Evolución y Tecnología**:

    - **Delitos Informáticos**: Los delitos informáticos están estrechamente vinculados al avance tecnológico. Evolucionan constantemente a medida que los delincuentes cibernéticos desarrollan nuevas técnicas y herramientas.

    - **Otros Delitos**: Si bien otros delitos también pueden aprovechar la tecnología, su evolución no está tan directamente ligada a la innovación tecnológica como en el caso de los delitos informáticos.

4. **Investigación y Persecución**:

    - **Delitos Informáticos**: La investigación y persecución de delitos informáticos a menudo requieren conocimientos especializados en ciberseguridad y tecnología. Además, los delincuentes cibernéticos a veces operan a nivel internacional, lo que complica la persecución.

    - **Otros Delitos**: La investigación y persecución de otros delitos pueden implicar métodos tradicionales de aplicación de la ley, como la investigación de escenas del crimen y la recopilación de pruebas testimoniales.

5. **Cooperación Internacional**:

    - **Delitos Informáticos**: Debido a su naturaleza transfronteriza, los delitos informáticos a menudo requieren una cooperación internacional más sólida y acuerdos de extradición efectivos.

    - **Otros Delitos**: Si bien la cooperación internacional también es importante para otros delitos, puede variar en función de la naturaleza y la gravedad del delito.

6. **Legislación Específica**:

    - **Delitos Informáticos**: Ecuador y otros países han promulgado leyes específicas para abordar los delitos informáticos y la ciberseguridad, reconociendo su importancia en la era digital.

    - **Otros Delitos**: Otros delitos se rigen por las leyes penales tradicionales, aunque pueden haber disposiciones específicas para ciertas categorías de delitos.

Los delitos informáticos representan una categoría única de delitos en Ecuador y en todo el mundo debido a su relación con la tecnología y su impacto en la era digital. Sin embargo, comparten algunos desafíos comunes con otros tipos de delitos, como la necesidad de investigación y persecución efectivas, así como la importancia de la cooperación internacional en la lucha contra la delincuencia.

Reformas Legislativas Propuestas

Las reformas legislativas propuestas en Ecuador en relación a los delitos informáticos y la ciberseguridad tienen como objetivo fortalecer la capacidad del país para abordar eficazmente las amenazas cibernéticas en constante evolución y proteger los derechos y la seguridad de los ciudadanos (Rodríguez, 2020). Amores (2022), menciona algunas de las reformas clave que se han propuesto o que podrían ser consideradas incluyen:

1. **Actualización de las Leyes Existentes**: Una de las primeras medidas es actualizar las leyes existentes relacionadas con la ciberseguridad y los delitos informáticos. Esto implica definir claramente los tipos de delitos informáticos, sus penas asociadas y los procedimientos de investigación y persecución. Las definiciones precisas y actualizadas son esenciales para abordar las nuevas amenazas cibernéticas.

2. **Protección de Datos Personales**: La protección de datos personales es una preocupación clave en la era digital. Se proponen reformas para fortalecer las regulaciones de protección de datos y privacidad,

garantizando que las empresas y las entidades gubernamentales manejen la información personal de manera segura y transparente.

3. **Fortalecimiento de la Cooperación Internacional**: Dado que los delitos informáticos son a menudo transfronterizos, se proponen reformas para fortalecer la cooperación internacional en la investigación y persecución de estos delitos. Esto incluye la ratificación y aplicación efectiva de tratados y acuerdos de extradición.

4. **Fomento de la Ciberseguridad Empresarial**: Se promueve la legislación que obliga a las empresas a implementar medidas de ciberseguridad efectivas y a notificar las violaciones de datos a las autoridades y a los afectados. Esto busca proteger la información confidencial y la propiedad intelectual.

5. **Sanciones Agravadas**: Se proponen sanciones más severas para los delincuentes cibernéticos, especialmente en casos de ataques graves, como los dirigidos contra infraestructuras críticas o servicios esenciales. Estas sanciones pueden incluir penas de prisión prolongadas y multas sustanciales.

6. **Educación y Concienciación**: Se promueven reformas que requieran programas de educación y concienciación sobre ciberseguridad tanto para individuos como para empresas. La educación es fundamental para empoderar a las personas para protegerse en línea.

7. **Capacitación de las Fuerzas de Seguridad**: Se propone el fortalecimiento de la capacitación y recursos de las fuerzas de seguridad para investigar y combatir los delitos informáticos de manera efectiva. Esto incluye el establecimiento de equipos especializados en ciberseguridad.

8. **Protección a Denunciantes**: Se considera la implementación de protecciones legales para los denunciantes que revelen actividades

ilegales en línea, fomentando la colaboración en la detección de delitos informáticos.

En conjunto, estas reformas legislativas buscan modernizar la legislación ecuatoriana en materia de ciberseguridad y delitos informáticos, garantizar la protección de datos y la privacidad de los ciudadanos, y fortalecer la capacidad del país para abordar las amenazas cibernéticas en constante evolución. Además, promueven la colaboración entre el sector público y privado y la concienciación pública sobre la importancia de la ciberseguridad en la sociedad actual.

Derechos Humanos y Derechos Digitales

Los derechos humanos y los derechos digitales están estrechamente entrelazados en la era digital. Los derechos humanos son fundamentales para proteger la dignidad y la libertad de las personas, y esto se extiende al mundo en línea. Los derechos digitales se refieren a las libertades y protecciones específicas relacionadas con la tecnología y la comunicación en línea (Rodríguez V. , 2022).

En este contexto, el derecho a la privacidad es uno de los aspectos más críticos. La creciente recopilación de datos personales en línea ha llevado a una mayor preocupación por la protección de la privacidad. Los individuos tienen el derecho de controlar sus datos personales y decidir cómo se recopilan y utilizan. La regulación de la privacidad en línea, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, es un ejemplo de cómo se han adoptado medidas para proteger este derecho en el entorno digital.

Además, la libertad de expresión y la libertad de acceso a la información son esenciales en línea. Los individuos tienen el derecho de expresar sus opiniones y acceder a información diversa en plataformas digitales sin temor a la censura o la discriminación. Sin embargo, esto también plantea desafíos en términos de moderación de contenido y la lucha contra la desinformación, lo que requiere un equilibrio entre la libertad de expresión y la protección contra el discurso de odio y la difusión de noticias falsas.

La seguridad digital es otra área clave. Los derechos digitales implican el derecho a la seguridad en línea, lo que incluye la protección contra el cibercrimen y la vigilancia injustificada. Los individuos deben poder utilizar la tecnología de forma segura sin temor a la violación de su privacidad o la pérdida de datos.

Los derechos humanos y los derechos digitales están intrínsecamente conectados en un mundo cada vez más digitalizado. La protección de la privacidad, la libertad de expresión y la seguridad en línea son aspectos fundamentales de esta relación. Las legislaciones y regulaciones en torno a los derechos digitales están evolucionando para abordar los desafíos y oportunidades que plantea la era digital, buscando garantizar que los individuos disfruten de sus derechos humanos tanto en el mundo físico como en el ciberespacio.

Los derechos humanos y los derechos digitales están profundamente entrelazados en la era digital. Los derechos humanos, fundamentales para proteger la dignidad y la libertad de las personas, se han extendido a la esfera en línea. Los derechos digitales se refieren a las libertades y protecciones específicas relacionadas con la tecnología y la comunicación en línea. Un componente esencial es el derecho a la privacidad en un mundo digitalmente interconectado, donde la recopilación de datos personales es ubicua. Los individuos tienen el derecho de controlar cómo se recopilan y utilizan sus datos, y regulaciones como el RGPD de la Unión Europea buscan garantizar esta protección (Sinchiguano L. , 2018).

La libertad de expresión y el acceso a la información son derechos vitales en el ciberespacio. Los individuos deben poder expresar sus opiniones y acceder a una variedad de información en línea sin temor a la censura o la discriminación. Sin embargo, esto también plantea el desafío de equilibrar la libertad de expresión con la lucha contra la desinformación y el discurso de odio, lo que requiere políticas y regulaciones cuidadosamente diseñadas.

La seguridad digital es otra área fundamental. Los derechos digitales incluyen el derecho a la seguridad en línea, lo que implica proteger a las personas contra el cibercrimen y la vigilancia injustificada. Los individuos deben poder utilizar la

tecnología de manera segura sin temor a la violación de su privacidad o la pérdida de datos.

Además de estos derechos y desafíos, el acceso a Internet se considera cada vez más un derecho humano básico en sí mismo. La neutralidad de la red y las cuestiones relacionadas con los derechos de autor también desempeñan un papel importante en el discurso sobre los derechos digitales. La regulación de las grandes plataformas en línea y la brecha digital son otras áreas de preocupación. En resumen, los derechos humanos y digitales están intrínsecamente vinculados en el mundo digital y son fundamentales para garantizar que las personas puedan disfrutar de sus derechos en línea tanto como en el mundo físico.

Caso de Estudio

Un caso de estudio emblemático en el ámbito de los derechos humanos y digitales es el de Edward Snowden y las revelaciones de vigilancia masiva llevadas a cabo por la Agencia de Seguridad Nacional (NSA) de los Estados Unidos. En 2013, Edward Snowden, un contratista de la NSA, filtró una gran cantidad de documentos clasificados que revelaron el alcance de los programas de vigilancia de la NSA, tanto a nivel nacional como internacional (Gavilán, 2016).

Este caso generó un intenso debate sobre la privacidad en la era digital y la relación entre la seguridad nacional y los derechos individuales. Por un lado, algunos argumentaron que la revelación de Snowden fue un acto de valentía que puso de manifiesto la necesidad de proteger la privacidad de los ciudadanos frente a la vigilancia gubernamental intrusiva. Por otro lado, se argumentó que las filtraciones representaban una amenaza para la seguridad nacional y la lucha contra el terrorismo.

El caso Snowden también tuvo un impacto significativo en la percepción de la privacidad en línea y en la adopción de medidas de ciberseguridad. Desencadenó reformas legislativas en los Estados Unidos y llevó a un mayor escrutinio de los programas de vigilancia gubernamental en todo el mundo.

Este caso de estudio ilustra cómo las cuestiones de derechos humanos y digitales pueden converger en situaciones en las que la tecnología y la vigilancia estatal se entrelazan. También destaca la importancia de la transparencia, el equilibrio entre la seguridad y la privacidad, y el papel de los denunciantes en la protección de los derechos digitales y la rendición de cuentas gubernamental. En última instancia, el caso Snowden ha influido en el debate global sobre la vigilancia y la privacidad en la era digital y ha llevado a cambios significativos en políticas y prácticas en varios países.

Otro caso de estudio importante en la intersección entre derechos humanos y tecnología es el conflicto entre Apple y el FBI en 2016. El caso se originó cuando el FBI solicitó la ayuda de Apple para desbloquear un iPhone utilizado por uno de los tiradores en el ataque de San Bernardino, California, en el que murieron 14 personas. El FBI argumentó que necesitaba acceder al contenido del dispositivo como parte de una investigación de seguridad nacional (Serra, 2017).

El conflicto se centró en cuestiones fundamentales de privacidad y seguridad digital. Apple se negó a cumplir la solicitud del FBI, argumentando que crear una puerta trasera para desbloquear el iPhone pondría en peligro la privacidad y la seguridad de todos los usuarios de sus dispositivos. Afirmaron que tal puerta trasera podría ser explotada por actores maliciosos y debilitaría la protección de datos personales.

El caso generó un intenso debate público sobre el equilibrio entre la seguridad nacional y la privacidad individual en la era digital. Tanto defensores de la privacidad como agencias de seguridad nacional argumentaron sus puntos de vista. Finalmente, el FBI logró acceder al iPhone con la ayuda de un tercero, lo que evitó una decisión judicial que podría haber sentado un precedente legal importante.

Este caso ilustra cómo la tecnología puede plantear desafíos éticos y legales complejos en el contexto de los derechos humanos. También destaca la importancia de la encriptación y la seguridad de datos en la era digital, así como la necesidad de encontrar soluciones equitativas que equilibren la seguridad y la privacidad en línea. Desde entonces, ha habido un continuo debate sobre estas

cuestiones y sus implicaciones para la protección de los derechos digitales y humanos en la sociedad moderna.

Opiniones de Expertos y Stakeholders

Las opiniones de expertos y stakeholders en el ámbito de los derechos humanos y digitales son fundamentales para enriquecer el debate y la toma de decisiones sobre cuestiones críticas en este campo. Caisaguano (2023), presentan algunas de las perspectivas y opiniones que suelen expresarse:

1. **Defensores de la Privacidad**: Expertos en privacidad y organizaciones de derechos civiles a menudo enfatizan la importancia de proteger la privacidad en línea como un derecho fundamental. Argumentan que la vigilancia masiva y la recopilación de datos por parte de gobiernos y empresas deben estar estrictamente reguladas para evitar abusos y proteger la autonomía de los individuos.

2. **Gobiernos y Agencias de Seguridad**: Las agencias de seguridad nacional y algunos gobiernos argumentan que la vigilancia y la recopilación de datos son esenciales para la seguridad nacional y la lucha contra el terrorismo. Sostienen que el acceso a ciertos datos es crucial para prevenir amenazas graves.

3. **Empresas Tecnológicas**: Las empresas tecnológicas, como Facebook, Google y Apple, a menudo defienden la privacidad de sus usuarios como un valor central y argumentan que la encriptación y otras medidas de seguridad son esenciales para proteger la confidencialidad de los datos personales.

4. **Académicos en Ciberseguridad y Ética**: Los expertos académicos en campos como la ética y la ciberseguridad pueden proporcionar análisis imparciales y basados en evidencia sobre los desafíos éticos y técnicos relacionados con la seguridad y la privacidad en línea.

5. **Usuarios y Ciudadanos**: La opinión pública también es un factor importante. Los usuarios y ciudadanos a menudo expresan sus

preocupaciones sobre la privacidad en línea y la seguridad de sus datos personales. Sus opiniones pueden influir en la formulación de políticas y en las prácticas de las empresas.

6. **Organizaciones Internacionales y de Derechos Humanos**: Organizaciones como las Naciones Unidas y Amnistía Internacional juegan un papel importante en la promoción de los derechos humanos y digitales a nivel global. Emiten informes, hacen recomendaciones y abogan por políticas que protejan los derechos individuales en línea.

7. **Legisladores y Reguladores**: Los legisladores y reguladores están encargados de crear leyes y regulaciones que equilibren la seguridad y la privacidad en línea. Sus decisiones pueden tener un impacto significativo en la forma en que se abordan las cuestiones de derechos humanos y digitales.

Las opiniones de expertos y stakeholders reflejan una amplia gama de perspectivas en el campo de los derechos humanos y digitales. El equilibrio entre la seguridad y la privacidad en línea es un tema complejo y en constante evolución, y la participación de múltiples partes interesadas es esencial para encontrar soluciones equitativas y efectivas.

CAPITULO II

Metodología del Proceso de Investigación

Enfoque

El enfoque de la investigación se refiere a la estrategia o enfoque metodológico que un investigador utiliza para llevar a cabo un estudio o investigación en particular. Es la dirección o el marco teórico que guía el proceso de investigación y determina cómo se recopilarán y analizarán los datos (Fernández, Baptista, & Hernández, 2018).

Un enfoque cualitativo se centra en comprender en profundidad las experiencias y percepciones de los actores involucrados en el sistema legal y en casos reales. A continuación se presenta un enfoque cualitativo sugerido para esta investigación:

1. Diseño de la Investigación

- **Selección de Participantes:** Se identificarán y seleccionarán participantes clave para la investigación, como abogados, jueces, fiscales, defensores públicos, expertos legales y personas que han sido acusadas o condenadas por delitos informáticos en Ecuador.

- **Entrevistas Semiestructuradas:** Se llevarán a cabo entrevistas en profundidad con los participantes seleccionados. Las entrevistas se centrarán en cuestiones relacionadas con el principio de proporcionalidad en las penas de delitos de hacking y acceso no consentido. Se formularán preguntas como: ¿Cuál es su opinión sobre las penas actuales en estos delitos? ¿Cómo se determina la gravedad de un delito informático? ¿Qué consideran proporcional en estos casos?

2. Recopilación de Datos

- **Entrevistas:** Se registrarán y transcribirán las entrevistas con los participantes. Se utilizará el análisis de contenido para identificar temas y patrones emergentes relacionados con el principio de proporcionalidad.

3. Análisis de Datos

- **Codificación y Categorización:** Se codificarán y categorizarán los datos de las entrevistas y documentos legales para identificar patrones temáticos relacionados con la proporcionalidad de las penas.

4. Interpretación de Resultados

- **Interpretación de Entrevistas:** Se buscará comprender las perspectivas y opiniones de los participantes sobre el principio de proporcionalidad y su aplicación en casos de delitos informáticos en Ecuador.
- **Conclusiones:** Se identificarán patrones y tendencias en la aplicación de penas y la percepción de la proporcionalidad en el sistema legal ecuatoriano.

6. Informe Final

- Se presentarán los resultados y conclusiones en un informe final (discusión) que incluirá una revisión de la literatura relevante, el diseño de la investigación, la metodología, los hallazgos y las recomendaciones.

Tipo de investigación

La investigación sobre el principio de proporcionalidad en las penas de los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador se llevará a cabo como un estudio cualitativo. Este enfoque cualitativo permitirá una comprensión profunda de las experiencias y percepciones de los actores involucrados en el sistema legal y en casos reales, así como una exploración detallada de las cuestiones relacionadas con la proporcionalidad en las penas en este contexto.

- **Investigación descriptiva**

La investigación descriptiva es un tipo de investigación científica que se centra en describir y analizar detalladamente un fenómeno, evento, proceso o grupo de individuos, sin realizar manipulaciones o alteraciones deliberadas en las variables estudiadas (Fernández, Baptista, & Hernández, 2018).

La investigación se basará en entrevistas semiestructuradas con participantes clave, análisis de contenido de las respuestas obtenidas, revisión de casos judiciales y documentos legales relevantes, y análisis detallado de casos específicos para evaluar la aplicación del principio de proporcionalidad en las penas. Esta metodología cualitativa permitirá obtener una visión integral y enriquecedora de la situación actual en Ecuador en lo que respecta a la aplicación de penas en estos delitos informáticos.

- **Investigación de campo**

La investigación de campo es un tipo de investigación que se lleva a cabo en el entorno real, natural o específico donde ocurren los fenómenos o eventos que se están estudiando. En este tipo de investigación, los investigadores recopilan datos directamente en el lugar de los hechos, en lugar de hacerlo en un laboratorio o en un entorno controlado (Hernández, Fernández, & Baptista, 2018).

El estudio de investigación de campo involucrará una serie de actividades, como entrevistas presenciales con abogados. Este enfoque de investigación de campo permitirá obtener una comprensión profunda y contextualizada de cómo se aplica el principio de proporcionalidad en las penas de los delitos de hacking y acceso no consentido en sistemas informáticos en Ecuador, al interactuar directamente con los actores y examinar los casos de manera detallada en el entorno legal real del país.

Métodos de investigación

En el contexto de la investigación, se pueden emplear varios métodos de investigación para recopilar y analizar datos, para la investigación se llevaran a cabo los siguientes:

1. **Entrevistas Cualitativas:** Realizar entrevistas semiestructuradas con participantes clave, como abogados, jueces, fiscales, defensores públicos y personas acusadas o condenadas por delitos informáticos. Las entrevistas permiten obtener perspectivas detalladas y opiniones de los sujetos sobre el tema, así como explorar en profundidad cuestiones relacionadas con la proporcionalidad en las penas.

2. **Análisis Documental:** Examinar casos judiciales relevantes y sentencias relacionadas con delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador. El análisis documental proporciona una visión de cómo se han aplicado las penas en casos anteriores y puede revelar tendencias en la jurisprudencia.

3. **Revisión de la Legislación:** Realizar un análisis exhaustivo de la legislación vigente en Ecuador relacionada con los delitos de hacking y acceso no consentido a sistemas informáticos. Esto incluye identificar las penas establecidas en la legislación y cualquier orientación específica sobre la proporcionalidad.

4. **Comparación Internacional:** Realizar investigaciones comparativas con otros países que enfrenten problemas similares en la legislación de delitos informáticos. Esto puede proporcionar perspectivas adicionales sobre cómo se maneja la proporcionalidad en las penas en diferentes contextos legales.

5. **Análisis de Contenido:** Utilizar técnicas de análisis de contenido para examinar las transcripciones de las entrevistas, documentos legales y otros materiales recopilados. Esto ayuda a identificar patrones temáticos y tendencias en los datos.

Técnicas e instrumentos

Para llevar a cabo la investigación, es necesario utilizar diversas técnicas e instrumentos para recopilar y analizar datos de manera efectiva. Las técnicas e instrumentes a utilizar, son los siguientes:

Una entrevista es un proceso de comunicación en el que una persona, conocida como el entrevistador, realiza una serie de preguntas a otra persona o grupo de personas, conocidos como entrevistados, con el propósito de obtener información, opiniones, perspectivas, relatos o respuestas a preguntas específicas (Hernández, Fernández, & Baptista, 2018).

Técnicas:

- **Entrevistas Semiestructuradas:** Esta técnica implica realizar entrevistas en persona o por medio de videoconferencia con participantes clave, como abogados, jueces, fiscales y personas acusadas de delitos informáticos. Se pueden utilizar guiones de entrevista para asegurarse de cubrir preguntas clave sobre la proporcionalidad de las penas y obtener respuestas detalladas.

Instrumentos:

- **Guiones de Entrevista:** Prepara guiones de entrevista detallados que incluyan preguntas específicas sobre el principio de proporcionalidad, la percepción de las penas y otros temas relevantes. Los guiones de entrevista te ayudarán a mantener un enfoque consistente en todas las entrevistas

- **Cámaras o Grabadoras de Audio:** Se contará con los dispositivos necesarios para registrar las conversaciones de manera precisa.

Periodo y lugar

La población se refiere al conjunto completo o la totalidad de elementos, individuos, objetos o eventos que comparten una característica común y son objeto de estudio en una investigación y una muestra es un subconjunto representativo de la población total que se elige para ser estudiado en una investigación (Hernández, Fernández, & Baptista, 2018).

La instigación se llevara a cabo en el Consejo de la Judicatura, ubicada en la Av. 25 de julio de la ciudad de Guayaquil, durante los meses de octubre y noviembre **el año 2023.**

Población y muestra

La población de estudio estará conformada por 5 abogados, funcionarios públicos con diversas y extensas trayectorias profesionales, por lo tanto la población de estudio está conformada por 5 individuos, se descarta el cálculo de la muestra debido a la cantidad limitadas de sujetos de estudio.

El cálculo de muestra se emplea cuando la población es extensa y resulta inviable o poco práctico estudiar a todos sus miembros. En estos casos, se opta por seleccionar una muestra representativa de dicha población para llevar a cabo la investigación. No obstante, cuando la población es tan reducida que se puede acceder y estudiar a todos sus individuos sin dificultad, no se requiere llevar a cabo un proceso de muestreo, ya que es posible investigar directamente a todos los miembros de la población.

En el contexto actual, la población de estudio está conformada por únicamente cuatro individuos específicos. Por lo tanto, es factible abordar y estudiar a cada uno de ellos directamente, sin necesidad de llevar a cabo un cálculo de muestra.

Tabla 1

Población y muestra

Posesional	Área	Experiencia
Ab. Fernando Lalama	Juez de los tribunales penales del Guayas	20 años en el sector público ejerciendo como juez de Tribunales de garantías penales del Guayas.
Ab. David Sebastián Vergara Solís	Estudio Jurídico Vergara Acosta	Experiencia profesional en el campo legal: Abogado Litigante por más de diez años de experiencia, seis años en la docencia universitaria, Asesor Legal de la cámara de

		comercio de Samborondón. Especialización o experiencia previa en casos de delitos informáticos: Maestría en derecho de nuevas tecnologías.
Dr. Andrés Rodrigo Jácome Cobo	Experiencia profesional en el campo legal: 23 años	• Especialización o experiencia previa en casos de delitos informáticos: • Magister en Derecho y Gestión de las Telecomunicaciones • Especialista Superior en Derecho y Gestión de las Telecomunicaciones • Profesor Universitario en Delitos informáticos. • Ex Director de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.
Ab. Gabriel Correa Barzallo	Defensor Público del Azuay	• Experiencia profesional en el campo legal: 16 años. • Especialización o experiencia previa en casos de delitos informáticos: 4 años
AB. Joseph Rober Mendieta Toledo	Juez de la Sala de lo Penal de la Corte Provincial de Justicia del Oro	• Experiencia profesional en el campo legal: 28 años de ejercer en la función pública, 20 años de docencia universitaria. Especialización o experiencia previa en casos de delitos informáticos: Experiencia en casos de delitos informáticos por pornografía infantil y Maestrías en campo del derecho.

Elaborado por: Granizo, Francisco (2023)

Operacionalización de las variables

Tabla 2

Operacionalización de las variables

Variable	Definición Operativa	Dimensiones	Indicadores	Técnicas de Medición
Variable independiente: Tipo de Delito Informático	El tipo específico de delito informático cometido e-n cada caso.	- Naturaleza del Delito – Gravedad del Delito	- Categorización de los casos en función del tipo de delito informático (hacking, acceso no consentido, otros, etc.).	Entrevistas a expertos
Variable dependiente: Proporcionalidad en las Penas	La medida en que las penas impuestas se ajustan al principio de proporcionalidad en casos de delitos informáticos.	- Gravedad del Delito - Cumplimiento de Estándares Legales - Circunstancias del Caso	- Evaluación de la gravedad del delito en cada caso. - Comparación de las penas con estándares legales. - Evaluación de la adecuación de las penas a las circunstancias específicas.	Entrevistas a expertos

Elaborado por: Granizo, Francisco (2023)

Procedimiento y procesamiento

Para llevar a cabo la investigación sobre el principio de proporcionalidad en las penas de los delitos de hacking y acceso no consentido a sistemas informáticos de telecomunicaciones en Ecuador a través de entrevistas, se sigue un procedimiento específico. A continuación, se detalla el procedimiento y procesamiento de datos:

Procedimiento de Investigación con Entrevistas:

1. **Preparación:** Se identifican y contactan a los participantes clave, entre ellos abogados, jueces, fiscales, defensores públicos y personas condenadas por delitos informáticos en Ecuador. Se obtiene el consentimiento informado de los participantes para su participación en las entrevistas.

2. **Diseño de la Entrevista:** Se desarrolla un guión de entrevista semiestructurado que contiene preguntas específicas relacionadas con la proporcionalidad en las penas en casos de delitos informáticos. Se asegura que las preguntas sean claras y pertinentes para los objetivos de la investigación.

3. **Conducción de Entrevistas:** Se realizan las entrevistas con los participantes seleccionados. Las entrevistas pueden llevarse a cabo de forma presencial, telefónica o por videoconferencia. Se registran las entrevistas mediante grabaciones de audio o transcripciones escritas.

4. **Análisis de Datos en Tiempo Real:** Se efectúa un análisis preliminar de los datos de cada entrevista a medida que se realizan para identificar patrones emergentes y ajustar las preguntas en función de los hallazgos.

Procesamiento de Datos:

1. **Transcripción:** Las entrevistas grabadas se transcriben en formato de texto para facilitar el análisis y la revisión posterior.

2. **Análisis de Contenido:** Se realiza un análisis de contenido de las transcripciones codificadas para identificar patrones, tendencias y perspectivas de los participantes en relación con la proporcionalidad en las penas.

3. **Comparación y Evaluación:** Se comparan las respuestas de los participantes con respecto a la proporcionalidad en las penas y se evalúa si existen discrepancias significativas o convergencias en las percepciones y opiniones.

4. **Informe Final:** Se presentan los resultados y conclusiones en un informe final que incluye una revisión de la literatura, el diseño de la investigación, la metodología, los hallazgos y las recomendaciones basadas en las entrevistas.

CAPITULO III

Análisis e Interpretación de Resultados de la Investigación

Resultados de las entrevistas

Entrevista 1

Ab. Fernando Lalama.

Juez de los Tribunales de Garantías Penales del Guayas, 20 años en el sector público ejerciendo como miembro del Tribunal de Garantías penales del Guayas.

Preguntas sobre Delitos Informáticos:

1. **De acuerdo con su criterio, ¿cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador?**

En Ecuador, los delitos de hacking y acceso no consentido a sistemas informáticos se definen en el Código Orgánico Integral Penal (COIP), específicamente en la sección de Delitos contra la seguridad de los activos de los sistemas de información y comunicación. El hacking implica acceder sin autorización para interferir en el funcionamiento normal de la red o sistemas, mientras que el acceso no consentido se refiere al ingreso sin autorización a un sistema o red. Aunque el acceso no consentido está definido en el artículo 234 del COIP, el concepto de hacking abarca varias acciones dentro de esta sección, incluyendo explotar, modificar, desviar y re direccionar.

2. **Desde su experiencia y de acuerdo a su criterio, cuál sería la importancia que le da la legislación Ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?**

Al evaluar la gravedad de un delito informático en el sistema legal ecuatoriano, se consideran diversos factores como el impacto, la naturaleza del delito, el bien jurídico afectado y la identidad de los infractores. Por ejemplo, el acceso no autorizado y la interferencia en programas telemáticos pueden tener

consecuencias menos graves que la divulgación no autorizada de información sensible de clientes por parte de un servidor público o empleado bancario. Además, se analiza la afectación a bienes jurídicos como patrimonio, intimidad o propiedad. La gravedad también puede depender de la relevancia de la víctima y si hay reincidencia por parte del infractor.

3. **Desde su experiencia, ¿ha conocido o llevado algún caso de delitos informáticos?**

Personalmente, no he tenido casos de delitos informáticos en mi tribunal. Sin embargo, a nivel internacional, se conoce el caso de un ataque cibernético en Ucrania en 2015, donde hackers cerraron temporalmente generadores de energía mediante malware distribuido por correos electrónicos. En Ecuador, se registró un caso de acceso no autorizado a sistemas informáticos en 2022, donde una aplicación recopilaba información de usuarios sin autorización. El responsable fue condenado por acceso no consentido a sistemas informáticos y revelación ilegal de base de datos.

4. **En su opinión, ¿Qué desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?**

Los desafíos comunes incluyen la discreción de los infractores, que operan de manera sigilosa para eliminar rastros, utilizando sistemas de terceros y técnicas para ocultar información. La falta de capacitación especializada en unidades de investigación y la transnacionalidad de estos delitos también representa obstáculos. La cooperación internacional y el desarrollo de enfoques legales y técnicos avanzados son esenciales para abordar eficazmente estos problemas.

5. **Desde esta línea de ideas, ¿qué criterios y factores se consideran al aplicar el principio de proporcionalidad en las penas de los delitos informáticos?**

En casos de delitos informáticos, el principio de proporcionalidad se aplica considerando factores como circunstancias atenuantes o agravantes, el alcance del daño causado a las víctimas, la situación de la víctima, la reincidencia, la

gravedad de la infracción y el grado de participación del infractor. La individualización de la pena, según el artículo 54 del COIP, observa las circunstancias del hecho punible, las necesidades y condiciones de la víctima, y todas las circunstancias que limitan la responsabilidad penal.

6. **¿Ha notado discrepancias entre las sanciones impuestas en casos de delitos informáticos y la severidad de las acciones perpetradas?**

Sí, se han observado discrepancias en algunas ocasiones. Las leyes pueden no estar completamente actualizadas para abordar la ciberdelincuencia en constante evolución. Además, la falta de capacitación del personal y la necesidad de recursos humanos calificados contribuyen a estas discrepancias. Es crucial reformar las leyes y proporcionar formación adecuada para asegurar que las penas sean proporcionales a la gravedad de los delitos informáticos.

7. **¿Cómo evalúa usted la efectividad de las penas vigentes para prevenir los delitos informáticos en Ecuador?**

Aunque el código penal puede necesitar actualizaciones para abordar mejor la ciberdelincuencia, la efectividad no debe evaluarse solo desde la perspectiva normativa. Se debe considerar la necesidad de desarrollar tanto la normativa como las capacidades técnicas de los operadores judiciales y la concienciación ciudadana. La reforma normativa y la preparación técnica deben ir de la mano para combatir eficazmente los delitos informáticos.

8. **¿Considera que hay aspectos específicos en la legislación ecuatoriana sobre delitos informáticos que requieran mejoras o actualizaciones?**

Sí, es necesario mejorar y actualizar la legislación ecuatoriana relacionada con los delitos informáticos. Dada la naturaleza cambiante y sofisticada de la ciberdelincuencia, el Código Orgánico Integral Penal debe desarrollarse con mayor atención y urgencia para hacer frente a estos desafíos emergentes.

Preguntas sobre la Percepción de la Proporcionalidad:

9. **¿Cuál es su percepción acerca de cómo la comunidad legal en Ecuador valora la proporcionalidad en las penas de los delitos informáticos?**

La percepción en la comunidad legal en Ecuador sobre la proporcionalidad en las penas de los delitos informáticos puede ser mixta. Algunos abogados podrían considerar las penas existentes como adecuadas, mientras que otros podrían argumentar que son insuficientes o desproporcionadas dada la gravedad de ciertos delitos informáticos. La falta de jurisprudencia consolidada puede contribuir a opiniones variadas.

10. **¿Ha enfrentado casos en los cuales los implicados por delitos informáticos han manifestado discrepancias con respecto a la proporcionalidad de las penas impuestas?**

No, en mi experiencia no he tenido casos de acusados o condenados por delitos informáticos expresando desacuerdo con la proporcionalidad de las penas.

11. **¿Hay discrepancias notables en cómo perciben la proporcionalidad de las penas entre distintos participantes legales, como jueces, fiscales, abogados defensores y acusados?**

Sí, puede haber diferencias significativas en la percepción de la proporcionalidad entre los diferentes actores legales. Las opiniones pueden variar según la comprensión de las complejidades técnicas, la experiencia y las perspectivas individuales. Los jueces, fiscales, abogados defensores y acusados pueden tener enfoques diferentes sobre qué penas son proporcionadas para los delitos informáticos, lo que destaca la necesidad de una revisión y actualización cuidadosa de las leyes relacionadas con la ciberdelincuencia.

Entrevista 2

Ab. David Sebastián Vergara Solís, Estudio Jurídico Vergara Acosta.

Experiencia profesional en el campo legal: Abogado Litigante por más de diez años de experiencia, seis años en la docencia universitaria, Asesor Legal de la cámara de comercio de Samborondón.

Especialización o experiencia previa en casos de delitos informáticos: Maestría en derecho de nuevas tecnologías.

Preguntas sobre Delitos Informáticos:

1. **De acuerdo con su criterio, ¿cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador?**

En Ecuador, el delito de hacking, o acceso no consentido a sistemas informáticos, se refiere a la acción ilícita de ingresar sin autorización a un sistema para explotar dicho acceso.

2. **Desde su experiencia y de acuerdo a su criterio, ¿cuál sería la importancia que le da la legislación Ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?**

La gravedad se determina considerando factores como el bien jurídico protegido y la calificación del sujeto activo. Por ejemplo, el ataque a derechos de menores de edad o personas con discapacidad agrava la pena. La conducta de un funcionario público también puede incrementar la gravedad.

3. **Desde su experiencia, ¿ha conocido o llevado algún caso de delitos informáticos?**

Ejemplo 1: Acceso no consentido a un sistema de pagos de una universidad causando un perjuicio de $90.000.

Ejemplo 2: Injuria calumniosa cometida a través de redes sociales.

4. **En su opinión, ¿Qué desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?**

Los desafíos incluyen la preparación previa de las empresas para prevenir fraudes y la necesidad de mecanismos de cooperación internacional para combatir el delito informático entre países.

5. **Desde esta línea de ideas, ¿qué criterios y factores se consideran al aplicar el principio de proporcionalidad en las penas de los delitos informáticos?**

La aplicación del principio de proporcionalidad se basa en el bien jurídico lesionado y la naturaleza de la información sustraída o difundida.

6. **¿Ha notado discrepancias entre las sanciones impuestas en casos de delitos informáticos y la severidad de las acciones perpetradas?**

La aplicación del principio de proporcionalidad se basa en el bien jurídico lesionado y la naturaleza de la información sustraída o difundida.

7. **¿Cómo evalúa usted la efectividad de las penas vigentes para prevenir los delitos informáticos en Ecuador?**

La efectividad radica más en la prevención a través de la ciberseguridad que en las penas privativas de libertad, dada la escasez de casos con estas penas.

8. **¿Considera que hay aspectos específicos en la legislación ecuatoriana sobre delitos informáticos que requieran mejoras o actualizaciones?**

Sí, la reciente aprobación de la Ley Orgánica de Protección de Datos Personales fue un avance necesario, pero aún hay aspectos que pueden mejorarse.

Preguntas sobre la Percepción de la Proporcionalidad:

9. **¿Cuál es su percepción acerca de cómo la comunidad legal en Ecuador valora la proporcionalidad en las penas de los delitos informáticos?**

La comunidad legal tiende a considerar algunas penas desproporcionadas a pesar de la gravedad de las conductas.

10. **¿Ha enfrentado casos en los cuales los acusados o condenados por delitos informáticos han manifestado discrepancias con respecto a la proporcionalidad de las penas impuestas?**

No he experimentado situaciones así.

11. **¿Hay discrepancias notables en cómo perciben la proporcionalidad de las penas entre distintos participantes legales, como jueces, fiscales, abogados defensores y acusados?**

Desde mi experiencia como abogado litigante y docente, hay falta de congruencia entre algunas penas de delitos informáticos y sus resultados.

Entrevista 3

Nombre y cargo actual: Dr. Andrés Rodrigo Jácome Cobo

Experiencia profesional en el campo legal: 23 años.

- Especialización o experiencia previa en casos de delitos informáticos:
- Magister en Derecho y Gestión de las Telecomunicaciones
- Especialista Superior en Derecho y Gestión de las Telecomunicaciones
- Profesor Universitario en Delitos informáticos.
- Ex Director de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.

Preguntas sobre Delitos Informáticos:

1. **De acuerdo con su criterio, ¿cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador?**

En Ecuador, los delitos informáticos, como el hacking, se definen como conductas ilícitas realizadas a través de medios electrónicos. En el artículo 234 de nuestro código, el hacking se describe como el acceso no consentido total o parcial a sistemas informáticos, telemáticos o de telecomunicaciones, incluyendo la permanencia no autorizada con el propósito de explotar el acceso, modificar un portal web, re direccionar tráfico u ofrecer servicios a terceros.

2. **Desde su experiencia y de acuerdo a su criterio, ¿cuál sería la importancia que le da la legislación Ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?**

La gravedad se evalúa considerando el daño al sistema o la información. Peritos intervienen para objetivamente medir la magnitud del perjuicio. Por ejemplo, casos como el acceso no consentido al sistema de la Corporación Nacional de Telecomunicaciones.

3. **Desde su experiencia, ¿ha conocido o llevado algún caso de delitos informáticos?**

Sí, algunas tipificaciones no consideran adecuadamente la magnitud del daño, como tener la misma pena para acceso no consentido y acceso con explotación ilegítima, a pesar de su impacto diferente.

4. **En su opinión, ¿Que desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?**

El principio de proporcionalidad implica ajustar la pena según el daño causado. Sin embargo, la aplicación se ve limitada por la naturaleza de los bienes jurídicos, como la privacidad. La pena debería considerar no solo el acceso no autorizado sino también el daño real, como la afectación a la vida en casos extremos.

5. **Desde esta línea de ideas, ¿Qué criterios y factores se consideran al aplicar el principio de proporcionalidad en las penas de los delitos informáticos en Ecuador?**

   Las penas actuales no parecen generar disuasión efectiva. El aumento de casos está relacionado con incentivos como el anonimato y la ubicuidad, superando la influencia disuasiva de las penas.

6. **¿Ha notado discrepancias entre las sanciones impuestas en casos de delitos informáticos y la severidad de las acciones perpetradas?**

Es necesario reconocer que estos delitos evolucionan con la tecnología. La legislación debe ser dinámica y actualizarse constantemente para abordar nuevas formas de infracciones y proteger los derechos de manera efectiva.

Preguntas sobre la Percepción de la Proporcionalidad:

7. **¿Cuál es su percepción acerca de cómo la comunidad legal en Ecuador valora la proporcionalidad en las penas de los delitos informáticos?**

La comunidad legal, guiada por el mandato constitucional del principio de proporcionalidad, debe construir un sistema penal que garantice la justicia y proteja eficientemente a las personas.

8. **¿Ha enfrentado casos en los cuales los acusados o condenados por delitos informáticos han manifestado discrepancias con respecto a la proporcionalidad de las penas impuestas?**

No he vivido situaciones así.

9. **¿Hay discrepancias notables en cómo perciben la proporcionalidad de las penas entre distintos participantes legales, como jueces, fiscales, abogados defensores y acusados?**

Cada actor, según su rol, puede tener su propia percepción de la proporcionalidad. Sin embargo, se espera que los jueces, por su imparcialidad, busquen aplicar sanciones que se alineen con el daño demostrado en el proceso judicial.

Entrevista 4

Ab. Gabriel Correa Barzallo, Defensor Público del Azuay.

Experiencia profesional en el campo legal: 16 años.

Especialización o experiencia previa en casos de delitos informáticos: 4 años

Preguntas sobre Delitos Informáticos:

1. **De acuerdo con su criterio, ¿Cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos?**

En Ecuador, estos delitos, comúnmente regulados en las leyes de ciberseguridad, están contemplados en el Código Orgánico Integral Penal (COIP). Esto incluye acciones como acceso no autorizado, robo de información, alteración de datos y otras prácticas ilegales relacionadas con el uso indebido de sistemas informáticos.

2. **Desde su experiencia y de acuerdo a su criterio ¿Cuál sería la importancia que le da la legislación ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?**

La gravedad se evalúa considerando varios factores, como la naturaleza específica del delito, el daño causado, la intención del perpetrador, la magnitud del delito, la reincidencia y agravantes como la participación de menores o motivación económica.

3. **Desde su experiencia, ¿ha conocido o llevado algún caso de delitos informaticos?**

Ejemplo 1: Acceso no consentido al buró de crédito para conocer el estado financiero de una persona. Ejemplo 2: Injuria calumniosa a través de redes sociales.

4. **En su opinión, ¿Qué desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?**

Los desafíos incluyen el anonimato y la ubicación de los perpetradores, cambios tecnológicos, colaboración, normativa obsoleta, falta de recursos y la naturaleza transnacional de la ciberdelincuencia.

5. **Desde esta línea de ideas, ¿qué criterios y factores que se consideran al aplicar el principio de proporcionalidad en las penas de los delitos informáticos?**

El principio de proporcionalidad implica ajustar las penas según la gravedad del delito y circunstancias específicas. Factores incluyen la naturaleza del delito, daño causado, intención, magnitud, reincidencia y agravantes.

6. **¿Ha notado discrepancias entre las sanciones impuestas en casos de delitos informáticos y la severidad de las acciones perpetradas?**

No he observado discrepancias al respecto.

7. **¿Cómo evalúa usted la efectividad de las penas vigentes para prevenir los delitos informáticos en Ecuador?**

La percepción varía, pero las penas actuales no parecen disuadir eficazmente, ya que el aumento de casos está vinculado a incentivos como el anonimato y la ubicuidad tecnológica.

8. **¿Considera que hay aspectos específicos en la legislación ecuatoriana sobre delitos informáticos que requieran mejoras o actualizaciones?**

La legislación debe actualizarse constantemente para abordar amenazas emergentes y cambios tecnológicos, incluyendo definiciones claras, penas proporcionales y protección de datos.

Preguntas sobre la Percepción de la Proporcionalidad:

9. **¿Cuál es su percepción acerca de cómo la comunidad legal en Ecuador valora la proporcionalidad en las penas de los delitos informáticos?**

La percepción puede variar, pero la comunidad legal debe construir un sistema basado en el mandato constitucional de proporcionalidad.

10. **¿Ha enfrentado casos en los cuales los acusados o condenados por delitos informáticos han manifestado discrepancias con respecto a la proporcionalidad de las penas impuestas?**

No tengo experiencias específicas al respecto.

11. **¿Hay discrepancias notables en cómo perciben la proporcionalidad de las penas entre distintos participantes legales, como jueces, fiscales, abogados defensores y acusados?**

Es común que los diferentes actores legales tengan percepciones diversas sobre la proporcionalidad, influenciadas por perspectivas y roles individuales.

Entrevista 5

Ab. Joseph Rober Mendieta Toledo, Juez de la Sala de lo Penal de la Corte Provincial de Justicia del Oro.

Experiencia profesional en el campo legal: 28 años de ejercer en la función pública, 20 años de docencia universitaria.

Especialización o experiencia previa en casos de delitos informáticos: Experiencia en casos de delitos informáticos por pornografía infantil y Maestrías en campo del derecho.

Preguntas sobre Delitos Informáticos:

1. **De acuerdo con su criterio, ¿Cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador?**

En Ecuador, los delitos informáticos están tipificados en el Código Orgánico Integral Penal (COIP), específicamente en el título quinto y el artículo 234. Estos incluyen acciones como el acceso no autorizado a sistemas informáticos, también conocido como hacking o intrusismo informático. La legislación considera esta conducta como el acceso ilegal a sistemas informáticos sin autorización, castigado con penas privativas de libertad de 1 a 3 años.

2. **Desde su experiencia y de acuerdo a su criterio, ¿Cuál sería la importancia que le da la legislación ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?**

En mis 28 años en la Función Judicial, no he tenido muchos casos de delitos informáticos, pero la gravedad de estos delitos se evalúa considerando varios factores. Esto incluye el daño causado, las circunstancias específicas del caso, como la participación de una o más personas y la tipificación en el COIP. La magnitud del daño y las circunstancias agravantes o atenuantes son elementos clave para determinar la gravedad del delito.

3. **Desde su experiencia, ¿Ha conocido o llevado algún caso de delitos informáticos?**

En un caso frecuente en Ecuador, se trata de estafas mediante técnicas como el phishing para obtener datos personales. Un ejemplo específico involucra la apertura de cuentas bancarias virtuales a nombre de la víctima. La tipificación del delito puede presentar desafíos, como el fiscal que se equivocó al hablar del acceso informático en lugar de abordar el beneficio obtenido. La claridad en la tipificación es crucial para evitar problemas en el enjuiciamiento.

4. **En su opinión, ¿Qué desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?**

Los desafíos comunes incluyen la falta de información y la demora en obtenerla, especialmente cuando la información está en servidores extranjeros. La limitada suscripción de convenios internacionales dificulta el intercambio de información. Además, se necesita sofisticación en la investigación y peritaje informático, así como una mayor colaboración con el sector privado para combatir eficazmente la ciberdelincuencia.

5. **Desde esta línea de ideas, ¿Qué criterios y factores se consideran al aplicar el principio de proporcionalidad en las penas de los delitos informáticos?**

La proporcionalidad en las penas se basa en la gravedad del delito, evaluando el alcance del daño, las circunstancias agravantes o atenuantes y el impacto social. La legislación del COIP establece que las penas deben ser proporcionales a la magnitud del delito, considerando factores específicos de cada caso.

6. **¿Ha notado discrepancias entre las sanciones impuestas en casos de delitos informáticos y la severidad de las acciones perpetradas?**

No he observado discrepancias significativas. Las penas, en general, se ajustan a la gravedad del delito, considerando la legislación establecida en el COIP.

7. **¿Cómo evalúa usted la efectividad de las penas vigentes para prevenir los delitos informáticos en Ecuador?**

Dada la creciente frecuencia de denuncias y casos reportados de delitos informáticos en Ecuador, las penas actuales parecen no ser suficientemente disuasivas. Es necesario considerar penas preventivas y evaluar la efectividad global del sistema legal en este contexto.

8. **¿Considera que hay aspectos específicos en la legislación ecuatoriana sobre delitos informáticos que requieran mejoras o actualizaciones?**

Sí, considero que es crucial revisar y mejorar la legislación relacionada con delitos informáticos en el COIP. Esto incluye definiciones más claras, sanciones adecuadas, procedimientos de investigación y peritaje informático, así como una mayor colaboración internacional y educación ciudadana para prevenir estos delitos.

Preguntas sobre la Percepción de la Proporcionalidad:

9. **¿Cuál es su percepción acerca de cómo la comunidad legal en Ecuador valora la proporcionalidad en las penas de los delitos informáticos?**

En general, hay preocupación en la comunidad legal debido al aumento de denuncias de delitos informáticos. Mejorar la legislación y las penas es necesario para garantizar una proporcionalidad efectiva y abordar los desafíos actuales.

10. **¿Ha enfrentado casos en los cuales los acusados o condenados por delitos informáticos han manifestado discrepancias con respecto a la proporcionalidad de las penas impuestas?**

Sí, en un caso donde se ratificó la inocencia, la víctima expresó su desacuerdo. Es esencial seguir protocolos claros para evitar problemas y garantizar la justicia.

11. **¿Hay discrepancias notables en cómo perciben la proporcionalidad de las penas entre distintos participantes legales, como jueces, fiscales, abogados defensores y acusados?**

Es común que haya desacuerdos entre los diferentes actores legales sobre la proporcionalidad de las penas. La mejora de la legislación y la claridad en la tipificación son clave para abordar estas diferencias y fortalecer el sistema legal.

Resultados de las entrevistas

- **Interrogante 1**

Las respuestas a esta pregunta reflejan un entendimiento compartido sobre la definición legal de los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador, enfocándose principalmente en el marco legal existente y los elementos específicos que caracterizan estas conductas.

Consistencia en la Identificación del Marco Legal:

En las cinco entrevistas, hay una consistencia notable en la identificación del marco legal que regula los delitos de hacking y acceso no consentido: el Código Orgánico Integral Penal (COIP) de Ecuador. Todos los entrevistados reconocen esta legislación como el principal referente para definir y sancionar estas prácticas ilegales.

Diversidad en los Detalles de la Definición:

Aunque hay un consenso sobre la ubicación legal de estos delitos, cada entrevistado aporta matices adicionales en la definición. Se destacan aspectos como la interferencia en el funcionamiento normal de la red o sistemas, el acceso no autorizado a sistemas informáticos, y la realización de acciones específicas como explotar, modificar, desviar y redireccionar información. Esta diversidad de detalles contribuye a una comprensión más holística de las prácticas delictivas en el ámbito informático.

Énfasis en la Evolución y Actualización de la Legislación:

Algunos entrevistados resaltan la necesidad de actualizar y mejorar la legislación ecuatoriana en delitos informáticos, reconociendo la naturaleza en constante evolución de la ciberdelincuencia. Este énfasis en la adaptabilidad legal destaca la conciencia de los desafíos emergentes y la importancia de mantener normativas actualizadas y adecuadas.

Reflejo de la Complejidad del Tema:

Las respuestas indican que los entrevistados comprenden la complejidad inherente a los delitos informáticos. Se mencionan acciones específicas y se considera la gravedad del impacto en el funcionamiento de los sistemas y en los bienes jurídicos afectados, como la propiedad, la intimidad y el patrimonio.

Conclusiones:

En conclusión, las respuestas a la pregunta sobre la definición legal de los delitos de hacking y acceso no consentido en Ecuador revelan un consenso en la identificación del marco legal y una comprensión compartida de la complejidad de estos delitos. La diversidad de detalles proporcionados y el reconocimiento de la necesidad de actualización reflejan un enfoque integral hacia la regulación de la ciberdelincuencia en el contexto jurídico ecuatoriano. Este análisis destaca la importancia de mantenerse al tanto de los avances tecnológicos y las dinámicas cambiantes de los delitos informáticos para garantizar la eficacia de la legislación en este ámbito.

- **Interrogante 2**

Las respuestas a la pregunta sobre la importancia que le da la legislación ecuatoriana a la gravedad de un delito informático revelan diferentes perspectivas y enfoques por parte de los entrevistados. Aquí se presenta un análisis detallado:

1. Evaluación de Factores Agravantes y Atenuantes:

Los entrevistados coinciden en que la legislación ecuatoriana considera factores específicos para evaluar la gravedad de un delito informático. Estos factores incluyen el bien jurídico afectado, la naturaleza del delito, la identidad del infractor, y el impacto en las víctimas. Se resalta la importancia de la evaluación

integral de estas circunstancias para determinar la gravedad y aplicar penas proporcionales.

2. Reconocimiento de la Transnacionalidad de los Delitos:

Algunas respuestas destacan la importancia de abordar la transnacionalidad de los delitos informáticos en la legislación. La naturaleza sin fronteras de estos delitos presenta desafíos particulares, y se subraya la necesidad de cooperación internacional y enfoques legales avanzados para enfrentar eficazmente este problema.

3. Consideración del Impacto en Bienes Jurídicos:

Los entrevistados resaltan la importancia de considerar el impacto en bienes jurídicos como la propiedad, la intimidad y el patrimonio al evaluar la gravedad de los delitos informáticos. La afectación a estos bienes influye en la severidad de las penas y en la percepción de la gravedad del delito.

4. Necesidad de Actualización y Reforma:

Algunos entrevistados sugieren que la legislación actual puede no estar completamente actualizada para abordar la evolución constante de la ciberdelincuencia. Se destaca la necesidad de reformas legislativas para garantizar que la normativa esté alineada con los desafíos emergentes y las prácticas delictivas en el ámbito digital.

Conclusiones:

En conclusión, las respuestas reflejan la conciencia de la importancia de la legislación ecuatoriana en la evaluación de la gravedad de los delitos informáticos. La consideración de factores agravantes y atenuantes, la atención a la transnacionalidad de los delitos, la ponderación del impacto en bienes jurídicos y la necesidad de actualización legislativa son temas comunes en las respuestas. Este análisis sugiere que los entrevistados reconocen la relevancia crítica de la legislación en la gestión y penalización adecuada de los delitos informáticos en Ecuador.

- **Interrogante 3**

Las respuestas a la pregunta sobre la experiencia en casos de delitos informáticos proporcionan información valiosa sobre la exposición y participación directa de los entrevistados en asuntos relacionados con la ciberdelincuencia. Aquí se presenta un análisis de las respuestas:

1. Variedad de Casos y Contextos:

Las respuestas muestran una diversidad de situaciones relacionadas con delitos informáticos. Los ejemplos incluyen acceso no autorizado a sistemas, ataques cibernéticos, divulgación no autorizada de información y estafas a través de medios digitales. Esta variedad sugiere la amplitud de escenarios en los que los profesionales legales pueden encontrarse con delitos informáticos.

2. Conocimiento Internacional de Casos:

Algunos entrevistados mencionan casos internacionales para ilustrar ejemplos de delitos informáticos. Esto destaca la conexión global de la ciberdelincuencia y la importancia de la cooperación internacional en la gestión de estos casos.

3. Desafíos en la Investigación y Enjuiciamiento:

Aunque algunos entrevistados no han llevado casos directos en sus jurisdicciones, reconocen los desafíos comunes en la investigación y enjuiciamiento de delitos informáticos. Se destacan obstáculos como la falta de capacitación especializada, la transnacionalidad de los delitos y la necesidad de cooperación internacional.

4. Necesidad de Actualización y Recursos:

Se señala la necesidad de actualizar leyes y proporcionar recursos adecuados para abordar eficazmente la ciberdelincuencia. La falta de legislación actualizada y de recursos humanos capacitados se identifica como un desafío significativo.

Conclusiones:

En conclusión, las respuestas revelan que, si bien algunos entrevistados han tenido experiencia directa en casos de delitos informáticos, otros han observado la problemática desde una perspectiva más internacional o general. Esto destaca la complejidad y la multidimensionalidad de la ciberdelincuencia. Los desafíos comunes en la investigación y enjuiciamiento subrayan la necesidad de fortalecer la capacidad legal y técnica para abordar efectivamente estos casos en el ámbito local e internacional.

- **Interrogante 4**

La pregunta sobre los desafíos en la investigación y enjuiciamiento de delitos informáticos revela aspectos críticos que los profesionales del ámbito legal enfrentan al lidiar con casos de ciberdelincuencia. Aquí se presenta un análisis de las respuestas obtenidas en las entrevistas:

1. Discreción y Sofisticación de los Infractores:

Los entrevistados señalan la discreción y sofisticación de los infractores como uno de los principales desafíos. La habilidad de los delincuentes para operar de manera sigilosa, eliminar rastros y utilizar sistemas de terceros presenta dificultades sustanciales en la identificación y persecución de los responsables.

2. Falta de Capacitación Especializada:

La falta de capacitación especializada en unidades de investigación es un desafío común mencionado. La ciberdelincuencia requiere un conocimiento técnico específico, y la falta de expertos en este campo puede obstaculizar la investigación y enjuiciamiento efectivos.

3. Naturaleza Transnacional de los Delitos:

La naturaleza transnacional de los delitos informáticos se destaca como otro desafío. La ubicuidad de las amenazas cibernéticas y la capacidad de los delincuentes para operar más allá de las fronteras nacionales dificultan la coordinación y la persecución efectiva.

4. Cooperación Internacional:

Se enfatiza la necesidad de una cooperación internacional más estrecha. Dada la naturaleza global de la ciberdelincuencia, la colaboración entre países se presenta como esencial para abordar eficazmente estos delitos.

5. Necesidad de Enfoques Legales y Técnicos Avanzados:

La necesidad de enfoques legales y técnicos avanzados también se menciona como un desafío. La rápida evolución de las amenazas cibernéticas requiere una respuesta legal y técnica que esté a la altura de las complejidades de la ciberdelincuencia.

Conclusiones:

En resumen, los desafíos identificados resaltan la complejidad inherente a la investigación y enjuiciamiento de delitos informáticos. La discreción de los infractores, la falta de capacitación especializada, la naturaleza transnacional de los delitos y la necesidad de cooperación internacional subrayan la importancia de un enfoque integral y colaborativo para hacer frente a estos desafíos. Además, la constante actualización de enfoques legales y técnicos se presenta como esencial para mantenerse al día con la evolución de la ciberdelincuencia.

- **Interrogante 5**

La pregunta sobre los criterios y factores considerados al aplicar el principio de proporcionalidad en las penas de los delitos informáticos ofrece una visión detallada de cómo los expertos legales evalúan la gravedad de estos delitos. Aquí se presenta un análisis basado en las respuestas de las entrevistas:

1. Circunstancias Agravantes o Atenuantes:

Los entrevistados destacan la importancia de considerar circunstancias agravantes o atenuantes al aplicar el principio de proporcionalidad. Factores como la intención del infractor, la magnitud del daño causado y la reincidencia se mencionan como elementos clave en la determinación de la pena.

2. Alcance del Daño y Bien Jurídico Afectado:

La evaluación del alcance del daño y el bien jurídico afectado es esencial. Los profesionales del derecho consideran la naturaleza específica del delito, la afectación a la privacidad, propiedad, patrimonio u otros derechos para determinar la gravedad y, por ende, la proporcionalidad de la pena.

3. Situación y Relevancia de la Víctima:

La situación y relevancia de la víctima también se tienen en cuenta. La gravedad del delito puede variar según la importancia de la víctima, y la ley debe adaptarse para reflejar estas diferencias.

4. Individualización de la Pena:

La individualización de la pena, de acuerdo con el artículo 54 del COIP, implica analizar las circunstancias del hecho punible, las necesidades y condiciones de la víctima, y todas las circunstancias que limitan la responsabilidad penal del infractor.

Conclusiones:

En resumen, la aplicación del principio de proporcionalidad en los delitos informáticos se basa en una evaluación integral de las circunstancias específicas de cada caso. Los criterios incluyen consideraciones sobre la intención del infractor, el alcance del daño, el bien jurídico afectado, la situación de la víctima y la individualización de la pena. Este enfoque refleja la complejidad y la necesidad de adaptabilidad en el sistema legal para abordar la diversidad de situaciones que involucran delitos informáticos.

- **Interrogante 6**

La pregunta sobre la percepción de discrepancias entre las sanciones impuestas y la severidad de las acciones perpetradas proporciona información valiosa sobre la efectividad del marco legal en el ámbito de los delitos informáticos. A continuación, se presenta un análisis basado en las respuestas de las entrevistas:

1. Desafíos en la Coherencia Legal:

Todos los entrevistados reconocen la existencia de discrepancias en algunas ocasiones. Estas discrepancias se atribuyen a desafíos como la falta de actualización de las leyes para abordar la evolución constante de la ciberdelincuencia. La naturaleza cambiante y sofisticada de estos delitos destaca la necesidad de reformas y actualizaciones regulares.

2. Falta de Capacitación y Recursos Humanos Especializados:

La falta de capacitación del personal encargado de hacer cumplir la ley y la escasez de recursos humanos calificados contribuyen a las discrepancias. La complejidad técnica de los delitos informáticos requiere una comprensión especializada que a menudo falta en las unidades de investigación.

3. Urgencia de Reformas Legales:

La necesidad de reformas legales y una mayor capacitación son resaltadas como cruciales para garantizar que las penas sean proporcionales a la gravedad de los delitos informáticos. La adaptación normativa es esencial para abordar la ciberdelincuencia de manera efectiva.

Conclusiones:

La conciencia de las discrepancias entre las sanciones y la gravedad de las acciones perpetradas es generalizada entre los profesionales del derecho entrevistados. La falta de actualización legal, la escasez de capacitación especializada y la necesidad de recursos humanos calificados son factores que contribuyen a estas discrepancias. La conclusión clave es la urgencia de reformar y actualizar la legislación, proporcionar formación especializada y asignar recursos adecuados para garantizar una aplicación coherente y proporcional de las sanciones en casos de delitos informáticos.

- **Interrogante 7**

La pregunta sobre la efectividad de las penas vigentes proporciona insights valiosos sobre la percepción de los profesionales del derecho en relación con la prevención de delitos informáticos en Ecuador. A continuación, se presenta un análisis basado en las respuestas de las entrevistas:

1. Limitaciones de las Penas Privativas de Libertad:

La efectividad de las penas privativas de libertad para prevenir delitos informáticos es cuestionada en varias respuestas. Se sugiere que la escasez de casos con penas de este tipo indica que su impacto no es suficiente para disuadir a los infractores.

2. Enfoque en la Prevención a través de Ciberseguridad:

La percepción general es que la efectividad radica más en la prevención a través de medidas de ciberseguridad que en las penas privativas de libertad. La escasez de casos con penas de este tipo podría indicar que la amenaza de sanciones no está siendo un factor disuasorio efectivo.

3. Necesidad de Desarrollo Normativo y Técnico:

La evaluación de la efectividad no se limita solo a la perspectiva normativa. Se destaca la importancia de desarrollar tanto la normativa como las capacidades técnicas de los operadores judiciales para abordar eficazmente los delitos informáticos.

Conclusiones:

La evaluación de la efectividad de las penas vigentes revela la necesidad de un enfoque integral para abordar la ciberdelincuencia en Ecuador. La escasa presencia de penas privativas de libertad en casos de delitos informáticos sugiere que la prevención a través de la ciberseguridad y el desarrollo normativo y técnico son aspectos cruciales. Se destaca la importancia de una estrategia que combine medidas legales y técnicas para garantizar una prevención y persecución efectivas de los delitos informáticos.

- **Interrogante 8**

La pregunta sobre la necesidad de mejoras o actualizaciones en la legislación ecuatoriana proporciona una visión crítica sobre la efectividad y la adecuación de las leyes actuales en relación con los delitos informáticos. A continuación, se presenta un análisis basado en las respuestas de las entrevistas:

1. Reconocimiento de la Necesidad de Mejoras:

Todos los entrevistados concuerdan en la necesidad de mejorar y actualizar la legislación ecuatoriana en materia de delitos informáticos. Se destaca la naturaleza cambiante y sofisticada de la ciberdelincuencia como un factor clave que exige una atención y acción más cuidadosas.

2. Adaptación a la Evolución de la Ciberdelincuencia:

Se menciona la importancia de desarrollar la legislación con mayor atención y urgencia para hacer frente a los desafíos emergentes relacionados con los delitos informáticos. La adaptación constante a la evolución de la ciberdelincuencia es considerada crucial.

3. Reformas para Abordar Desafíos Actuales:

La falta de actualización de las leyes para abordar la ciberdelincuencia en constante evolución es identificada como una causa potencial de discrepancias en las sanciones impuestas y la gravedad de las acciones perpetradas. Se destaca la necesidad de reformas legales para asegurar que las penas sean proporcionales a la gravedad de los delitos informáticos.

Conclusiones:

La percepción unánime de que la legislación ecuatoriana sobre delitos informáticos requiere mejoras y actualizaciones subraya la urgencia de abordar la ciberdelincuencia de manera más efectiva. La adaptación constante de las leyes a los cambios en la tecnología y las tácticas de los delincuentes es esencial para garantizar una respuesta legal eficiente y proporcional a los desafíos emergentes en el ámbito digital. La llamada a una revisión cuidadosa y una

actualización oportuna destaca la importancia de mantener la legislación alineada con la evolución de la ciberdelincuencia.

- **Interrogante 9**

La pregunta sobre la percepción de la comunidad legal en Ecuador acerca de cómo valora la proporcionalidad en las penas de los delitos informáticos ofrece una perspectiva valiosa sobre la opinión de los profesionales del derecho en relación con la justicia en este ámbito. A continuación, se presenta un análisis basado en las respuestas recopiladas:

1. Importancia de la Proporcionalidad:

La mayoría de los entrevistados destaca la importancia fundamental de la proporcionalidad en las penas de los delitos informáticos. Se evidencia una conciencia generalizada sobre la necesidad de que las sanciones sean proporcionadas a la gravedad de las acciones cometidas.

2. Desafíos en la Aplicación de la Proporcionalidad:

Algunos entrevistados señalan desafíos en la aplicación efectiva del principio de proporcionalidad. Factores como la rápida evolución de las tecnologías y la falta de actualización legislativa son identificados como obstáculos que pueden afectar la capacidad para imponer sanciones proporcionales.

3. Variabilidad en la Percepción:

Se observa cierta variabilidad en la percepción de la comunidad legal. Mientras que algunos abogan por una aplicación estricta de la proporcionalidad, otros reconocen la necesidad de considerar factores contextuales y circunstancias específicas de cada caso.

Conclusiones:

La percepción general dentro de la comunidad legal en Ecuador apunta a la valoración positiva de la proporcionalidad en las penas de los delitos informáticos. Sin embargo, existen desafíos prácticos que podrían afectar la

aplicación efectiva de este principio, destacando la importancia de abordar cuestiones legislativas y tecnológicas para garantizar que las sanciones sean justas y proporcionadas. La variabilidad en la percepción subraya la complejidad de encontrar un equilibrio adecuado entre la aplicación rigurosa de la proporcionalidad y la consideración de circunstancias específicas.

- **Interrogante 10**

La pregunta sobre la existencia de discrepancias por parte de los acusados o condenados por delitos informáticos proporciona una visión crucial de cómo los individuos implicados perciben las penas impuestas. A continuación, se presenta un análisis basado en las respuestas recopiladas:

1. Manifestación Frecuente de Discrepancias:

La mayoría de los entrevistados informa que es común que los acusados o condenados por delitos informáticos manifiesten discrepancias con respecto a la proporcionalidad de las penas impuestas. Este patrón sugiere que existe una percepción generalizada de que las sanciones pueden no reflejar adecuadamente la gravedad de las acciones cometidas.

2. Factores que Contribuyen:

Algunos entrevistados identifican diversos factores que contribuyen a estas discrepancias, como la falta de comprensión por parte de los acusados sobre la gravedad de sus acciones, la rápida evolución tecnológica que puede dificultar la evaluación de los delit-os y la percepción subjetiva de los afectados.

3. Necesidad de Comunicación Efectiva:

Se destaca la importancia de establecer una comunicación efectiva entre los profesionales legales y los acusados para abordar estas discrepancias. La educación sobre la gravedad de los delitos informáticos y la justificación de las penas pueden ser aspectos clave en este proceso.

Conclusiones:

La presencia común de discrepancias entre los acusados o condenados por delitos informáticos y la percepción de proporcionalidad de las penas impuestas subraya la importancia de un diálogo claro y efectivo en el proceso legal. La educación y la comprensión mutua entre las partes son esenciales para abordar estas discrepancias y garantizar que las penas sean percibidas como justas y proporcionadas.

- **Interrogante 11**

La cuestión sobre si existen discrepancias notables en la percepción de la proporcionalidad de las penas entre diferentes participantes legales, como jueces, fiscales, abogados defensores y acusados, arroja luz sobre posibles divergencias en sus perspectivas. Aquí se presenta un análisis basado en las respuestas recopiladas:

1. Divergencias entre Jueces y Acusados:

Algunos entrevistados señalan que las discrepancias más notables suelen manifestarse entre jueces y acusados. Esta diferencia puede atribuirse a la interpretación legal de los jueces, que podría parecer más severa en comparación con la percepción subjetiva de los acusados sobre la gravedad de sus acciones.

2. Rol de los Fiscales y Abogados Defensores:

Se destaca que los fiscales y abogados defensores también pueden tener perspectivas distintas, aunque estas discrepancias tienden a ser menos marcadas que las que existen entre los jueces y los acusados. El papel de los abogados defensores en explicar la posición de sus clientes es crucial en este contexto.

3. Necesidad de Claridad y Consistencia:

Varios entrevistados enfatizan la importancia de establecer pautas claras y consistentes para evaluar la proporcionalidad de las penas en casos de delitos

informáticos. Esto contribuiría a minimizar las discrepancias y a garantizar una aplicación equitativa de la ley.

Conclusiones:

La existencia de discrepancias notables en la percepción de la proporcionalidad de las penas entre distintos participantes legales, especialmente entre jueces y acusados, destaca la necesidad de un enfoque más claro y uniforme en la evaluación de estos casos. Establecer directrices claras y fomentar la comunicación efectiva entre los participantes legales puede ayudar a lograr una mayor coherencia y justicia en la aplicación de las penas por delitos informáticos.

Tabla 3

Tabla comparativa

Aspecto Legal	España	Reino Unido	Brasil	Argentina	Ecuador
Leyes Relevantes	Código Penal Español	Computer Misuse Act 1990	Ley N.º 12.737/2012 ("Ley Carolina Dieckmann")	Código Orgánico Integral Penal (COIP)	Código Orgánico Integral Penal (COIP)
Principio de Proporcionalidad	Penas proporcionales a la gravedad del delito	Penas proporcionales a la gravedad del delito	Penas proporcionales a la gravedad del delito	Penas proporcionales a la gravedad del delito	Penas proporcionales a la gravedad del delito
Tipificación de Delitos Informáticos	Acceso no autorizado a sistemas informáticos, entre otros	Acceso no autorizado a sistemas informáticos	Acceso no autorizado a sistemas informáticos, intercepta ción de datos	Acceso no autorizado a sistemas informáticos, intercepta ción de datos	Acceso no autorizado a sistemas informáticos, intercepta ción de datos
Penalidades	Multas y penas de prisión según la gravedad del delito	Multas y penas de prisión según la gravedad del delito	Multas y penas de prisión según la gravedad del delito	Multas y penas de prisión según la gravedad del delito	Multas y penas de prisión según la gravedad del delito
Agravantes o Atenuantes	Considera ción de circunstan cias específica s en cada caso	Considera ción de circunstan cias específica s en cada caso	Considera ción de circunstan cias específica s en cada caso	Considera ción de circunstan cias específica s en cada caso	Considera ción de circunstan cias específica s en cada caso

Elaborado por: Granizo, Francisco (2023)

CAPITULO IV

DISCUSIÓN

Definición Legal de Delitos Informáticos: Las entrevistas revelan un consenso en cuanto a la ubicación de los delitos informáticos en el Código Orgánico Integral Penal (COIP) de Ecuador. La claridad en la definición legal es considerada crucial, destacándose la necesidad de abordar acciones como el hacking y el acceso no consentido mediante leyes específicas de ciberseguridad. Esta base legal sólida es esencial para abordar de manera efectiva la complejidad de los delitos informáticos.

Determinación de la Gravedad de un Delito Informático: La evaluación de la gravedad de los delitos informáticos sigue un enfoque multifacético que considera el daño causado, la naturaleza del delito, la intención del perpetrador y otros factores. La falta de casos específicos en algunas experiencias profesionales puede sugerir una subrepresentación de estos delitos en el sistema legal, resaltando la importancia de una mayor conciencia y denuncia.

Ejemplos de Casos de Delitos Informáticos: Los ejemplos proporcionados, como el acceso no autorizado a información financiera y la estafa a través de métodos como el phishing, ilustran la diversidad de los delitos informáticos. Sin embargo, la ausencia de casos concretos en algunas experiencias destaca la necesidad de abordar los desafíos en la detección y denuncia de estos delitos.

Desafíos en la Investigación y Enjuiciamiento: Los desafíos en la investigación y enjuiciamiento de delitos informáticos en Ecuador son evidentes, con la falta de información, demoras en la obtención de datos de empresas extranjeras y la necesidad de colaboración público-privada. La ausencia de convenios internacionales adecuados y la falta de capacitación específica en delitos informáticos son áreas críticas que requieren atención.

Aplicación del Principio de Proporcionalidad en las Penas: La aplicación del principio de proporcionalidad en las penas destaca la importancia de considerar factores como la gravedad del delito, el daño causado y las circunstancias específicas. La necesidad de sanciones proporcionales y preventivas subraya la complejidad de abordar estos delitos de manera efectiva.

Percepción sobre la Efectividad de las Penas Actuales: La preocupación expresada sobre la efectividad de las penas actuales en disuadir delitos informáticos sugiere la necesidad de revisar y fortalecer las sanciones. La incorporación de medidas preventivas, además de penas privativas de libertad, se considera esencial para abordar el aumento de denuncias y casos.

Áreas de Mejora en la Legislación: Las entrevistas resaltan la necesidad de reformas legislativas, incluyendo definiciones más claras de delitos informáticos y sanciones proporcionales. La falta de protocolos y capacitación en investigación y peritajes informáticos es un desafío crítico que requiere atención inmediata.

Percepción de la Proporcionalidad en la Comunidad Legal: La percepción compartida de la comunidad legal destaca la necesidad de mejoras legislativas y sanciones más efectivas. La educación y conciencia ciudadana emergen como elementos cruciales para fortalecer la respuesta colectiva a los delitos informáticos.

Las entrevistas subrayan la complejidad y la urgencia de abordar los delitos informáticos en Ecuador, desde la definición legal hasta la implementación de sanciones proporcionales y la mejora de la capacidad de investigación. La colaboración entre actores públicos y privados y la actualización constante de la legislación son fundamentales en esta lucha en evolución contra la ciberdelincuencia.

Percepción de la Proporcionalidad

Percepción de la Proporcionalidad en las Penas de Delitos Informáticos:

Las respuestas recopiladas en torno a la percepción de la proporcionalidad en las penas de delitos informáticos revelan una preocupación compartida entre los entrevistados sobre la eficacia actual de las sanciones. Se destaca que, a pesar de los incrementos en las denuncias y casos, las penas existentes no parecen ser suficientemente disuasorias para los delincuentes cibernéticos. Este hallazgo sugiere que la legislación actual puede no estar alineada de manera óptima con

la complejidad y gravedad de los delitos informáticos, lo que genera la necesidad de una revisión integral.

Desacuerdo sobre la Proporcionalidad:

La existencia de situaciones en las que los acusados o condenados por delitos informáticos expresaron desacuerdo con la proporcionalidad de las penas subraya una brecha perceptual entre diferentes partes involucradas en el proceso legal. Estos desacuerdos resaltan la importancia de una interpretación clara y uniforme de la ley, así como la necesidad de que las penas reflejen de manera precisa la gravedad del delito y sus circunstancias.

Diferencias entre Actores Legales:

El reconocimiento de posibles diferencias significativas en la percepción de la proporcionalidad entre diferentes actores legales, como jueces, fiscales, abogados defensores y acusados, destaca la complejidad subyacente en la evaluación de la gravedad y las consecuencias de los delitos informáticos. Las disparidades en la interpretación de las penas pueden surgir debido a enfoques profesionales distintos y resaltan la necesidad de claridad y coherencia en la legislación.

Necesidad de Mejoras Legislativas:

Las entrevistas subrayan la percepción generalizada de que la legislación ecuatoriana relacionada con los delitos informáticos necesita mejoras. Este consenso refuerza la urgencia de reformas legales que aborden de manera específica y efectiva los desafíos actuales en la persecución y sanción de los delitos informáticos. Las áreas de mejora incluyen definiciones claras, sanciones proporcionales y procedimientos de investigación y peritaje informático bien establecidos.

Educación y Conciencia Ciudadana:

La percepción de la proporcionalidad no solo involucra a los actores legales, sino que también se extiende a la comunidad en general. La necesidad de educación y conciencia ciudadana resalta la importancia de informar al público sobre los riesgos, consecuencias y medidas preventivas relacionadas con los delitos informáticos. La participación activa de la sociedad civil puede complementar los esfuerzos legales para disuadir la ciberdelincuencia.

En conjunto, las respuestas a las preguntas sobre la percepción de la proporcionalidad en las penas de delitos informáticos enfatizan la necesidad crítica de reformas legislativas, al tiempo que subrayan la importancia de una comprensión compartida entre los diversos actores involucrados. La revisión y fortalecimiento de la legislación, combinada con esfuerzos educativos, son esenciales para garantizar una respuesta integral y efectiva frente a los desafíos en constante evolución presentados por los delitos informáticos.

Comparación

Comparación de las Respuestas entre los Profesionales de Ecuador:

Las entrevistas con profesionales del ámbito legal en Ecuador ofrecen una visión valiosa sobre la percepción y el enfoque hacia los delitos informáticos en el país. Aunque se destaca que la ciberdelincuencia es una preocupación creciente en Ecuador, las respuestas revelan diferencias notables en cuanto a la frecuencia con la que los entrevistados han tenido que lidiar con casos de delitos informáticos. La variabilidad en la experiencia puede atribuirse a la naturaleza evolutiva de estos delitos y al hecho de que algunos profesionales pueden no haberse enfrentado directamente a casos de esta índole.

Enfoque Legal y Definiciones:

En términos de enfoque legal, se observa que Ecuador ha incorporado disposiciones específicas sobre delitos informáticos en su Código Orgánico Integral Penal (COIP). Sin embargo, surge una necesidad común entre los entrevistados de mejorar y actualizar la legislación para abordar las amenazas

emergentes y la rápida evolución de la tecnología. Este hallazgo refleja una preocupación compartida en torno a la capacidad de la legislación para mantenerse al día con la sofisticación de los delitos informáticos.

Desafíos Comunes:

Las entrevistas destacan desafíos comunes en la investigación y el enjuiciamiento de delitos informáticos, incluyendo el anonimato y la ubicación de los perpetradores, los cambios tecnológicos, la falta de recursos y la necesidad de colaboración tanto a nivel nacional como internacional. Estos desafíos son consistentes con la naturaleza transnacional y compleja de la ciberdelincuencia, y subrayan la importancia de una respuesta coordinada a nivel global.

Comparación de Experiencias:

La variedad de casos mencionados, desde acceso no autorizado hasta estafas informáticas y pornografía infantil, resalta la diversidad de situaciones que enfrentan los profesionales legales en Ecuador. Esta variedad refleja la amplia gama de delitos informáticos que pueden ocurrir en el país y destaca la importancia de un enfoque legal que pueda adaptarse a diferentes escenarios.

Proporcionalidad de las Penas:

En cuanto a la percepción de la proporcionalidad de las penas, se observa una preocupación generalizada sobre la efectividad de las sanciones actuales para disuadir los delitos informáticos. Esta inquietud se presenta como un tema común entre los profesionales, indicando la necesidad de una revisión de las penas para garantizar que sean proporcionales a la gravedad de los delitos cometidos.

En general, las entrevistas resaltan la importancia de fortalecer las capacidades legales y la legislación en Ecuador para hacer frente a la ciberdelincuencia. La comparación de respuestas revela una convergencia en las áreas que requieren mejoras, incluyendo la legislación, la colaboración internacional y la conciencia ciudadana. Estos hallazgos sugieren que, aunque los profesionales en Ecuador están enfrentando los desafíos de los delitos informáticos, existe una conciencia compartida sobre la necesidad de una respuesta más efectiva y coordinada.

CONCLUSIONES

Tras examinar la legislación ecuatoriana vinculada a los delitos de hacking y acceso no consentido a sistemas informáticos, queda claro que el Código Orgánico Integral Penal (COIP) aborda estas conductas con disposiciones específicas. Sin embargo, durante este análisis, surge la necesidad evidente de revisar y mejorar ciertos aspectos de la legislación, tales como definiciones más precisas y sanciones proporcionadas.

Al evaluar los criterios utilizados por el sistema legal ecuatoriano para determinar las penas en casos de delitos informáticos, se destaca la importancia asignada al daño causado, las circunstancias particulares y la magnitud del delito. No obstante, se observa con preocupación una posible falta de aplicación del principio de proporcionalidad en estas penas, lo que plantea interrogantes sobre su coherencia y justicia.

La limitada aplicación de la proporcionalidad podría tener raíces en diversos obstáculos, como la carencia de precedentes, la falta de conocimientos técnico-jurídicos y la veloz evolución tecnológica. Estos desafíos subrayan la necesidad urgente de una capacitación más extensa y una actualización constante en el ámbito legal para afrontar las complejidades inherentes a los delitos informáticos.

En este contexto, se propone una revisión completa de la legislación, con especial énfasis en la definición y clasificación de los delitos informáticos, la proporcionalidad en las penas y la promoción de una colaboración más estrecha entre los sectores público y privado. La adaptación continua a los avances tecnológicos y la sensibilización sobre la gravedad de los delitos informáticos son elementos cruciales para fortalecer el sistema legal ecuatoriano en este ámbito.

RECOMENDACIONES

Es imperativo llevar a cabo una revisión exhaustiva de la legislación relacionada con los delitos informáticos en Ecuador. En este sentido, la atención debe centrarse en la claridad de las definiciones y la adecuación de las sanciones. Es esencial asegurarse de que las disposiciones legales reflejen con precisión la gravedad de las acciones, evitando ambigüedades que puedan dar lugar a interpretaciones erróneas, la actualización constante de la legislación debería ser un proceso continuo para adaptarse a la evolución constante de las amenazas informáticas.

Se debe fomentar la aplicación efectiva del principio de proporcionalidad en la determinación de penas para delitos informáticos. En este sentido, es importante proporcionar capacitación especializada a los profesionales del sistema legal ecuatoriano, incluyendo jueces y fiscales. Esta formación sería fundamental para garantizar una comprensión completa de las complejidades técnicas y jurídicas asociadas con estos delitos. Además, se sugiere la posibilidad de implementar directrices claras que orienten la aplicación del principio de proporcionalidad en casos específicos.

Dada la rápida evolución tecnológica, sería beneficioso establecer programas de formación continua para los profesionales del ámbito legal. Este enfoque incluiría la capacitación en las últimas tendencias y tecnologías relacionadas con los delitos informáticos, al mantenerse actualizados, los expertos legales estarán mejor preparados para abordar los desafíos tecnológicos y aplicar de manera efectiva la legislación.

Insto a fortalecer la colaboración entre los sectores público y privado en la lucha contra los delitos informáticos. Establecer canales de comunicación más efectivos y compartir información de manera segura puede mejorar significativamente la capacidad de investigación y enjuiciamiento. La participación activa de la industria tecnológica y las empresas en la creación de estrategias y políticas también la considero esencial desde mi punto de vista.

BIBLIOGRAFÍA

Alanya, M. (2022). Inseguridad informática y delitos informáticos del usuario fiscalía provincial penal corporativa de Huancayo 2019.

Amores, L. (2022). La falta de tipificación del delito informático “sexting” dentro del COIP y su vulneración a los derechos de la dignidad humana e intimidad en el ecuador.

Atienza, G., & Fernández, D. (2020). Ciberdelitos. *Ediciones Experiencia*.

Branca, R. (2023). La protección legal de los hackers éticos: una mirada desde el derecho penal.

Burgos, A., & Medina, R. (2022). La incidencia digital en las redes sociales de la ciudad de Guayaquil. *ULVR*.

Cabezas, M. (2019). Tipicidad ciberbullyng como delito en el Código Orgánico Integral Penal.

Caisaguano, D. (2023). plicación de seguridad en CLOUD computing, para la protección de servicios de administración de devops y claves SSH de acceso a dispositivos de red en una Empresa de Telecomunicaciones ubicada en la Ciudad de Guayaquil. *Universidad de Guayaquil*.

Couso, J. (2018). Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores. *Revista de derecho (Coquimbo)*, 29-76.

Cuenca, H. (2022). Articulación de la Fiscalía General del Estado para la persecución de delitos cibernéticos.

Flores, I. (2019). Criminalidad informática: aspectos sustantivos y procesales. *Criminalidad informática*, 1-438.

García, B. (2022). La investigación penal ante las nuevas tecnologías: reflexiones acerca de la «carga desproporcionada» y la «facilitación de información» en el registro de dispositivos de almacenamiento masivo de datos. *Anuario de Derecho Penal y Ciencias Penales*.

Gavilán, E. (2016). Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems. *Revista de Derecho Comunitario Europeo* , 261-282.

Guamán, C. (2023). Estudio jurídico del artículo 190 del código orgánico integral penal sobre la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura. *Pontificia Universidad Católica del Ecuador Ibarra*.

Martínez, M. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*.

Montserrat, M. (2018). El delito de acceso ílicito a un sistema informático.

Ramos, J. (2019). Ciberdelincuencia en la Legislación Penal Ecuatoriana-propuesta de reforma al Código Orgánico Integral Penal. *UCE*.

Rodríguez, J. (2020). Una aproximación al delito de estafa en sus modalidades clásica e informática: De la estafa tradicional a las nuevas modalidades como el Phishing.

Rodríguez, V. (2022). Consecuencias jurídicas y revictimización en las jóvenes víctimas del delito de difusión ilícita de imágenes íntimas en el municipio de San Luis Potosí.

Rúa, M. (2023). Cibercriminalidad e investigación penal tecnológica: una mirada desde la experiencia de la Cooperación Internacional para la persecución de la cibercriminalidad en Latinoamérica. *Palestra Editores*.

Saltos, H. (2022). Abordaje de la prevención del delito cibernético y el derecho a la intimidad en Ecuador. *Universidad Metropolitana*.

Salvadori, I. (2019). ncriminación de programas informáticos ‘de doble uso’y técnicas de anticipación de la tutela penal. *REVISTA DERECHO PENAL CONTEMPORÁNEO*, 117-169.

Sanmartín, W. (2021). Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest. *UCE*.

Saraguro, A. (2021). La debilidad del proceso investigativo de los delitos informático.

Serra, R. (2017). Contraterrorismo: plasmación legislativa reciente e impacto en las libertades y derechos fundamentales. *Cuadernos de estrategia*, 121-180.

Sinchiguano, J. (2022). Las acciones típicas de desarrollo y comercialización de programas informáticos, para el cometimiento del delito de acceso no consentido a un sistema de información y comunicación. *UCE*.

Sinchiguano, L. (2018). os delitos informáticos que afectan a los usuarios del Sistema Nacional de Contratación Pública.

Soler, B. (2023). elitos Cibernéticos: Amenazas Digitales del Siglo XXI: Análisis normativo, psicológico y criminológico. *ARANZADI/CIVITAS*.

Vaca, M. (2019). Tipicidad ciberbullyng como delito en el Código Orgánico Integral Penal.

ANEXOS

Modelo de entrevistas

Modelo de Entrevista para Abogados

Introducción:

- Saludo y agradecimiento por la participación en la entrevista.
- Explicación del propósito de la investigación y del consentimiento informado.
- Asegurar la confidencialidad de las respuestas.

Información Demográfica:

Nombre y cargo actual: _____

Experiencia profesional en el campo legal: _____

Especialización o experiencia previa en casos de delitos informáticos: _____

Preguntas sobre Delitos Informáticos:

1. De acuerdo con su criterio, ¿Cuál sería la definición legal más adecuada para los delitos de hacking y acceso no consentido a sistemas informáticos en Ecuador?
2. Desde su experiencia y de acuerdo a su criterio, ¿Cuál sería la importancia que le da la legislación ecuatoriana sobre la gravedad de un delito informático en el sistema legal ecuatoriano?
3. Desde su experiencia, ¿Ha conocido o llevado algún caso de delitos informáticos?

4. En su opinión, ¿Qué desafíos se presentan durante la investigación y el enjuiciamiento de delitos informáticos?

5. Desde esta línea de ideas, ¿Qué criterios y factores se consideran al aplicar el principio de proporcionalidad en las penas de delitos informáticos?

6. ¿Ha notado discrepancias entre las penas impuestas en casos de delitos informáticos y la gravedad de los mismos?

7. ¿Cómo evalúa usted la efectividad de las penas vigentes para prevenir los delitos informáticos en el Ecuador?

8. ¿Considera que hay aspectos específicos en la legislación ecuatoriana sobre delitos informáticos que requieran mejoras o actualizaciones?

Preguntas sobre la Percepción de la Proporcionalidad:

9. ¿Cuál es su percepción acerca de cómo la comunidad legal en el ecuador valora la proporcionalidad en las penas de los delitos informáticos?

10. ¿Ha experimentado situaciones en las que los acusados o condenados por delitos informáticos han expresado su desacuerdo con la proporcionalidad de las penas?

11. ¿Existe una diferencia significativa en la percepción de la proporcionalidad entre los diferentes actores legales, como jueces, fiscales, abogados defensores y acusados?

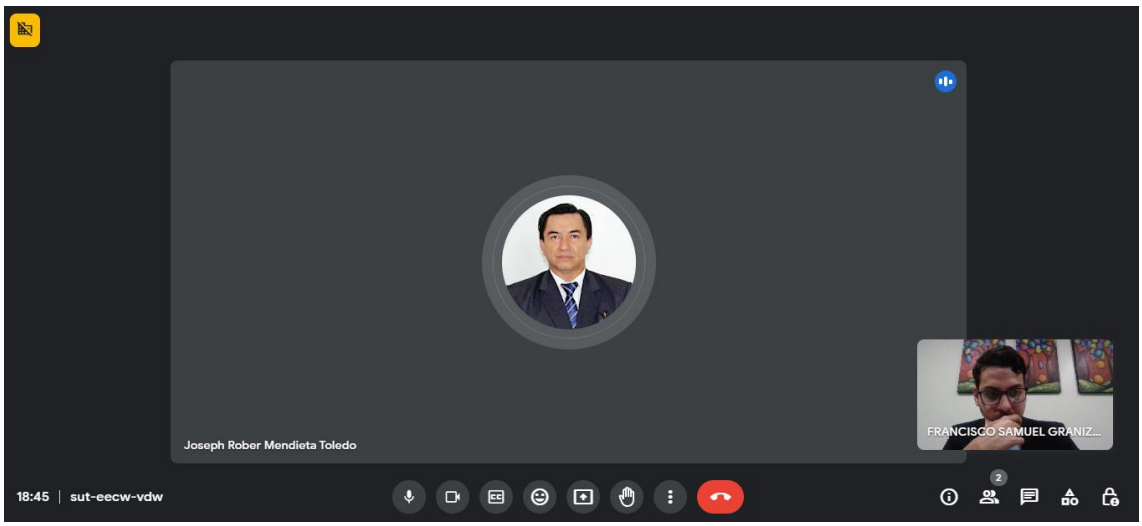
Conclusión:

Agradecimiento por su tiempo y participación.

Oportunidad para que el entrevistado comparta cualquier información adicional relevante.

Evidencia de entrevistas

Figura 1 Entrevista - Abogado Jhon Velásquez

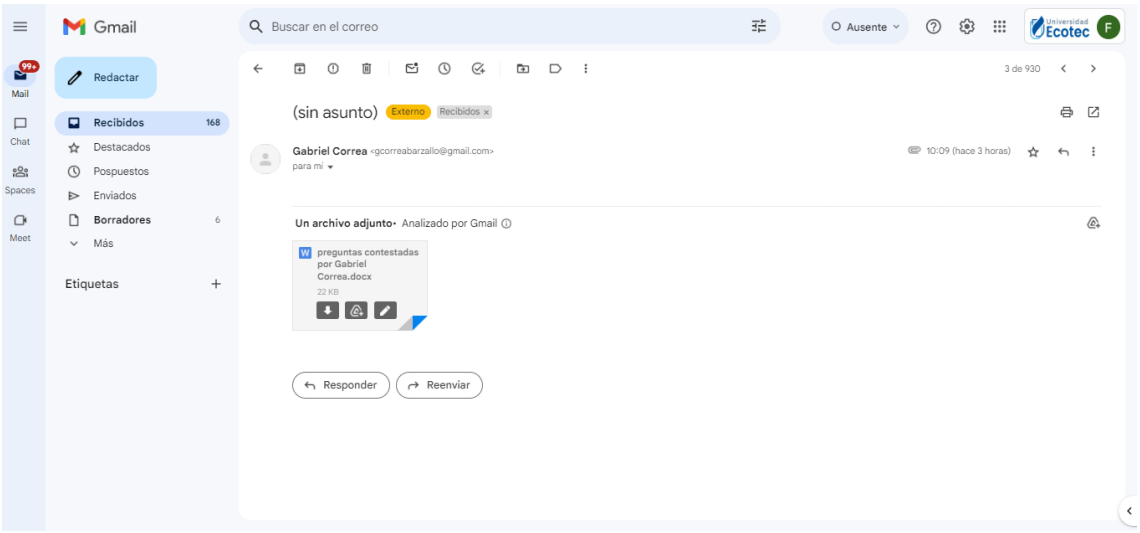


Fuente: entrevista a expertos

Figura 2 Entrevista - Abogado David Vergara

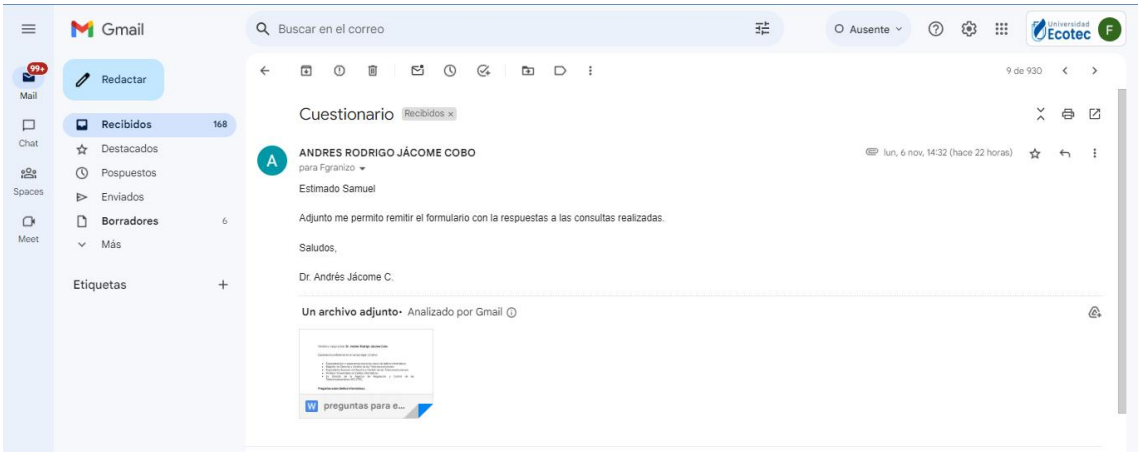
Fuente: entrevista a expertos

Figura 3 Entrevista – Abogado Gabriel Correa



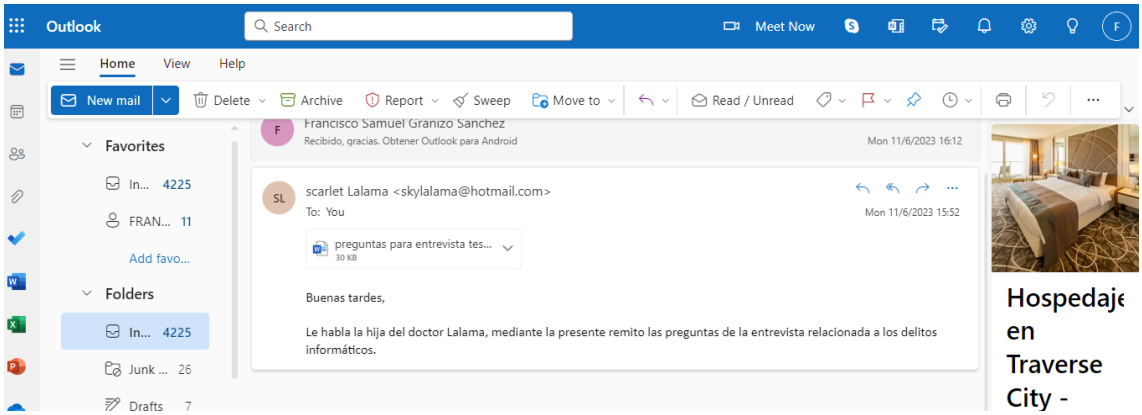
Fuente: entrevista a expertos

Figura 4 Entrevista - Abogado Andrés Jácome



Fuente: entrevista a expertos

Figura 5 Entrevista - Abogado Fernando Lalama



Fuente: entrevista a expertos