Universidad Ecotec

Facultad de Derecho y Gobernabilidad

Título del trabajo:

La ciberdelincuencia dentro de la Legislación Penal Ecuatoriana y el bloque de constitucionalidad durante los años del 2020 al 2024.

Carrera:

Derecho con Énfasis en Ciencias Penales y Criminológicas

Autores:

Amy Pamela Macias Guerrero

Andres Francisco Tenenuela Gonzalez

Tutor (a):

Abg. Jose Luis Sanchez

Samborondón, Ecuador

2024

RESUMEN

Este estudio se centra en la situación de Ecuador en el ámbito de la ciberdelincuencia y ciberseguridad ha como se enfrenta el país a la creciente amenaza del ciberdelito dentro del marco legal del país, así mismo se analiza cómo el sistema judicial ecuatoriano puede incluirse en el Convenio Internacional de Budapest para combatir los delitos informáticos, destacando las fortalezas y debilidades del marco legal ecuatoriano junto con ello el estudio de casos relacionados a estos delitos para su respectivo análisis, el estudio incluye entrevistas con fiscales especializados en ciberdelincuencia dentro de Guayaquil para ofrecer una perspectiva experta sobre los desafíos y avances en la lucha contra la ciberdelincuencia en el país.

ABSTRACT

This study focuses on the situation in Ecuador in the field of cybercrime and cybersecurity, how the country faces the growing threat of cybercrime within the country's legal framework, and how the Ecuadorian judicial system can be included in the Convention is also analyzed. Budapest International to combat computer crimes, highlighting the strengths and weaknesses of the Ecuadorian legal framework along with the study of cases related to these crimes for their respective analysis, the study includes interviews with prosecutors specialized in cybercrime within Guayaquil to offer a perspective expert on the challenges and advances in the fight against cybercrime in the country.

Dedicatoria:

De Amy:

En primer lugar, quiero expresar mi más profundo agradecimiento a mis padres, quienes han sido el pilar fundamental en mi vida, contando con su apoyo incondicional a lo largo de mi carrera universitaria, sus palabras de aliento en los momentos difíciles y su guía constante han sido esenciales para convertirme en la mujer que soy hoy en día.

A mis hermanos, quienes han estado a mi lado en esas largas noches de estudio y tareas, les debo más de lo que las palabras pueden expresar, sin su apoyo y compañía, no habría alcanzado las metas que hoy celebro con tanto orgullo, a mis perritos Murphy y Molly por acompañarme en las madrugadas y esperarme para irme a dormir.

De Andres:

Este logro se pudo alcanzar gracias al apoyo de todas esas personas quienes estuvieron alentando hasta el final, a mis padres quienes fueron mi guía y mi pilar para conseguir este logro, a mi hermana quien con sus palabras me alentaron a seguir adelante, a mi difunta nana quien desde antes de su fallecimiento esperaba verme cumpliento este sueño y ahora desde el otro lado podrá verme cumplirlo y finalmente a mis perros quienes me acompañaron en las madrugadas de tareas y estudios.

Agradecimientos:

De Amy:

Principalmente agradezco a mi familia quienes me han demostrado todo su apoyo a lo largo de mi carrera universitaria, por no dejar que nunca me sienta fuera de lugar en mi carrera y aconsejarme de la mejor manera siempre.

Agradezco de corazón a mis amigos, quienes ocupan un lugar muy especial en mi vida: Elena, Barbara, Gustavo, Doménica, Allison y Gianella, quienes han convertido esta etapa en una experiencia inolvidable, llenándola de alegría y emociones, demostrando su apoyo, en esa forma tan única que solo ellos conocen y han hecho que cada momento sea más significativo,sin ellos, este camino no habría sido el mismo.

Agradezco a mi tutor por guiarme durante toda la tesis, a los grandes profesionales por sus gratas experiencia y conocimientos compartidos, a mi compañero de tesis Andrés por acompañarme durante esta bonita experiencia, gracias por ser mi amigo y un gran compañero, por último agradezco a aquella persona que ha hecho mi vida mucho más bonita desde que llegó, gracias por apoyarme en etapa tan significativa.

De Andres:

Agradezco firmemente a toda mi familia desde la costa hasta la sierra pues ellos siempre me alentaban e inspiraban a cumplir con esta meta de vida, por alentarme aun en mis momentos más bajos a seguir con este camino y a tolerar a mi persona en todas los momentos en los que estuve bajo el estrés.

También agradezco a todos mis amigos ya sea dentro de la universidad como fuera de esta quienes a su manera me apoyaron incondicionalmente con especial mención a mi compañera Amy quien fue una excelente compañera de tesis y que sin su ayuda no podría terminar esta tesis, además de agradecer a todos ellos a los que quedaron como meros

conocidos que por medio de sus vivencias y consejos lograron infundir en mi persona para ser lo que soy ahora.

Finalmente a todos los docentes quienes con sus clases no solo me inculcaron el conocimiento que se me fue infundido sino también que con su ayuda y palabras de aliento lograron ayudarme a ser lo que soy ahora con especial honor a mi tutor quien supo guiarnos durante todo el desarrollo de la tesis corrigiendonos y ayudándonos a mejorar para cumplir con este nuestro última “Tarea” antes de ser profesionales.

Indice de contenido:

Introducción

La ciberdelincuencia representa una amenaza creciente y multifacética en el siglo XXI, la rápida evolución tecnológica y la expansión global de internet han proporcionado nuevas oportunidades para la delincuencia, que ahora puede operar en un entorno virtual que frecuentemente supera las fronteras físicas y jurídicas tradicionales desafiando la capacidad de los sistemas de justicia penal para adaptarse y responder eficazmente, generando la necesidad de reevaluar y fortalecer los marcos legales existentes.

Para entender mejor la ciberdelincuencia, es necesario comenzar por definir y conceptualizarla, abordando sus múltiples manifestaciones y los desafíos específicos que plantea.

Este fenómeno no se limita a delitos convencionales trasplantados al ciberespacio, sino que abarca nuevas formas de criminalidad, como el ransomware, el phishing y los ataques a infraestructuras críticas, estas actividades delictivas pueden tener consecuencias devastadoras, no solo económicas sino también sociales y políticas, afectando desde individuos hasta estados enteros.

En el contexto actual, donde la tecnología digital y la conectividad son elementos fundamentales de la vida cotidiana y las transacciones comerciales, influyendo así, su rápido desarrollo en beneficio de la sociedad ecuatoriana, por lo cual la legislación penal y el bloque de constitucionalidad deben enfrentar el desafío de definir y delimitar adecuadamente los actos de ciberdelincuencia para garantizar una respuesta jurídica efectiva.

Es por eso que en esta investigación se analiza la importancia jurídica de la ciberdelincuencia dentro de la Legislación Penal Ecuatoriana y el bloque de

constitucionalidad, considerando casos específicos relacionados a los ciberdelitos infringidos a nivel nacional e internacional entre los años 2020-2024.

Esta investigación es importante ya que radica en la necesidad urgente de actualizar y reforzar el marco legal para prevenir, investigar y sancionar de manera eficaz los ciberdelitos; la ciberdelincuencia no solo tiene el potencial de "causar pérdidas económicas cuantiosas", sino que también amenaza la seguridad nacional, la privacidad individual y la integridad de infraestructuras críticas (Thomas, 2020). Dado el carácter transnacional de muchos de estos delitos, es esencial que las leyes nacionales se armonicen con los tratados y convenios internacionales pertinentes, como el Convenio de Budapest sobre Ciberdelincuencia, que establece un marco integral para la cooperación internacional en la lucha contra estos delitos.

El Convenio de Budapest es un instrumento clave en este contexto, ya que proporciona directrices y estándares internacionales para la criminalización de actos de ciberdelincuencia, así como para la cooperación internacional en su combate . Por su parte el tratado ha sido adoptado por numerosos países como un marco de referencia para desarrollar sus propias legislaciones y políticas en materia de ciberdelincuencia, facilitando así la cooperación y coordinación global en la lucha contra estos delitos.

A través del análisis de casos específicos de ciberdelincuencia ocurridos en el período de estudio, se ilustran los desafíos prácticos que enfrentan los sistemas de justicia y se destacan las respuestas jurídicas que se han implementado considerando que los casos abarcan una variedad de delitos, desde el fraude en línea hasta el robo de identidad y los ataques a sistemas críticos.

El análisis de estos ejemplos no solo proporciona una visión de los métodos y técnicas utilizadas por los ciberdelincuentes, sino también de las estrategias y herramientas

empleadas por las autoridades para combatirlos; específicamente realizar un examen detallado de la legislación penal y constitucional ecuatoriana revelarà su capacidad para enfrentar la ciberdelincuencia, identificando áreas de fortaleza y debilidad, y proponiendo recomendaciones para su mejora .

Este análisis incluye la revisión de leyes existentes, la identificación de lagunas legales y la propuesta de reformas necesarias para fortalecer la respuesta del país frente a la ciberdelincuencia. Asimismo, se considera la importancia de la formación y capacitación continua de los operadores de justicia y la implementación de tecnologías avanzadas para la detección y prevención de ciberdelitos.

Se aspira a contribuir al entendimiento y fortalecimiento de la capacidad del Estado ecuatoriano para prevenir y combatir eficazmente la ciberdelincuencia, protegiendo así a sus ciudadanos y garantizando la seguridad en el ciberespacio.

Al proporcionar un análisis detallado y contextualizado, esta investigación busca ofrecer una base sólida para la formulación de políticas públicas y reformas legislativas que respondan a los desafíos contemporáneos de la ciberdelincuencia, además, pretende fomentar una mayor colaboración internacional, reconociendo que la lucha contra la ciberdelincuencia requiere de esfuerzos conjuntos y coordinados a nivel global.

Este período ha sido testigo de un incremento significativo en la incidencia de ciberdelitos, impulsado en parte por la pandemia de COVID-19, que provocó un desplazamiento masivo hacia las actividades en línea.

Planteamiento del Problema

La rápida evolución de las tecnologías de la información y su amplio alcance han permitido que los delincuentes cometan delitos en el ciberespacio, muchas veces superando el marco

legal existente llegando a afectar incluso a nivel internacional, a causa de la falta de claridad y especificidad en las leyes actuales siendo esta la raíz de la necesidad actual.

Ahora bien la omisión legal deja lagunas en la protección de la privacidad en línea y dificulta el procesamiento de los infractores, lo que afecta negativamente las vidas de las víctimas y socava la confianza en el sistema legal, siendo así que la necesidad radica en adecuar la legislación ecuatoriana para garantizar la protección de derechos individuales en el ámbito digital con el bloque de constitucionalidad.

Para alcanzar una situación óptima, es esencial reconocer el constante desarrollo de los delitos cibernéticos asimismo prevenir el surgimiento de nuevas amenazas mediante una definición jurídica precisa y exhaustiva que abarque sus diversas modalidades, así como los medios para su identificación y persecución.

La incorporación de nuestro país al Convenio de Budapest también sería beneficiosa, ya que este tratado proporciona una ventaja significativa en la tipificación de estos delitos y en la gestión de la extradición, en consonancia con la práctica de muchos países de Latinoamérica.

Aunque existen estudios generales sobre ciberseguridad así como de legislación penal en la región, se observa una carencia de investigaciones específicas que aborden la delimitación jurídica de estos delitos por lo tanto se espera que, como resultado, consiga lograr una delimitación tanto clara como precisa de los ciberdelitos, fortaleciendo así la capacidad del sistema judicial para una persecución efectiva.

Además, un análisis detallado de los delitos tipificados en el Código Orgánico Integral Penal (COIP) y su comparación con los delitos del Convenio de Budapest permitirá evaluar la factibilidad de que Ecuador se adhiera a dicho convenio, asegurando la equivalencia en la

tipificación de delitos, con cual el objetivo se alcanzará mediante un análisis minucioso de la legislación vigente en la normativa ecuatoriana junto con el examen de convenios internacionales sobre ciberdelitos, así como la consulta con expertos jurídicos en el área de delitos electrónicos.

La pregunta que desarrolla el problema y que se plantea para resolver en este trabajo de investigación es: ¿Cómo puede reforzarse el marco legal penal y constitucional respecto a los ciberdelitos en el ámbito nacional e internacional?

Objetivo General

Analizar la importancia jurídica de la ciberdelincuencia dentro de la Legislación Penal Ecuatoriana y el bloque de constitucionalidad, considerando casos específicos relacionados a los ciberdelitos infringidos a nivel nacional e internacional entre los años 2020-2024.

Objetivos Específicos

- Identificar la legislación actual relacionada a la ciberdelincuencia sobre la protección de datos como en los delitos tipificados

- Comparar los tipos penales sobre ciberdelincuencia en las normativa ecuatoriana con el convenio internacional de ciberdelincuencia de Budapest

- Examinar sentencias judiciales en casos específicos de ciberdelincuencia ocurridos en Ecuador durante el periodo 2020 a 2024.

Justificación

La presente investigación es relevante debido a la evolución de la tecnología la cual es de carácter constante puesto que siempre está cambiando y mejorando en la mayoría de casos para el beneficio de la sociedad humana, sin embargo, existen aquellos que la utilizan para afectar a las demás personas así mismo como al ambiente en el que se concentran estas interacciones siendo el conocido ciberespacio. (Hernandez, 2014)

Para la legislación del Estado de Argentina se establece que el ciberespacio es como un ambiente complejo resultante de la interacción de las personas, el software y los servicios de internet utilizando como medio de interacción el uso de las redes de los dispositivos conectados a esta red. (Rosas, 2024)

Por lo que el ciberespacio se funda como la estructura primordial de la comunicación virtual por medio de mensajes de datos los cuales están ligados a cada uno de los usuarios lo que consiste en un nuevo bien jurídico que proteger.

Es por ello que es necesario tener asegurado la disponibilidad, integridad, confidencialidad, y la capacidad de las tecnologías de la información ya sea el uso de hardware como las computadoras, el smartphone como el software dado por los programas dentro de la red global del internet.

Junto con el crecimiento exponencial de la tecnología que ha llevado consigo un aumento significativo de amenazas cibernéticas las cuales trascienden las capacidades de la legislación ecuatoriana existente.

En primer lugar, la definición precisa de la ciberdelincuencia permitirá una persecución más efectiva de estos delitos, proporcionando a las autoridades judiciales las herramientas necesarias para afrontar las complejidades tecnológicas asociadas a estos actos ilícitos.

Además, al incluir la perspectiva del bloque de constitucionalidad se fortalecerán las garantías de derechos fundamentales, protegiendo la privacidad y la seguridad de los ciudadanos en el entorno digital.

Por lo que es un paso fundamental para llenar las lagunas legales, proporcionando claridad conceptual y normativa en torno a la ciberdelincuencia, los beneficios derivados de los resultados de esta investigación serán significativos y se traducirán en mejoras concretas tanto para la sociedad ecuatoriana como para el sistema legal, también aportará beneficios tangibles al ámbito empresarial, al facilitar la creación de estrategias de ciberseguridad más robustas y adecuadas a la legislación actualizada.

1.- Marco Teórico

1.1- Ciberdelincuencia

1.1.1.- Antecedentes

El avance de la tecnología tanto en telecomunicaciones como en la informática ha representado un avance indiscutible para la humanidad en diversas áreas, como la comunicación, el trabajo, los estudios, la medicina y lo que es el comercio considerando que han cambiado, aportando beneficios significativos para el desarrollo económico, cultural y social, el uso frecuente de esta ha generado una transformación en la sociedad la cual es muy comparable a la de la Revolución Industrial puesto dentro de aquella época se mejoró mucho las actividades agrícolas facilitando gradualmente la comunicación entre las comunidades, es por esto que en efecto la tecnología está alterando la manera en que las personas llevan a cabo sus actividades cotidianas. (JUCA MALDONADO & MEDINA PEÑA, 2023, 326-327)

La humanidad se encuentra en una etapa histórica donde para las generaciones recientes, es inimaginable vivir sin tecnología, es por eso que la diferencia en el impacto tecnológico entre generaciones se evidencia en la habilidad para manejar estas herramientas aunque los baby boomers y la Generación X se han ido adaptando a la tecnología gradualmente a lo largo de sus vidas, los millennials, la Generación Z y la Generación Alpha han estado rodeados de un entorno digital desde su infancia, lo cual se refleja en sus distintos hábitos de consumo y uso de las tecnologías, no obstante, a medida que crece el uso de la tecnología, también aumentan los métodos para emplearla con fines dañinos o moralmente cuestionables. (GALAN GUIZADO, 2023)

Por lo tanto el avance en la creación de aplicaciones y sitios web para diversas actividades, junto con el acceso casi irrastreable y anónimo, han llevado a las instituciones de control, tanto nacionales como internacionales, a implementar nuevas normas, reglamentos, estatutos y tratados para regular su uso, de igual manera esto ha tenido un impacto significativo en la delincuencia cibernética en las redes sociales a nivel global, incluyendo dentro del Ecuador, en base a que las redes sociales proporcionan información personal valiosa que los ciberdelincuentes pueden utilizar para sus actividades ilegales, es por ello que es esencial implementar medidas efectivas para proteger a los usuarios y prevenir la delincuencia cibernética en Ecuador, además la detección temprana de tendencias emergentes en la delincuencia cibernética en las redes sociales permite a las autoridades actuar rápidamente para evitar que estas tendencias se conviertan en problemas mayores. (Macias Lara, 2022, 232-233)

Al mismo tiempo que surgen nuevas innovaciones tecnológicas, grupos delictivos aprovechan esta oportunidad, así como la falta de conocimiento sobre delitos informáticos entre los nuevos usuarios que ingresan a la red a diario para cometer actos delictivos.

1.1.2.- Definición

En cuanto a la definición de la ciberdelincuencia esta se refiere a cualquier actividad ilegal llevada a cabo mediante el uso de tecnología, es decir que se la considera como uno de los delitos transnacionales de más rápido crecimiento a los que se enfrentan los países miembros de Interpol, puesto que la rápida evolución de Internet y la tecnología informática han permitido el crecimiento económico y social, además de generar una mayor dependencia de Internet originando más riesgos y vulnerabilidades para nuevas posibilidades de actividades delictivas. (INTERPOL, 2024)

Como expresa JAVIER CHINCHILLA MORALES en su artículo científico “La ciberdelincuencia es toda aquella actividad que a través de un sistema informático o por medio de una red de comunicaciones que tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos” (CHINCHILLA MORALES, 2021)

Otra conceptualización que se le da a la ciberdelincuencia es que es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito. (Lenguaje Juridico.com, 2024)

1.1.3.- Las amenazas a la red y el efecto pandemia.

En relación con los grandes avances de la tecnología en la última década se han desarrollo nuevos grupos delictivos los cuales se dirigen completamente a atacar el ciberespacio, buscando la manera de aprovechar los beneficios que dan las redes informáticas al poder ingresar desde pestañas en incógnita o diferentes equipos camuflando de esta manera sus

pasos delictivos y siendo más fácil para estos delincuentes el no dejar rastro de sus crímenes.

Por esta razón es que utilizan esta transformación digital para atacar redes, infraestructuras y sistemas informáticos a través de sus puntos débiles, además de que se tiene un impacto económico y social significativo en todo el mundo, afectando a gobiernos, empresas y particulares dado que buscan en su mayoría arremeter contra las grandes instuticiones.

Los ciberdelitos no tienen fronteras teniendo en cuenta que el internet es un mundo amplio es por esto que tanto los delincuentes como las víctimas y las infraestructuras técnicas se encuentran dispersos por múltiples jurisdicciones, lo que hace más complicado las investigaciones y la toma de acciones legales; estos delitos engloban una serie de actividades criminales que los distintos países intentan encasillar dentro de figuras delictivas tradicionales, como robos, hurtos, fraudes, falsificaciones, estafas, perjuicios, sabotajes, entre otros, pero llevados a cabo mediante el uso de sistemas informáticos. (Solano Gutiérrez, 2023, 1139-1140)

Las cuatro amenazas más comunes asociadas a la ciberdelincuencia se pueden clasificar de la siguiente manera:

- Estafas informáticas: Son aquellas acciones engañosas que causan un desplazamiento patrimonial en perjuicio de la víctima, con el fin de obtener ganancias, es por ello que la diferencia principal con una estafa convencional es que el engaño se realiza a través de sistemas informáticos, lo que confunde a la víctima. (CHINCHILLA MORALES, 2021)

- Delitos informáticos de daños: Son aquellos que consisten en borrar, compartir, dañar, alterar o suprimir datos informáticos sin autorización de la víctima, mediante

sus datos la cual acapara consecuencias perjudiciales para quien sea el afectado, así mismo es importante de resaltar que no se requiere una cantidad mínima para que se considere cometido el delito y se imponga una condena. (CHINCHILLA MORALES, 2021)

- Defraudaciones de telecomunicaciones: Se refieren a situaciones donde se causa un perjuicio económico al acceder ilícitamente a servicios de comunicación, como el uso no autorizado de una red Wi-Fi ajena. (CHINCHILLA MORALES, 2021)

- Ciberdelitos contra la intimidad: Son aquellos a los que se definen como el acto delictivo donde se involucran casos en los que se instala un software en un dispositivo sin autorización para acceder a información personal del propietario, esto puede constituir un delito de descubrimiento y revelación de secretos, con penas que son significativas. (CHINCHILLA MORALES, 2021)

Hay que hacer notar que la pandemia del COVID-19 ha tenido un impacto negativo en el ámbito de la ciberseguridad a nivel mundial en vista que durante este período se han llevado a cabo nuevas y diversas modalidades con respecto a la ciberdelincuencia por lo que se menciona que esta evoluciona a medida que aumenta el número de usuarios, lo cual refleja un incremento tanto en la cantidad como en la diversidad de modalidades delictivas en el ámbito digital.

Es por esto que Ecuador no ha sido ajeno a esta problemática; de hecho, los delitos informáticos han experimentado un aumento durante la emergencia sanitaria trayendo consecuencias negativas dentro del país. (Zambrano Rendón, 2022)

1.1.4 .- Delitos informáticos en la legislación ecuatoriana

En el Ecuador los delitos informáticos como tal aparecen tipificados por primera vez en el año 2002, mediante el Suplemento del Registro Oficial 557 en la Ley de Comercio Electrónico, Firmas y Mensajes de Texto, en donde dio paso a una reforma en el Código Orgánico Integral Penal actual donde se incluyen 5 tipos de delitos informáticos: delitos contra la información protegida, obtención y utilización no autorizada de la información, destrucción maliciosa de documentos electrónicos, falsificación electrónica, daños informáticos y la estafa informática

Desde su inclusión en el Código Orgánico Integral Penal, los delitos informáticos han sido objeto de sanción, no obstante, desde el año 2009 hasta la fecha actual, es posible que persistan actividades delictivas en el ámbito digital que aún no estén definidas y tipificadas como delitos informáticos, lo que resulta en lo que comúnmente se conoce como "vacíos legales" y son estos vacíos legales los que dificultan la capacidad de las autoridades para combatir eficazmente estos crímenes en el entorno digital.

Entre los delitos informáticos establecidos en Ecuador, se encuentran aquellos que afectan la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, como el acceso ilícito, el espionaje de datos, la intervención ilícita, la manipulación de datos y los ataques contra la integridad del sistema, asi mismo, también se incluyen delitos relacionados con el contenido, como la distribución de material erótico o pornográfico como por ejemplo la pornografía infantil, así como delitos relacionados con el discurso de odio, como el racismo y el lenguaje ofensivo. (Yagos Estrada & Pilamunga Tigllán, 2023)

En el Estado ecuatoriano, existen ciberdelitos que son reconocidos, tipificados y sancionados adecuadamente, esto ha permitido que estos delitos no queden en la impunidad y que las víctimas puedan obtener justicia, sin embargo, las sanciones no son lo

suficientemente graves como para que los ciberdelincuentes reduzcan sus actividades ilícitas, en base a lo expuesto encontramos dentro de la normativa vigente penal en Ecuador, el cual es el Código Orgánico Integral Penal los siguientes ciberdelitos más importantes:

Art. 178.- Violación a la intimidad.- El presente artículo sanciona con uno a tres años de prisión a quien, sin autorización, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, comunicaciones privadas o información en soportes informáticos protegiendo así el derecho a la intimidad de las personas, asegurando la privacidad y confidencialidad de su información personal. (Código Orgánico Integral Penal, 2024)

Art. 190.- Apropiación fraudulenta por medios electrónicos.- Como tal el artículo establece una pena de uno a tres años de prisión para quien utilice fraudulentamente sistemas informáticos para apropiarse de bienes ajenos o transferir bienes, valores o derechos sin consentimiento incluyendo alterar, manipular o modificar el funcionamiento de redes, programas, sistemas informáticos, telemáticos y equipos de telecomunicaciones, en beneficio propio o de terceros. (Codigo Organico Integral Penal, 2024)

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- El artículo sanciona con trece a dieciséis años de prisión a quien produzca o distribuya materiales de pornografía infantil incluyendo dos agravantes siendo asi en caso la víctima tiene una discapacidad o enfermedad grave, la pena es de dieciséis a diecinueve años mientras que si el infractor es un familiar cercano, tutor, ministro, profesor o alguien en una posición de confianza o autoridad, la pena sera de entte veintidós a veintiséis años.

Este artículo busca proteger a los menores de la explotación sexual y castiga severamente el abuso de posiciones de confianza o autoridad. (Código Orgánico Integral Penal, 2024)

Art. 229.- Revelación ilegal de base de datos.- Sanciona con uno a tres años de prisión a quien revele ilegalmente información de bases de datos, violando la intimidad y privacidad de las personas teniendo como agravante si el delito es cometido por un servidor público, empleado bancario o contratista, la pena aumenta de tres a cinco años.

Con la tipificación de este delito se protege la confidencialidad de la información personal y castiga más severamente a quienes, por su posición, tienen un mayor deber de proteger estos datos. (Código Orgánico Integral Penal, 2024)

Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.- Dentro se establece una pena privativa de libertad de siete a diez años para cualquier persona que utilice medios electrónicos o telemáticos, como correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs o juegos en red, para ofrecer servicios sexuales con menores de dieciocho años. (Código Orgánico Integral Penal, 2024)

Por lo que dentro del presente artículo se protege la integridad y dignidad de los menores de edad, específicamente contra la explotación sexual las conductas prohibidas incluyen el uso de diversas tecnologías para facilitar la oferta de servicios sexuales con menores, destacando la gravedad de estos actos y la necesidad de combatir la explotación infantil en el entorno digital.

Se consideran a estos delitos unos de los más importantes porque atentan directamente contra la integridad de sus víctimas, no obstante existen otros delitos que siguen siendo importantes dentro del Código Orgánico Penal Integral como por ejemplo la estafa informática.

1.1.5 Derechos Relacionados a la Ciberseguridad en el bloque Constitucional

La población ecuatoriana por medio de su constitución goza tanto de derechos como de obligaciones los cuales en unión conforman una armonía que permite que los ciudadanos tengan acceso a todo lo que nos permita alcanzar el buen vivir y con la llegada de las tecnologías de la información a la cotidianidad era inevitable la integración de su uso y posterior protección a los usuarios.

Por lo tanto en base al ámbito del bloque constitucional nuestra Constitución de la República del Ecuador establece ciertos artículos en los que se refiere a la protección de los datos y la información de los usuarios en el Ecuador, tales como:

1.- Art. 25.- El presente artículo de la Constitución de la República del Ecuador garantiza a todas las personas el derecho a disfrutar de los beneficios y aplicaciones del progreso científico y de los saberes ancestrales, este se enmarca en los derechos fundamentales protegidos por la Constitución, la cual establece que el más alto deber del Estado es respetar y hacer respetar estos derechos, al reconocer la importancia tanto del conocimiento científico moderno como de los conocimientos ancestrales, el artículo destaca la diversidad y riqueza del conocimiento humano y su aplicación para el beneficio de la sociedad. (Constitución, 2024)

2.- Art 66.- Este artículo de la Constitución de la República del Ecuador, dentro de sus numerales 19 y 25, establece derechos fundamentales relacionados con la protección de datos personales y el acceso a bienes y servicios de calidad.

Para entender un mejor mejor el numeral 19 garantiza el derecho a la protección de datos personales, permitiendo a las personas acceder y decidir sobre su información personal, y estableciendo que la recolección, archivo, procesamiento, distribución o difusión de estos

datos sólo puede realizarse con la autorización del titular o por mandato legal mientras que el numeral 25 reconoce el derecho a acceder a bienes y servicios públicos o privados de calidad, enfatizando la eficiencia, eficacia y buen trato en su provisión, por lo que estos derechos subrayan la importancia de la privacidad, el control de la información personal y la calidad en la prestación de servicios. (Constitución, 2024)

Los derechos que se establecen en la constitución, en este caso en los artículos mencionados, son de total trascendencia, puesto que en estos últimos tiempos hemos sido testigos de varias denuncias que quedaron en la impunidad de manera que no se podían dar con sus autores por la razón de que se trataba de delitos cometidos por medio de los instrumentos tecnológicos que hoy en día están al alcance de todos.

Esto conlleva perjuicios al estado y en especial a las personas quienes son víctimas de estos ciberdelincuentes, además que también por vacíos legales de nuestro sistema de leyes existen conductas contrarias al buen vivir.

1.1.6.- Introducción al Convenio de Budapest

El Convenio de Budapest, formalmente conocido como el Convenio sobre Ciberdelincuencia del Consejo de Europa, es un tratado internacional pionero en la regulación de delitos cometidos a través de redes informáticas e Internet, fue adoptado el 23 de noviembre de 2001 en Budapest, Hungría, y entró en vigor el 1 de julio de 2004.

El convenio no solo se centra en la penalización de ciertas conductas delictivas, sino que también establece medidas procesales y fomenta la colaboración entre países para enfrentar la naturaleza transnacional de los delitos cibernéticos, con la rápida evolución de la tecnología y la creciente dependencia de las sociedades modernas de las infraestructuras digitales.

1.1.7.- Objetivos del Convenio

El Convenio de Budapest tiene varios objetivos fundamentales que buscan proporcionar una respuesta coordinada y efectiva a la ciberdelincuencia:

Armonización de legislaciones: Busca que los estados miembros adopten leyes nacionales coherentes que tipifiquen de manera similar los delitos cibernéticos, facilitando así la cooperación y el enjuiciamiento transnacional de estos delitos.

Fortalecimiento de la cooperación internacional: Facilita la colaboración entre los estados miembros en la investigación y persecución de delitos cibernéticos, esto incluye mecanismos para la asistencia mutua, la extradición de delincuentes y el intercambio de información, todo con el fin de mejorar la eficiencia y efectividad de las respuestas legales a la ciberdelincuencia.

Desarrollo de capacidades: Promueve el intercambio de conocimientos, experiencias y mejores prácticas en la lucha contra la ciberdelincuencia, este objetivo incluye la capacitación de personal, el desarrollo de tecnologías avanzadas y la implementación de procedimientos eficaces para la prevención, detección y enjuiciamiento de delitos cibernéticos. (Gomez, 2010)

1.1.8.- Términos y Definiciones

Este capítulo proporciona las definiciones clave y establece el ámbito de aplicación del convenio. Entre las definiciones más relevantes se incluyen:

Sistema informático: Cualquier dispositivo o grupo de dispositivos interconectados que realizan el procesamiento de datos según un programa.

Datos informáticos: Cualquier representación de hechos, información o conceptos en una forma apta para su procesamiento en un sistema informático.

Proveedor de servicios: Cualquier entidad pública o privada que ofrezca a usuarios la posibilidad de comunicarse mediante sistemas informáticos. (Novoa, 2020)

1.1.9.- Medidas que deben adoptar a nivel internacional

Este capítulo detalla las obligaciones para los estados miembros de incorporar ciertos delitos en sus legislaciones nacionales.

Las principales disposiciones incluyen:

Acceso ilícito: Entrada no autorizada a sistemas informáticos, lo cual puede implicar hackeo o cualquier otro método de intrusión.

Interceptación ilícita: Intercepción no autorizada de comunicaciones no públicas, incluyendo correos electrónicos y datos transmitidos a través de redes.

Interferencia con datos: Daño, eliminación, deterioro, alteración o supresión de datos informáticos sin derecho.

Interferencia con sistemas: Interferencia grave y sin derecho en el funcionamiento de un sistema informático, como ataques de denegación de servicio.

Uso indebido de dispositivos: Fabricación, venta, adquisición, importación, distribución o puesta a disposición de dispositivos, programas o contraseñas con la intención de cometer delitos informáticos. (Gomez, 2010)

1.1.10.- Cooperación internacional

Este capítulo es esencial para la implementación efectiva del convenio, ya que la ciberdelincuencia a menudo trasciende las fronteras nacionales.

Las disposiciones incluyen:

La asistencia mutua siendo procedimientos para solicitar y proporcionar asistencia en la investigación de delitos cibernéticos.

La extradición: Normas para la entrega de delincuentes cibernéticos entre países, el convenio facilita la extradición al considerar los delitos cibernéticos como extraditables, siempre y cuando sean castigables con una pena privativa de libertad de al menos un año.

1.1.11.- Impacto y Relevancia del Convenio

El Convenio de Budapest ha tenido un impacto significativo en la lucha contra la ciberdelincuencia a nivel global, entre sus logros y desafíos se destaca el transformarse en el estándar de facto para la legislación sobre ciberdelincuencia, influenciando tanto a los países miembros como a aquellos fuera del Consejo de Europa.

Por lo que en muchos países han adoptado o modificado sus leyes nacionales para alinearlas con las disposiciones del Convenio de Budapest, lo que ha facilitado la cooperación internacional y la creación de un marco jurídico común.

A pesar de su éxito, el Convenio de Budapest ha enfrentado críticas y desafíos, algunos críticos han señalado preocupaciones sobre la protección de los derechos humanos y la privacidad, argumentando que las disposiciones del convenio podrían ser utilizadas para justificar la vigilancia masiva y la recopilación de datos sin las debidas salvaguardias.

Además, la rápida evolución de las tecnologías de la información y las comunicaciones plantea la necesidad de actualizaciones periódicas del convenio para mantener su relevancia y efectividad. (Gomez, 2010)

Para abordar estos desafíos, el Convenio de Budapest ha sido objeto de enmiendas y actualizaciones por ejemplo en el 2018, el Consejo de Europa adoptó el Protocolo Adicional al Convenio de Budapest, que aborda la cooperación reforzada y la divulgación de pruebas electrónicas.

1.1.12.- Implementación del Convenio en Ecuador

Ecuador, aunque no es miembro del Consejo de Europa, ha mostrado interés en alinearse con los principios del Convenio de Budapest en su legislación nacional, la adopción de medidas acordes a este convenio puede fortalecer la capacidad del país para enfrentar la ciberdelincuencia de manera más efectiva y colaborativa.

Es crucial analizar cómo las disposiciones del Convenio de Budapest pueden ser incorporadas en el Código Penal ecuatoriano, esto incluye la tipificación de nuevos delitos, la actualización de las definiciones legales existentes y la implementación de procedimientos adecuados para la investigación y el enjuiciamiento de delitos cibernéticos, además, es importante considerar cómo las leyes ecuatorianas pueden ser armonizadas con las disposiciones del convenio para asegurar una cooperación internacional efectiva.

Evaluar los mecanismos de cooperación internacional de Ecuador en la lucha contra la ciberdelincuencia y su alineación con los principios del convenio, la cooperación internacional es esencial para enfrentar la naturaleza transnacional de la ciberdelincuencia y asegurar una respuesta coordinada y efectiva.

1.1.13.- Casos relevantes

1. - **Ataque de ransomware a la Corporación Nacional de Telecomunicaciones (CNT) – 2021**

Descripción:

La Corporación Nacional de Telecomunicaciones (CNT) de Ecuador sufrió un fuerte ataque de ransomware en julio de 2021, lo que causó un grave daño a su infraestructura tecnológica, los atacantes cifraron datos importantes y pidieron criptomonedas como rescate para liberar las claves de descifrado, los clientes residenciales y comerciales se vieron gravemente afectados por los servicios de telecomunicaciones ofrecidos por CNT como resultado de este ataque.

Análisis:

Este suceso destaca la susceptibilidad de las infraestructuras vitales a los ataques de ransomware y la urgencia de implementar medidas de ciberseguridad más efectivas, el incidente resalta la importancia de tener leyes punitivas y estrategias preventivas efectivas y de respuesta rápida, aunque la legislación ecuatoriana, en particular el Código Orgánico Integral Penal (COIP), penaliza tales acciones, en comparación con el Convenio de Budapest, Ecuador podría obtener beneficios de una mayor colaboración internacional y ayuda técnica para fortalecer sus habilidades de respuesta y recuperación ante ataques cibernéticos.

Este caso también demuestra la importancia de implementar un enfoque integral que involucre la educación y la sensibilización sobre ciberseguridad en todos los niveles de la sociedad y las empresas.

2. - Incidente de Ciberseguridad en el Banco Pichincha – 2021

Descripción:

El Banco Pichincha ha experimentado un prolongado corte de más de 72 horas en sus servicios electrónicos debido a un "incidente de ciberseguridad" detectado en sus sistemas informáticos, según un comunicado publicado en su cuenta de Twitter el 11 de octubre de 2021.

El banco ha tomado medidas inmediatas para aislar los sistemas afectados y está colaborando con expertos en ciberseguridad para investigar el incidente. Hasta el momento, no se ha especificado el tipo de ciberataque ni la parte específica de la infraestructura afectada.

En febrero de 2021, se reportó una filtración masiva de datos personales de clientes, inicialmente negada por el banco como información falsa circulando en redes sociales. Posteriormente, se confirmó un acceso no autorizado a los sistemas de un proveedor que maneja servicios de marketing para el banco, el grupo de ciberdelincuentes Hotarus Corp estuvo involucrado en esta filtración, comprometiendo datos de clientes del Banco Pichincha y Grupo Diners, a pesar de que se exigía un rescate millonario por los datos robados, nunca se realizó el pago y la base de datos se distribuyó en foros de hackers meses después.

En julio de 2021, Hotarus Corp nuevamente apareció en foros de Internet y liberó la base de datos completa de manera gratuita aunque el banco afirmó que sus sistemas no fueron vulnerados, el grupo hacker contradice esta declaración.

Análisis

El incidente de ciberseguridad en Banco Pichincha, evidenciado por un prolongado corte de servicios electrónicos y la declaración oficial del banco sobre un "incidente de ciberseguridad", destaca la creciente vulnerabilidad de las instituciones financieras frente a amenazas digitales, la respuesta rápida del banco en aislar los sistemas afectados y colaborar con expertos en ciberseguridad muestra un intento por mitigar los efectos y restaurar la confianza pública.

Sin embargo, eventos previos como la filtración masiva de datos en febrero de 2021, atribuida a un acceso no autorizado a través de un proveedor externo y la participación del grupo Hotarus Corp, subrayan los desafíos persistentes que enfrentan las entidades financieras en proteger la integridad de los datos de sus clientes frente a ciberataques sofisticados y la importancia crucial de la transparencia y la comunicación efectiva en la gestión de crisis de ciberseguridad para preservar la confianza del público y mitigar riesgos reputacionales.

3. Red de pornografia infantil en Canoa Manabi – 2021

Descripción

En 2021 la parroquia Canoa en Manabí se convirtió en el centro de operaciones de una red internacional de pornografía infantil, destacándose por el uso intensivo de medios electrónicos para la producción, distribución y comercialización ilegal de material pornográfico infantil. Dos ciudadanos holandeses fueron condenados a 10 años de prisión por dirigir estas actividades desde un hotel local, incluso tras su reclusión en la cárcel de El Rodeo en Portoviejo continuaban con estas actividades.

Este caso ejemplifica la vulnerabilidad de las zonas costeras frente a los ciberdelitos, aprovechando la falta de presencia estatal y las carencias en infraestructura, la operación

reveló la magnitud del problema, identificando una red de pedófilos implicados en actividades ilícitas mediante plataformas web y redes, subrayando la necesidad urgente de mejorar la seguridad cibernética y fortalecer las respuestas institucionales para proteger a los niños y combatir el crimen organizado en Ecuador.

Análisis

Este caso revela no sólo la gravedad de los ciberdelitos aprovechando la falta de control estatal y las vulnerabilidades locales, sino también la crítica dependencia de medios electrónicos en su perpetración, este incidente subraya la urgencia de fortalecer las políticas de ciberseguridad y mejorar la vigilancia digital para combatir eficazmente este tipo de explotación infantil transnacional, además evidencia cómo la globalización y la tecnología permiten a organizaciones criminales operar más allá de fronteras físicas y eludir sistemas penitenciarios, enfatizando la necesidad de una cooperación internacional más robusta para abordar estos desafíos interconectados de manera integral y proteger efectivamente a las comunidades vulnerables.

Capítulo 2: Metodología del proceso de investigación

2.1 Enfoque de la investigación.

Enfoque cualitativo:

Según los autores Blasco y Pérez, señalan que este enfoque cualitativo “estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas.” (Blasco Mira & Pérez Turpin, 2007)

Por ello dentro de esta investigación se analiza los datos recopilados a través de un proceso empírico obtenidos por medio del análisis de la literatura, la investigación bibliográfica, la observación y las entrevistas.

Este enfoque fue el utilizado porque lo que se busca es tener una comprensión y un estudio profundo de las causas y consecuencias que generan estos delitos ya que al ser por medios electrónicos se vuelve complicado el investigarlos y mediante las entrevistas a Fiscales especializados en ciberdelitos se busca colegir la interpretación de experiencias, perspectivas y significados subyacentes.

2.2- Alcance de la investigación

2.2.1.- Investigación Exploratoria:

Tal como lo indica el autor Arias esta investigación “Es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir un nivel superficial de conocimiento”, (Arias, 2012).

Es por ello que se considera adecuado este tipo de investigación porque dentro del presente trabajo se tiene como objetivo explorar nuevas preguntas, desafiar las ideas y suposiciones tradicionales y sentar las recomendaciones para superar estos delitos.

2.2.2.- Investigación Descriptiva:

Por otro lado los autores, Hernández, Fernández, y Baptista señalan que una investigación descriptiva “ busca especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis, miden y evalúan

diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Desde el punto de vista científico, describir es medir" (Hernandez, 2014)

El uso de este tipo de investigación es necesario porque tiene como objetivo recopilar datos para su posterior análisis y proporcionar una imagen clara del sujeto, con el fin de describir y caracterizar la situación.

Permite obtener una comprensión sistemática y detallada del tema, identificando patrones y tendencias que pueden no ser evidentes a simple vista, aunque no pretende explicar causas o relaciones causales, brinda una descripción exhaustiva y contextualizada de los fenómenos estudiados, este enfoque enriquece el conocimiento existente, facilita el desarrollo de políticas y soluciones prácticas, y sirve como referencia para futuras investigaciones y estudios comparativos.

2.3.- Delimitación de la investigación

La presente investigación se desarrolló en el cantón Guayaquil, provincia del Guayas, enfocada durante el periodo 2020 al 2024

2.4 .- Población y muestra de la investigación

El universo de este estudio está orientado al desarrollo de entrevistas a los fiscales que hayan actuado dentro de un proceso judicial con respecto a ciberdelitos en el cantón Guayaquil, provincia del Guayas

La población a entrevistar en esta investigación es en base a la información proporcionada por la Fiscalía Provincial del Guayas mediante el derecho de petición realizado por medio de un oficio dirigido al Fiscal Provincial del Guayas en base a los artículos 66 #23 y 225 de la Constitución del Ecuador, obteniendo como respuesta de la Fiscalía Provincial del

Guayas un listado entregado en formato EXCEL en donde se puede visualizar que existen 52 fiscales con especialización en ciberdelitos, los cuales se encuentran en función.

La muestra probabilística usada en este estudio es la de 10 fiscales especializados en ciberdelitos puesto que al intentar entrevistar a los 52 fiscales la mayoría se negaba por diversas razones siendo las más reiteradas la falta tiempo, privacidad o sensibilidad en casos, por lo que se considera que las entrevistas a los 10 fiscales es una cantidad significativa.

2.5.- Métodos empleados.

Entrevistas:

El autor Javier Torrecilla define que la entrevista “Es una conversación provocada por un entrevistador con un número considerable de sujetos elegidos según un plan determinado con una finalidad de tipo cognoscitivo. Siempre está guiada por el entrevistador pero tendrá un esquema flexible no estándar” (Torrecilla, 2006)

Por ello dentro de la presente investigación las entrevistas fueron aplicadas a fiscales debido a su especialidad en el área de los ciberdelitos, los cuales brindaran su conocimiento para el mayor entendimiento de estos, y como en su basta experiencia pueden dar una opinión certera que permita obtener una visión más clara sobre estas actividades ilícitas.

Capítulo 3: Análisis de resultados de la investigación

A continuación, se presentan las entrevistas realizadas a Fiscales especializados en ciberdelitos:

Entrevista 1: Fiscal: ROMERO JAEN WALTER JUNIOR, trabaja en FISCALÍA ESPECIALIZADA EN SOLUCIONES RÁPIDAS CENTRO 5.

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Personalmente considero que sí, teniendo en cuenta que en el año 2002, recién a raíz de la publicación de la ley de comercio electrónico, se reformó el código penal y se introdujeron los delitos electrónicos e informáticos dentro de nuestro ordenamiento jurídico.

Ahora, en el COIP, en el año 2014, cuando fue publicado, sí reconoció figuras que anteriormente no se encontraban tipificadas, y en ese sentido había una evolución, tanto más que en el año 2021 también se reformó el COIP por la publicación de la ley orgánica contra la violencia digital y eso también reformó algunos artículos, incluyó otros en relación a los delitos informáticos y más que nada a las técnicas de la Fiscalía para poder investigarlos, cooperación internacional, conservación de datos y demás.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Bueno, como bien dices, para investigar, el hecho de que las pruebas son endebles y editables y borrables, y para procesar, porque el delito informático, como es cometido en línea, existen mecanismos para poder falsear o para poder maquillar o ocultar la dirección IP donde se cometen, y por esa razón es muy difícil poder establecer el autor o partícipe de la infracción.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Existen varios casos en base a la violación de la intimidad, son mucho más comunes de lo que uno espera tenemos como por ejemplo tenemos el caso de la aerovía ocurrido aquí en

la ciudad de Guayaquil, es verdad que las personas implicadas dentro de este no debieron de tomar conductas sexuales desde un principio pero en todo caso muy aparte de lo ocurrido, nunca tuvo que ser público el video puesto que de esta manera es donde se comete el delito de violación a la intimidad, al ser publicado cierto video vulneran sus derechos, es por eso que se toma como delito de violación a la intimidad tal acto y como este hay muchos más.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Bueno, siempre existirán normas tanto sustantivas como procesales acerca de los delitos, considero que nuestra legislación sustantiva contiene la mayoría de delitos informáticos a nivel internacional, cumple con los estándares del Convenio de Budapest, existen muchos delitos, aproximadamente 20 delitos en el COIP que tipifican las conductas principales.

Ya ciertas precisiones de lagunas en materia procesal, más bien, creería yo que sí existen. Por ejemplo, cuando el artículo que establece la competencia territorial en materia penal, por ejemplo, establece formas para poder establecer la competencia, pero siempre en relación al lugar donde se ha cometido el delito y en delitos informáticos, tú sabes que es difícil establecer el lugar exacto.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

La fiscalía hace cursos y obliga a que los funcionarios fiscales estén siempre actualizados,mientras que en materia de jueces y secretarios judiciales no existe esa constante actualización o formación.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Bueno, considero que sí, que el código penal actual, a raíz de la reforma del año 2021, por la ley contra la violencia digital, ya se encuentra, digamos que, apto para pedir que Ecuador forme parte y ratifique el convenio de Budapest.

Entonces, creo que si analizamos desde el punto de vista objetivo los articulados que se exigen o se recomiendan en el convenio de Budapest, creo que el COIP actual ya los cumple, entonces, estamos a la par para allá formar parte.

Entrevista 2: JUAN CARLOS VIVAR ÁLVAREZ trabaja en la Fiscalía de Fe Pública de Guayaquil.

1. - ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Bueno, considero que sí ha evolucionado, el Código Orgánico Integral Penal es una norma muy vanguardista, pero el problema que tenemos nosotros es en la aplicación y no lo digo en la aplicación por un mal servidor judicial, lo digo en la aplicación por no contar al 100% con herramientas tecnológicas o con herramientas que puedan fortalecer la prueba, ejemplo, necesitamos fortalecer un laboratorio de criminalística con informática forense de punta pero esa informática forense de punta se logra con mucho presupuesto.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Bueno, como lo manifesté, por ejemplo, tenemos problemas con el ámbito tecnológico, existen equipos electrónicos que, por ejemplo, no alcanzan para poder extraer información de teléfonos celulares, por ejemplo, iPhone 13 Promax, 14, 15, que son versiones bastante

complejas, bastante modernas adempas que limitan de cierta manera al trabajo que realiza la sección de informática forense del laboratorio de criminalística.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Bueno, como en muchos casos, estamos hablando desde la utilidad de la tecnología como tal pienso que cuando se extrae información de los teléfonos celulares, se logra obtener valiosa información que nos puede llevar a resolver un determinado hecho.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Como le dije en la primera pregunta, considero que no,yo creería más en los problemas relacionados hacia el marco probatorio.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Bueno en la Fiscalía General del Estado, en los últimos años, a raíz de la pandemia, hemos tenido un sinnúmero de cursos y no ha sido extraño el curso especializado en ciberdelitos, con la particularidad de que hoy los cursos se desarrollan de manera online, yo tuve la oportunidad de ser director de capacitación de la Fiscalía casi cinco años, y en mi época, los cursos, por las razones de ese entonces, eran todos presenciales, por lo que de cierta manera, la presencialidad acerca más a especializarse, quizás acerca más a entender el tipo de capacitación, la calidad de la capacitación, la dirección de fortalecimiento y capacitación del talento humano de la Fiscalía, creo que ha sido bastante generosa con los servidores en lo que tiene que ver con ciberdelincuencia.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Actualmente yo considero que la norma es óptima, la norma no es criticable, estamos próximos a reformar nuevamente el Código Orgánico Integral Penal porque se viene la inclusión de la variación de las penas en ciertos delitos, especialmente los delitos de corrupción, y también se viene una recodificación del Código Orgánico Integral Penal en el marco de ciertos delitos en los cuales está de por medio la ciberdelincuencia, entonces pienso que la ley no es mala, pienso que nosotros nos encontramos a la altura.

Entrevista 3: VILLARREAL CARDENAS TONSHAY JOSEFINA trabaja en la FISCALÍA ESPECIALIZADA EN VIOLENCIA DE GÉNERO 2

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Sí, considero que sí ha evolucionado mucho desde su integración en el Código Orgánico Integral Penal puesto que antes eran muy pocos los delitos que se encontraban dentro de la normativa penal.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Lo que más he encontrado es la falta de ajuste en la tipificación del delito.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Delito de pornografia usando a niños, niñas y adolescentes, en si estos son los casos que más suelen impactar al momento de investigarlos porque nos topamos con situaciones

inimaginables que sufren los menores de edad por parte de aquellas personas que distribuyen este tipo de contenido por el internet.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Si existen bastantes, porque en la actualidad algunos tipos penales no se ajustan a ciertas conductas que se han comenzado a dar desde un tiempo para acá con el desarrollo de la tecnología.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Capacitaciones consecutivas sobre varios temas entre ellos los ciberdelitos.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Aún falta por adaptar la normativa.

Entrevistado 4: FISCAL VELAZCO SOLIS JOFFREY ALFREDO trabaja en la FISCALÍA ESPECIALIZADA EN PATRIMONIO CIUDADANO 7

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

A ver, este sí, considero que sí ha evolucionado en cuanto a las cifras, más que nada porque simplemente hay un nuevo catálogo que se da a partir del 2021, porque antes se

sancionaba con la ley de comercio electrónico y ahora todo eso fue derogado por ese proyecto de ley y se incorporaron nuevos delitos al Código Orgánico Integral Penal.

Pero eso no quiere decir que haya evolucionado para bien, porque al ser ciberdelitos es muy difícil dar con el sujeto activo, la gran mayoría de delincuentes, cuando hablamos de ciberdelincuencia, se aprovechan de lo que les brinda la red, que es el anonimato y para romper con ese anonimato hay que tener ayuda internacional y muchas veces el país no tiene recursos, ni mucho menos tiene convenios que nos faciliten ese tipo de actividades.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

La mayor dificultad que se presenta a la hora de investigar o no saber delitos, es esa, el anonimato que te brinda la red porque fácilmente tu puedes crear un usuario, una contraseña en alguna página y empezar a estafar a personas, empezar a comerciar pornografía infantil o empezar a atacar sistemas financieros, los cuales pueden derivar hasta en un agitaje, en un pánico económico, que ya son otra clase de delitos, pero su génesis va a ser desde la internet.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

No sabría cual explicar porque no he abordado muchos ciberdelitos pero hay un caso que paso a los inicios de la pandemia fue cuando se investigó un caso de apropiación fraudulenta por medios electrónicos en contra de 6 personas, siendo la mayoría familia, quienes utilizaron números de tarjetas y códigos robados en Estados Unidos y Europa, para comprar cuentas de streaming y mercadería en plataformas virtuales, para luego venderlos, a través de redes sociales, a la mitad del precio real.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Claro, siempre van a existir algunas legales y áreas grises, lamentablemente con la calidad de legisladores que tenemos, pues sí lo va a ver, muchas de nuestras relaciones es populismo penal, entonces no van a atender la génesis del problema, sino que van a atender el tener gente en las cárceles, entonces sí, puede haber áreas legales o áreas grises porque no son expertos en técnicas legislativas.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

La formación, que no suelen dar, son pocas las capacitaciones, pero como te mencioné en un principio, el tema de los recursos a nivel estatal, a nivel nacional, es muy limitado.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Más que nada es adecuar las leyes que nosotros tenemos a lo internacional, porque el Convenio de Budapest sí habla de una cooperación internacional en cuanto a los tipos penales que se parezcan o se asemejen, por lo menos, en cuanto a la sanción, es muy importante para la ciberdelincuencia que los países estén prestos a ayudar, porque si el día de hoy es Ecuador, el día de mañana perfectamente puede ser alguno de los países potencias a nivel mundial, nadie está exento de un ataque a su red.

Debemos de aplicarlo, el mayor bloqueo constitucional que teníamos ya no está, entonces ya no habría más impedimentos que adecuar nuestras leyes al convenio.

Entrevista 5: VERA ARIAS ZOILA PRICILA trabaja en la FISCALÍA ESPECIALIZADA EN SOLUCIONES RÁPIDAS CENTRO 7

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Yo creo que la legislación si se ha modernizado, si ha existido un avance en la tipificación de estos delitos porque en el código anterior no había mención siquiera de estos delitos, pero ahora de acuerdo a la sociedad que ha evolucionado, que ha cambiado, que se ha desarrollado mediante los aparatos electrónicos, mediante estos sistemas electrónicos, entonces si hay un avance en nuestro código, si hay un avance, pero que la tecnología va muy rápido, demasiado rápido, que así mismo nosotros deberíamos estar al pie con las reformas, deberían tomarse mucho más en cuenta el hacer reformas a los códigos, porque así como avanza la tecnología también avanza la forma en la que las personas buscan romper o agredir mediante estos medios tecnológicos, evadir las normas, lo regular de la sociedad.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Las dificultades son podría decir que primero por los presupuestos y segundo por el mal manejo de los funcionarios, porque primero se necesita tener un presupuesto grande para poder adquirir aparatos tecnológicos mediante el cual se pueda llegar a investigar de una manera correcta los ciberdelitos además necesitamos también personal que esté capacitado, no es suficiente que sean abogados o que conozcan de derechos, sino que también necesitan estar empapados sobre computación, sobre sistemas, sobre todo lo que comprende el funcionamiento de las redes, la web, todo.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

En sí dentro de nuestro despacho hemos tenido varios casos acerca de regulación ilegal de base de datos**,** lo más relevantes son aquellos que se cometen en contra de entidades

financieras en vista de que para los hackers es más importante el revelar información confidencial de aquellas entidades por las grandes cantidades de dinero que pueden obtener de estos delitos.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Aunque el sistema ha avanzado todavía existen bastantes lagunas legales o áreas que no se han cubierto como lo mencionaba anteriormente el mundo ahora va muy rápido y aún con más velocidad el mundo electrónico o este mundo de la web entonces si existe mucho vacío porque digamos se lo tipifica que tal conducta no es un delito pero no existe el proceso no existe un manual de cómo de cómo se va a investigar el delito de cómo se va a hacer procesado de cómo se va a llevar la prueba de estos delitos cómo se va a hacer tratada o sea necesitamos también no sólo reconocer la acción sino también profundizar y que exista un todo un complemento de la legislación para que pueda aplicarse de manera correcta estas estos hay ya no sé qué para que pueda aplicarse de manera correcta la ley.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Las capacitaciones para los fiscales si son constantes, existe una escuela de fiscales donde se debe cumplir, se debe responder a pruebas de manera constante, pero todo esto es hecho de manera online, entonces considero que es mejor o hay un contacto o un aprendizaje más óptimo cuando se hace esto de manera presencial, porque igual se podría tratar de sólo cumplir y no realmente estudiar o no realmente prestarle atención a las capacitaciones o no estar estudiando de manera consciente, sino que nada más completar una prueba por cumplir, si hay capacitaciones constantes.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Diría que sí ya que las normas ecuatorianas están adaptadas a los artículos establecidos en el Convenio de Budapest por lo que no habría problema en que Ecuador suscriba.

Entrevista 6: FISCAL CHACHO YEPEZ CELINDA KARINA trabaja en la FISCALÍA ESPECIALIZADA EN VIOLENCIA DE GÉNERO 4

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Sí, ya que se han implementado nuevas leyes y reformas que buscan adaptarse a la rápida evolución de la tecnología y los métodos utilizados por los ciberdelincuentes.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Las principales dificultades incluyen la falta de recursos técnicos adecuados, la necesidad de capacitación especializada para el personal, y la cooperación internacional limitada, que es crucial dado el carácter transnacional de muchos ciberdelitos.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Tuve un caso en la que se usó Facebook como la plataforma en la que se utilizó la captación de información ya que por medio de una cuenta falsa negociaba con una adolescente de 14 años para que esta le brinda servicios sexuales por suerte fue detenido antes de que llegara a peores

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Sí, aún existen lagunas legales especialmente en lo que respecta a la definición y tipificación de ciertos delitos cibernéticos. Además, la legislación no siempre se actualiza al ritmo de los avances tecnológicos.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Los fiscales y operadores de justicia reciben formación continua en temas de ciberdelincuencia, incluyendo cursos especializados, talleres y seminarios. Sin embargo, la capacitación puede variar en calidad y disponibilidad.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Las leyes ecuatorianas han avanzado significativamente y están en camino de cumplir con los requisitos del Convenio de Budapest. Sin embargo, aún se necesitan esfuerzos adicionales para alinear completamente nuestras normativas con los estándares internacionales establecidos en dicho convenio.

Entrevista 7: Fiscal Cristian Fares Falcones trabaja en la Fiscalía Unidad de uso ilegítimo de la Fuerza 1

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Al hablar de ciberdelitos, existe una amplia gama, un abanico grande de los delitos que deben estar reglados dentro de la normativa objetiva penal que habla de los procedimientos y también como norma sustantiva, en ese sentido, con el COIP sí se pudo avanzar en delitos que se refieren básicamente a la ciberdelincuencia, entre ellos como son la violación a la intimidad, pornografía infantil y lo que es la apropiación en el tema de delitos contra la propiedad o patrimonio por medios electrónicos, que es una variedad también del Estado.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Básicamente en las principales experiencias que practicamos, no sólo en unidades en las que se investiga esta tipología, sino en unidades distintas porque existe la necesidad de la utilización tecnológica considero que esta es una de las más complicadas de investigar ya que la tecnología es muy cambiante y compleja de averiguar por sus IP y demás medios.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Mi experiencia ha tenido múltiples casos, he estado en varias unidades fiscales, incluso en Galápagos, sii puedo hablar de relevancia en un caso emblemático, no sólo para mi trabajo, sino para el Estado, fue la interceptación del buque chino Fuyo Angiolín con 300 toneladas en la Reserva Marina de Galápagos.

La tecnología utilizada en el presente caso en mención tiene que ver con lo que es el ploteo. ¿Qué significa el ploteo? Es la búsqueda en el mapa GPS de los waypoints que contenían el cerebro de la embarcación, con el fin de verificar si la misma había ingresado dentro de la Reserva Marina de Galápagos, entonces es un trabajo pericial con el fin de determinar justamente la ubicación y determinar la materialidad y la tipología que íbamos imputando a los procesados.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Bueno, esta es una pregunta muy pero muy interesante. Si bien algunas tipologías no se encuentran expresamente señaladas, pero sí se encuentra una regulación adecuada, como les comenté, los principales delitos que están actualmente regulados o relacionados con la tecnología son los de pornografía infantil, los que realmente como Estado nos tenemos que preocupar, porque la trascendencia y la afectación al bien jurídico protegido y la dignidad o la integridad sexual de las víctimas hace que se deba tomar y rebasar las fronteras en el trabajo conjunto con otras agencias.

Entonces para ellos es necesaria la tecnología y de cierta manera la misma si se encuentra, por decirlo así, con elementos de convicción entonces en ese canal adecuado se puede preservar y podríamos decir que existe un vacío porque no está regulado expresamente, pero de manera un poco forzada nosotros tratamos de subsumir lo que es el sexting, lo que es el grooming en otros delitos como violación a la intimidad, como les referí también puede haber el delito de pornografía infantil, entre otros.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Bien, nosotros como Fiscalía General del Estado, y le voy a hablar en el caso concreto de los fiscales, dentro del sistema interno existe lo que es la escuela de fiscales, que anteriormente a la realidad actual nosotros teníamos capacitaciones y cursos presenciales, pero actualmente lo que se nos da son capacitaciones por medios virtuales, a lo que voy es que estas capacitaciones son a través de una plataforma en donde los fiscales y también los funcionarios misionales ingresan y hacen un curso en línea en donde existen sesiones grabadas, así como también cuestionarios, foros, con el fin de que participen pero soy un

poco antagónico a esta formación, porque no hay nada mejor que la comparecencia presencial, porque la interacción con el exponente hace que se capte mejor el mensaje, porque incluso estas capacitaciones virtuales en la práctica lo que se da, y les digo de manera concreta como funcionario, es que buscamos copiar rápidamente de otros con el fin de cumplir.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Los principios universales del derecho por control y convencionalidad están por encima de nuestra Carta de Responsabilidad, cuando se verifiquen los mismos mejores derechos que los consagrados en la Constitución entonces, en ese sentido, al hablar de una norma supraconstitucional como el convenio de Budapest, obliga a los Estados, parte en este caso de Ecuador, que dentro del desarrollo interno de sus derechos, se regulan tipologías que tienen que ver justamente con los delitos de ciberdelincuencia. Acogiendo esa disposición, nuestro Estado sí ha desarrollado algunas normativas.

Entrevista 8: Fiscal León Tenorio Víctor Hugo trabaja en la Fiscalía Especializada en Soluciones Rápidas 3

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Así es, puesto que en los años anteriores a la promulgación del Código Orgánico Integral Penal estas tipologías de delitos no eran tomados en consideración por cuanto ante la existencia de vacíos legales fue indispensable la implementación de los mismos.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Por el avance de la tecnología, es bastante complejo detectar a los autores de este tipo de delitos, complicaciones en la fase probatoria por cuanto es dificultoso la recopilación de pruebas ya que al momento de cometer este tipo de delitos difícilmente dejan rastros.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Un caso reciente fue cuando se procesó a una pareja por el delito de violación a la intimidad ya que enviaban mensajes a la víctima por medio de WhatsApp con mensajes como ¿Cuánto cobras? junto con imágenes íntimas las cuales solo le envió a su expareja, además de enviar esas mismas imágenes con distintos números

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Más que vacíos legales considero que falta conocimiento, fue a raíz de la pandemia por la necesidad de manejar la mayoría de las actividades de forma virtual, creó conciencia en la sociedad de este tipo de delitos, y su evidente afectación.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Existen capacitaciones constantes, pero realmente en comparación con otros tipos de delitos muchos de los servidores públicos, no los toman con la seriedad que amerita.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Consideraría que si pues el ecuador aun sin estar suscrito a este convenio tiene tipificado en su código penal los delitos establecidos en dicho convenio solo siendo falta la firma para entrar

Entrevista 9: Fiscal Alex Javier López Ávila trabaja en la fiscalía especializada en Patrimonio Ciudadano 6

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

¡Pero por supuesto! El único tipo penal que teníamos nosotros en el artículo 190, en algún tiempo en la vida, era la prospección ilícita por medios electrónicos, luego, simplemente un catálogo de delitos específicos para delitos electrónicos, que no excluye la utilización de algunas modalidades, como por ejemplo fishing, farming, para cuestiones de estafas, de abuso de confianza, o grooming para cuestiones sexuales, por ejemplo.

Así se va a ir avanzando. Nosotros no somos parte de un convenio, que es el convenio de Budapest, sobre ciberdelincuencia, pero sin perjuicio de aquello, hemos adaptado a nuestra legislación muchas normas internas.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Bueno, sucede que a veces tienes que tener un buen perito, el que te va a establecer y te va a dar los elementos del perito, sobre el perito que tú tengas, puedes solicitar ciertas informaciones que no lo veas, como, por ejemplo, si se puede ir lanzando con cuestiones de asistencias penales internacionales.

Porque hay peritos públicos que pertenecen al Departamento de Criminalística, en donde no cuesta, pero también hay peritos particulares, a los peritos particulares, en un momento, se

solicitó partidas para que cobraran estos honorarios, resulta que esas partidas eran muy caras y no se pagaban, motivos por los cuales, tiene que asumir directamente el costo de la parte entonces, eso es otro problema que podemos ver.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Yo revisé varios casos de extorsiones. A ver, ¿de dónde las tienes? La mayoría de los delitos que tú vas por estas cuestiones patrimoniales no los mandas a veces de un número local sino, tú te consigues un número extranjero a través de la plataforma WhatsApp para que no queden registrados entonces como tú no puedes hacer una triangulación de ubicaciones, como si no puedas hacer un código, una llamada normal o un SMS, sino que a través de esta moneda tú necesitas otro tipo de configuraciones, tú ahí necesitas pedirle al servidor.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

En mi experiencia profesional, he observado que sí existen lagunas legales y áreas grises en la legislación ecuatoriana en relación a los ciberdelitos aunque hemos hecho avances importantes, la rapidez con la que evolucionan las tecnologías y las tácticas de los ciberdelincuentes a menudo superan la capacidad de nuestras leyes para mantenerse al día, específicamente, la falta de definiciones claras y detalladas para ciertos tipos de ciberdelitos y la insuficiencia de procedimientos estandarizados para la recolección y manejo de evidencia digital son áreas que requieren mayor atención y desarrollo legislativo.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Hay cuestiones directamente relacionadas con el Consejo de la Judicatura a través de la escuela judicial en donde se forman personas, pero también tenemos que ir a las capacitaciones las cuales no son como las de antes por ejemplo cuando tú ibas te decían encarguese el despacho de esta persona y vaya 3 días o 4 días a un curso, ahora no, te dicen está abierto a tal fecha y a tal fecha entonces, como que no lo disfrutas igual, como que tú estás presencial y puedes ver, hacer preguntas, estar en tiempo real, hacerlo bien frente. Pero capacitaciones, eso sí hay.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Si me preguntas a mí sobre la legislación interna, yo creo que estamos al amparo de lo que dice el convenio de Budapest y sus protocolos, directamente con nuestra legislación.

Entrevista 10: Fiscal y Coordinadora de Fiscalías Especializadas en Violencia de Género Yoli Yelena Pinillo Castillo trabaja en la Fiscalía Provincial del Guayas Edificio la Merced.

1.- ¿Considera que la legislación penal ecuatoriana ha evolucionado con respecto a los ciberdelitos en los últimos años?

Bueno, considero que la legislación penal ecuatoriana sí ha evolucionado, no solamente sobre ciberdelitos, sino sobre todo lo que es la tipicidad penal que tenemos ahora por la dinámica que tiene y la mutación de los delitos, todos los delitos cometidos exactamente con el uso de medios electrónicos y también con medios electrónicos utilizados para la consumación.

También es importante indicar que ya no solamente ha ido en ese contexto, sino en el contexto de la violencia basada en género, como delitos de violación a la intimidad, ahora

ya está tipificada la extorsión sexual por medios electrónicos, sin embargo, no es menos cierto que todavía nos falta, nos falta que estar acorde a la normativa internacional, de cual de algunos instrumentos internacionales somos suscriptores, y de otros somos observadores, pero no nos hemos suscrito, como es la Convención de Budapest.

2.- ¿Qué dificultades ha encontrado al investigar o procesar casos de ciberdelitos?

Lo común del Ecuador es que normalmente las personas utilizan aplicaciones y sistemas operativos gratuitos o, digamos, ilícitos o ilegales por lo tanto no compran software. Entonces, al no comprar software original y adquirirlo de forma indebida, es una costumbre que se ha hecho, eso hace que estemos en medio de una sociedad muy vulnerable.

3.- ¿Cuál ha sido el caso que más relevancia ha tenido dentro de su despacho fiscal?

Bueno en la unidad que yo estaba de violencia de género como tal tuve casos de pornografía con el uso de niños y niñas adolescentes, explotación sexual y trata de personas donde desde a raíz de la pandemia este tipo de hechos se incrementaron y si bien es cierto podemos decir bueno es que es ciberdelito porque todas fueron captaron por medios cibernéticos hicieron la captación a través de mensajes de la red social Facebook y después a través del servicio de mensajería de WhatsApp entonces iniciaban mensajeando a las chicas con ofertas como que estás en pandemia tu familia se quedó sin empleo tú puedes ayudar y lo que hacían era concertar las citas en determinados moteles mal llamados hoteles de la ciudad y todas las víctimas eran adolescentes de 14 años hacia atrás o sea 12 ,13 ,14 años.

4.- ¿En base a su experiencia profesional, considera usted que existen lagunas legales o áreas grises en la legislación ecuatoriana en relación a los ciberdelitos?

Sí, como les indicaba que sí hay laguna fue la palabra que utilizo normalmente, bueno, el término jurídico es que hay los vacíos legales consideramos que un vacío importantísimo y que depende netamente del estado es que no ha suscrito Budapest si no suscribimos Budapest, como vacío considero que ya como política pública el Estado, porque eso es directamente el Estado tiene que suscribir Budapest no solamente ser observador, porque todo el articulado todo lo que comprende la convención de Budapest es lo que nosotros estamos viviendo a diario que, insisto, los hemos tipificado, sí, pero eso daría un afianzará.

5.- ¿Qué tipo de formación reciben los fiscales y otros operadores de justicia sobre la ciberdelincuencia?

Bueno, nosotros tenemos en la Escuela de Fiscales, o sea, la Fiscalía tiene la Dirección General de Capacitación y Fortalecimiento Misional, la Escuela de Fiscales y el Consejo de Judicatura también tiene la Escuela de Formación y Capacitación entonces, siempre son temas, diversos temas, no solamente hablamos de ciberdelitos o ciberdelincuencia o delitos cibernéticos, son muchos nombres y termina siendo lo mismo nos capacitan en todas las áreas y principalmente en estas áreas que están en auge violencia de género, ciberdelincuencia adicionalmente, y son cursos no solamente de participación sino de aprobación tenemos que hacer evaluaciones y todo.

6.- ¿Cree usted que las leyes ecuatorianas cumplen los requisitos para formar parte de los países asociados al Convenio de Budapest?

Sí, es decisión de política pública, de lo que he revisado es decisión del ejecutivo y el legislativo y a Ecuador reúne todos los presupuestos, es más, va de observador, o sea, lo que no se ha sentado es a revisar, y ahora sí, el compromiso, asumir el compromiso y suscribirse eso es lo que le falta, ya de lo que he revisado en los pronunciamientos que hacen las Naciones Unidas y todo el asunto, sin embargo no ha suscrito pero parte de lo

que establece la Convención de Budapest está aquí o sea, si ya lo tenemos acá, ¿qué falta? Decisión, decisión es la palabra

3.1.- Discusión de resultados

Análisis de los resultados obtenidos en base a las entrevistas realizadas a los fiscales especializados en ciberdelincuencia

Pregunta #1.

Los fiscales coinciden en que la legislación penal ecuatoriana ha experimentado una evolución significativa con el tiempo, especialmente desde la implementación del Código Orgánico Integral Penal (COIP), puesto que este marco legal ha incorporado nuevos tipos penales, entre ellos los ciberdelitos, adaptándose a las necesidades y desafíos contemporáneos.

Pregunta #2.

La mayoría de los fiscales coinciden en que el principal desafío en la investigación de ciberdelitos es rastrear a los ciberdelincuentes, en conclusión de que estos delincuentes cuentan con ventajas como el anonimato, el fácil acceso a los datos de las víctimas, la posibilidad de actuar de manera remota y la capacidad de distribuir información privada rápidamente, además, la fiscalía y los peritos expertos enfrentan desventajas significativas debido a la tecnología desactualizada que utilizan, lo que retrasa o incluso impide avanzar en las investigaciones y localizar a los culpables.

Pregunta #3.

Las respuestas varían según los fiscales entrevistados, cada uno especializado en diferentes áreas, por lo que entre los casos relevantes mencionados se encuentran los delitos de violación a la intimidad, la pornografía infantil, la oferta de servicios sexuales de menores de dieciocho años a través de medios electrónicos, la apropiación fraudulenta por medios electrónicos y la revelación ilegal de bases de datos.

Pregunta #4

Todos los fiscales entrevistados coincidieron en la existencia de lagunas legales dentro de la legislación ecuatoriana, las cuales son explotadas por los delincuentes, estas brechas en la ley surgen debido a la falta de especificidad en la normativa actual y al desconocimiento del poder legislativo sobre la naturaleza y complejidad de estos delitos y sus respectivas sanciones, por otro lado los fiscales subrayan la necesidad urgente de actualizar y fortalecer las leyes para enfrentar eficazmente los ciberdelitos y otros crímenes emergentes.

Así mismo destacaron la importancia de una capacitación continua para los legisladores, de modo que puedan comprender mejor estos delitos y desarrollar un marco legal más robusto y efectivo.

Pregunta #5.

Las capacitaciones virtuales y presenciales fueron el foco principal al abordar esta pregunta, subrayando además la importancia de la autoeducación entre los fiscales, estos enfatizaron que si bien las capacitaciones virtuales son convenientes y accesibles, la interacción directa y la dinámica de aprendizaje en las capacitaciones presenciales son percibidas como más efectivas, aquella preferencia se fundamenta en la capacidad de generar discusiones profundas, compartir experiencias prácticas y establecer conexiones más sólidas entre los participantes y los instructores, no obstante, los fiscales destacaron la necesidad de adaptar

los métodos de enseñanza a las complejidades cambiantes de los ciberdelitos, asegurando que tanto las modalidades virtuales como presenciales se mantengan actualizadas y pertinentes.

Pregunta #6.

La respuesta de los fiscales fue positiva respecto a que las leyes ecuatorianas cumplen con los requisitos para formar parte del Convenio de Budapest, un marco internacional crucial para la cooperación en la lucha contra los ciberdelitos, sin embargo, destacaron que la decisión definitiva para que Ecuador se adhiera a este convenio debe ser tomada por el Estado, por lo que expresaron la importancia de esta adhesión para fortalecer la capacidad del país en la investigación y persecución de delitos cibernéticos a nivel internacional, garantizando así una cooperación más efectiva con otras naciones.

4.- Conclusión

En conclusión, después de analizar los resultados en base a las entrevistas realizadas a los fiscales especializados en ciberdelitos, podemos afirmar que aunque el país dispone de una normativa que podría considerarse adecuada, esta no refleja la realidad crítica que enfrenta por lo que muchas veces no es tomada en cuenta y los ciberdelincuentes tienen el camino despejado para realizar sus delitos, por lo tanto, tener esta legislación actual resulta insuficiente además de el poco refuerzo en aquellos delitos de carácter internacional ya que al no estar suscritos al Convenio de Budapest perdemos la oportunidad de tener un gran apoyo internacional.

Junto con una deficiente educación sobre estas actividades ilícitas a los fiscales con el cambio que ha realizado de una modalidad presencial a una virtual lo que equivale a una

educación menos inmersiva poniendo en riesgo las actuaciones eficientes que deben de tener ellos al momento de investigar y solventar un caso de ciberdelito.

Resulta ser una constante razón de reclamo la falta de actualización a los medios tecnológicos y herramientas digitales en todos los sectores públicos ya que el Estado tiene poco o nulo interés en invertir en mejoras a estas herramientas lo que entorpece la eficiencia en la investigación de procesos delictivos de índole tecnológico incluyendo en estos aquellos que detectan y persiguen estos actos distintivos.

Es crucial que dentro del país se reconozca la importancia de adoptar medidas efectivas para proteger a la ciudadanía contra los ciberataques, los cuales se convierten en una gran amenaza para proveedores de servicios de comunicación nacionales, empresas vulnerables a hackers y para las personas naturales quienes pueden ser víctimas de cualquiera de estos delitos además de impactar la economía al ser hackeados sitios web de entidades financieras.

5.- Recomendaciones

Ahora bien basado en lo expuesto en las conclusiones, es necesario que se restauren las capacitaciones presenciales a los fiscales y agentes responsables de salvaguardar la seguridad de los ciudadanos, esto refiriéndose tanto a servidores públicos que trabajen para órganos como la Fiscalía como para también a aquellos que se encargan de crear, aprobar y modificar las normas.

Además es necesaria la implementación de nuevas herramientas tecnológicas que ayuden a la Fiscalía y a los peritos a detectar y perseguir estos ciberdelincuentes, teniendo en cuenta que lo apropiado es que el Estado otorgue los mecanismos adecuados que posee para la constante lucha contra la delincuencia.

Por otra parte, la integración del Ecuador al Convenio de Budapest es necesario para reforzar la protección a los datos de los ciudadanos permitiendo ayudar en actividades ilícitas que se realizan internacionalmente.

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

6.- Bibliografía

Arias, F. (2012). *El proyecto de investigación. Introducción a la metodología científica. 6ta*. https://books.google.com.ec/books?hl=es&lr=&id=W5n0BgAAQBAJ&oi=fnd&pg=PA11&dq=investigacion+exploratoria+fidias&ots=kZkI9qwsi8&sig=OzCGwUWYGcuGa3UeGPDGTBgtfUk

CHINCHILLA MORALES, J. (2021, 03). *LA CIBERDELINCUENCIA*. https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2393/LEC%20ING%20SIST%200035%202021.pdf?sequence=1&isAllowed=y

Codigo Organico Integral Penal. (2024). *Codigo Organico Integral Penal*. https://www.lexis.com.ec/biblioteca/coip

Constitucion. (2024). *Constitucion del Ecuador*. https://www.lexis.com.ec/biblioteca/constitucion-republica-ecuador

GALAN GUIZADO, A. P. (2023). *“DIAGNÓSTICO DE LA SITUACIÓN JURÍDICA DE LA CIBERDELINCUENCIA EN EL ECUADOR EN EL PERIODO 2022”*. file:///home/chronos/u-4a28f991fa1c5803255daf38b0ac97944747d9c7/MyFiles/Downloads/GAL%C3%81N%20GUIZADO%20ADRI%C3%81N%20PA%C3%9AL.pdf

Gomez, A. (2010). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

Hernandez, R. (2014). *Metodología de la investigación* (Vol. Tres). https://pdfs.semanticscholar.org/f6bf/7901dcceae8e87c5760eb13ff6ef5ff3f072.pdf

INTERPOL. (2024). *La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad*. Ciberdelincuencia. https://www.interpol.int/es/Delitos/Ciberdelincuencia

JUCA MALDONADO, F., & MEDINA PEÑA, R. (2023, 09 01). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Revista científica Portal de la Ciencia*, *4*(3), 326-327. https://institutojubones.edu.ec/ojs/index.php/portal/article/view/394

Lenguaje Juridico.com. (2024). *Ciberdelincuencia*. https://www.lenguajejuridico.com/diccionario-juridico/derecho-penal/ciberdelincuencia/

Macias Lara, R. A., Boné Andrade, M. F., Quiñonez Angulo, F., Mendoza Loor, J. J., Estupiñan Troya, G., & Rodríguez Vizuete, J. D. (2022, 04 30). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 232-233. https://www.journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324

Novoa, I. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional*. https://repositorio.uchile.cl/handle/2250/176344

Rosas, C. (2024). *Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la República del Ecuador, Colombia, Chile y Argentina*. https://repositorio.uta.edu.ec:8443/handle/123456789/41046

Solano Gutiérrez, G. A., Quintero Garcia, N. A., Cedeño Alcivar, L. L., & Eras Chancay, S. X. (2023, 05 17). Análisis de datos y tendencias emergentes en delitos informáticos en

redes sociales en Ecuador. *Polo del Conocimiento*, *8*(82), 1139-1140. https://dialnet.unirioja.es/servlet/articulo?codigo=9335839

Thomas, D. (2020, 04 20). *Cybercrime Losses*. National Institute of Standards and Technology. https://www.nist.gov/publications/cybercrime-losses-examination-us-manufacturing-and-total-economy

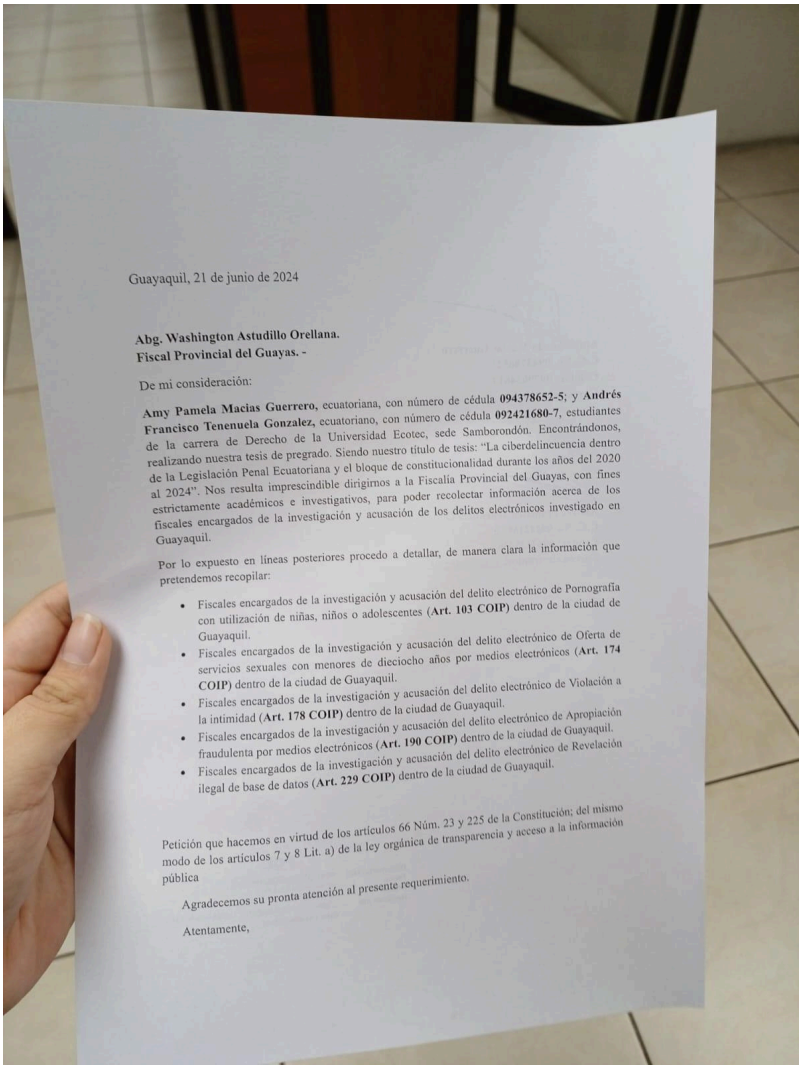
Torrecilla, J. (2006). *La entrevista*. http://www2.uca.edu.sv/mcp/media/archivo/f53e86_entrevistapdfcopy.pdf?f

Yagos Estrada, G. C., & Pilamunga Tigllán, D. P. (2023). *El ciberdelito del sexting y las dificultades probatorias.* http://dspace.unach.edu.ec/bitstream/51000/12676/1/Yagos%20Estrada%2C%20G%20y%20Pilamunga%20Tigll%C3%A1n%2C%20D%20%282024%29%20El%20ciberdelito%20del%20sexting%20y%20las%20dificultades%20probatorias.%20%28Tesis%20de%20Pregrado%29%20Universidad%20Nacional%2

Zambrano Rendón, A. D., Loor Campúes, F. D., Zambrano Vera, W. O., & Párraga Vera, R. G. (2022). *DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR*. https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

Anexos

Oficio dirigido al fiscal provincial del guayas para solicitar información sobre fiscales especializados en ciberdelincuencia



Guayaquil, 21 de junio de 2024

Abg. Washington Astudillo Orellana.
Fiscal Provincial del Guayas. -

De mi consideración:

Amy Pamela Macias Guerrero, ecuatoriana, con número de cédula **094378652-5**; y **Andrés Francisco Tenenuela Gonzalez,** ecuatoriano, con número de cédula **092421680-7**, estudiantes de la carrera de Derecho de la Universidad Ecotec, sede Samborondón. Encontrándonos, realizando nuestra tesis de pregrado. Siendo nuestro título de tesis: "La ciberdelincuencia dentro de la Legislación Penal Ecuatoriana y el bloque de constitucionalidad durante los años del 2020 al 2024". Nos resulta imprescindible dirigirnos a la Fiscalía Provincial del Guayas, con fines estrictamente académicos e investigativos, para poder recolectar información acerca de los fiscales encargados de la investigación y acusación de los delitos electrónicos investigado en Guayaquil.

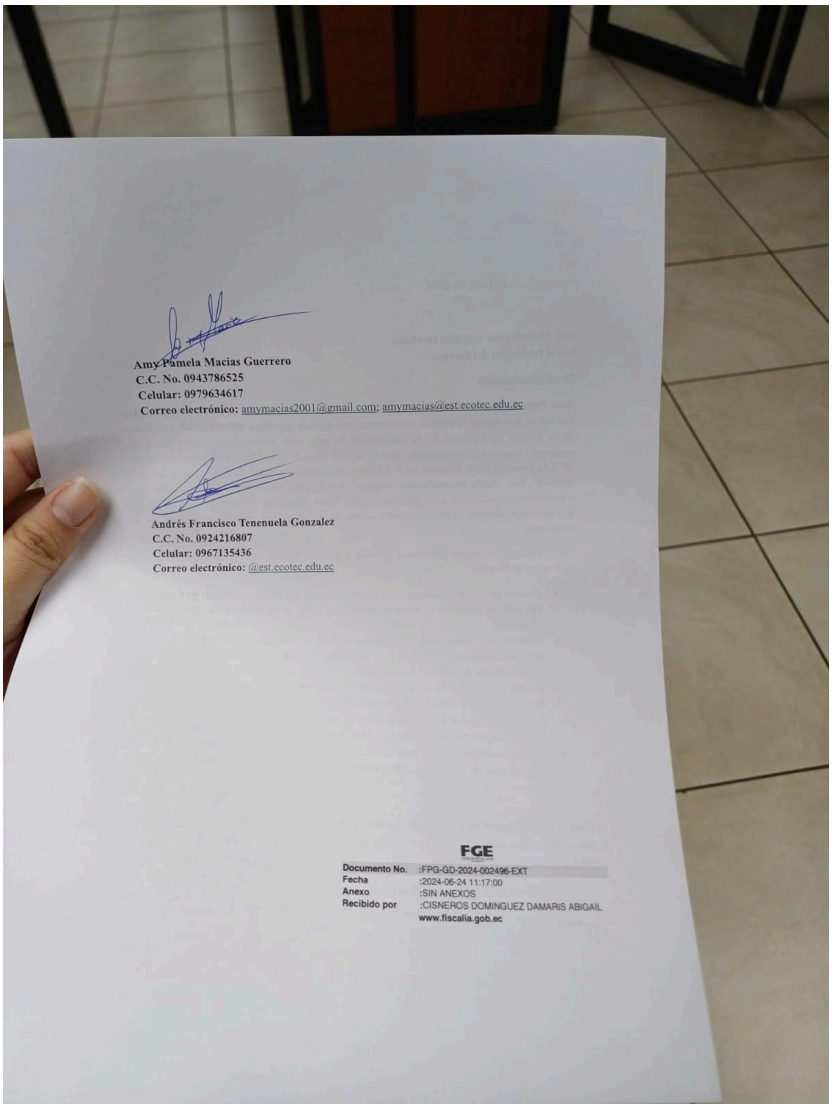
Por lo expuesto en líneas posteriores procedo a detallar, de manera clara la información que pretendemos recopilar:

- Fiscales encargados de la investigación y acusación del delito electrónico de Pornografía con utilización de niñas, niños o adolescentes (**Art. 103 COIP**) dentro de la ciudad de Guayaquil.
- Fiscales encargados de la investigación y acusación del delito electrónico de Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos (**Art. 174 COIP**) dentro de la ciudad de Guayaquil.
- Fiscales encargados de la investigación y acusación del delito electrónico de Violación a la intimidad (**Art. 178 COIP**) dentro de la ciudad de Guayaquil.
- Fiscales encargados de la investigación y acusación del delito electrónico de Apropiación fraudulenta por medios electrónicos (**Art. 190 COIP**) dentro de la ciudad de Guayaquil.
- Fiscales encargados de la investigación y acusación del delito electrónico de Revelación ilegal de base de datos (**Art. 229 COIP**) dentro de la ciudad de Guayaquil.

Petición que hacemos en virtud de los artículos 66 Núm. 23 y 225 de la Constitución; del mismo modo de los artículos 7 y 8 Lit. a) de la ley orgánica de transparencia y acceso a la información pública

Agradecemos su pronta atención al presente requerimiento.

Atentamente,



Correo en respuesta al oficio por parte de la Fiscalía Provincial del Guayas otorgando la información de sobre los fiscales

Fwd: ATENCION DE REQUERIMIENTO DE INFORMACION TRAMITE No. FPG-GD-2024-02496-EXT Recibidos ×

Amy Macias <amymacias2001@gmail.com> 29 jun 2024, 11:29

para mí

---------- Forwarded message ---------
De: **Larisa Maldonado Romero** <maldonadol@fiscalia.gob.ec>
Date: vie, 28 de jun de 2024, 10:38
Subject: ATENCIÓN DE REQUERIMIENTO DE INFORMACIÓN TRAMITE No. FPG-GD-2024-02496-EXT
To: amymacias2001@gmail.com <amymacias2001@gmail.com>, amymacias@est.ecotec.edu.ec <amymacias@est.ecotec.edu.ec>

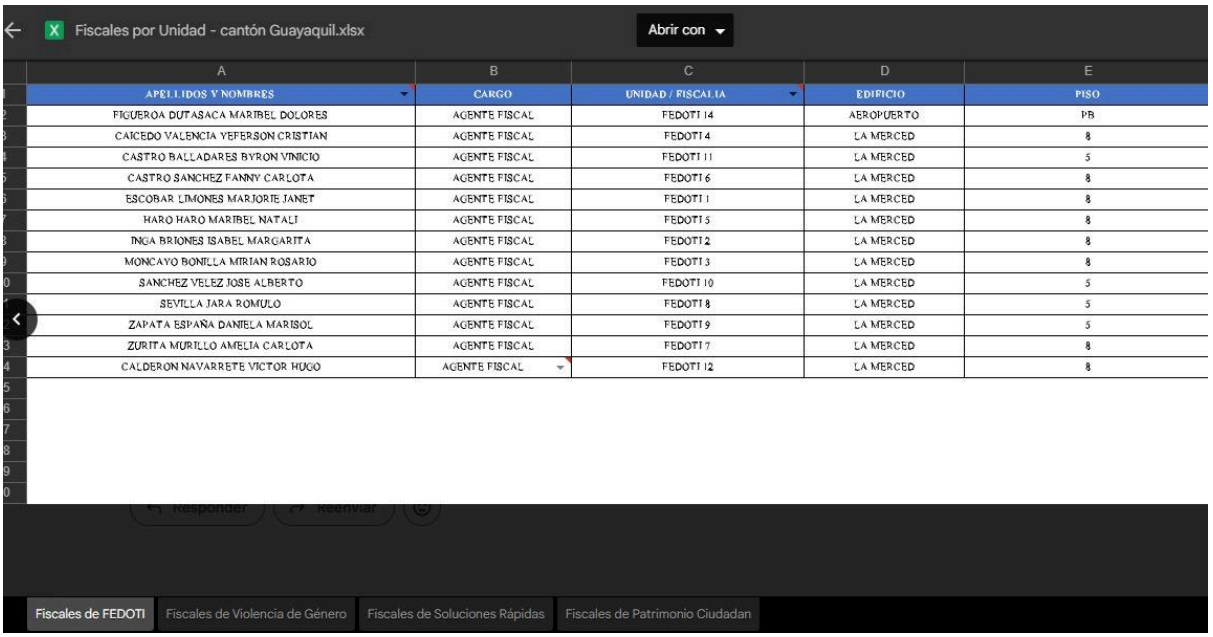
Buenos días:

En atención a su requerimiento recibido mediante Trámite No. FPG-GD-2024-02496-EXT de fecha 24 de junio 2024, me permito indicar lo siguiente:

Art.	Descripción	Unidad Fiscal
103	PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O ADOLESCENTES	FISCALIA DE DELINCUENCIA ORGANIZADA, TRANSNACIONAL E INTERNACIONAL (FEDOTI)
174	OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	FISCALIA DE VIOLENCIA DE GENERO
178	VIOLACIÓN A LA INTIMIDAD	FISCALIA DE SOLUCIONES RAPIDAS
190	APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	FISCALIA DE PATRIMONIO CIUDADANO
229	REVELACIÓN ILEGAL DE BASE DE DATOS	FISCALIA DE SOLUCIONES RAPIDAS

Fuente: Sistema SIAF

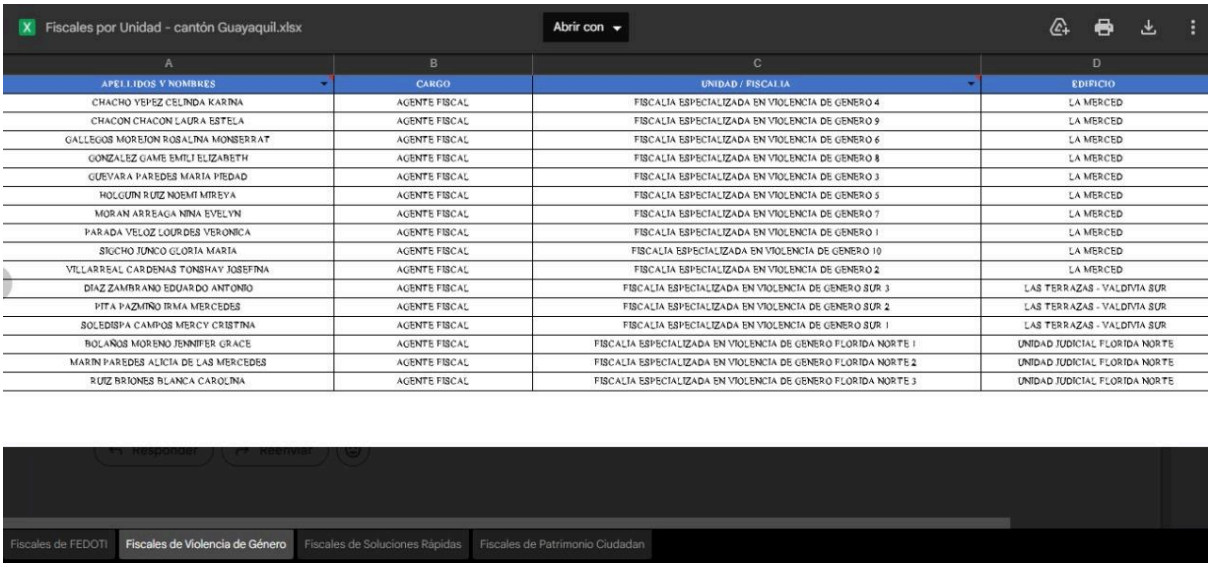
Información sobre los fiscales especializados en ciberdelincuencia y sus ubicaciones otorgadas en formato EXCEL



Fiscales por Unidad - cantón Guayaquil.xlsx — Abrir con

	A	B	C	D	E
1	APELLIDOS Y NOMBRES	CARGO	UNIDAD / FISCALIA	EDIFICIO	PISO
2	FIGUEROA DUTASACA MARIBEL DOLORES	AGENTE FISCAL	FEDOTI 14	AEROPUERTO	PB
3	CAICEDO VALENCIA YEFERSON CRISTIAN	AGENTE FISCAL	FEDOTI 4	LA MERCED	8
4	CASTRO BALLADARES BYRON VINICIO	AGENTE FISCAL	FEDOTI 11	LA MERCED	5
5	CASTRO SANCHEZ FANNY CARLOTA	AGENTE FISCAL	FEDOTI 6	LA MERCED	8
6	ESCOBAR LIMONES MARJORIE JANET	AGENTE FISCAL	FEDOTI 1	LA MERCED	8
7	HARO HARO MARIBEL NATALI	AGENTE FISCAL	FEDOTI 5	LA MERCED	8
8	INGA BRIONES ISABEL MARGARITA	AGENTE FISCAL	FEDOTI 2	LA MERCED	8
9	MONCAYO BONILLA MIRIAN ROSARIO	AGENTE FISCAL	FEDOTI 3	LA MERCED	8
10	SANCHEZ VELEZ JOSE ALBERTO	AGENTE FISCAL	FEDOTI 10	LA MERCED	5
11	SEVILLA JARA ROMULO	AGENTE FISCAL	FEDOTI 8	LA MERCED	5
12	ZAPATA ESPAÑA DANIELA MARISOL	AGENTE FISCAL	FEDOTI 9	LA MERCED	5
13	ZURITA MURILLO AMELIA CARLOTA	AGENTE FISCAL	FEDOTI 7	LA MERCED	8
14	CALDERON NAVARRETE VICTOR HUGO	AGENTE FISCAL	FEDOTI 12	LA MERCED	8
15					
16					
17					
18					
19					
20					

Fiscales de FEDOTI | Fiscales de Violencia de Género | Fiscales de Soluciones Rápidas | Fiscales de Patrimonio Ciudadan



Fiscales por Unidad - cantón Guayaquil.xlsx — Abrir con

A	B	C	D
APELLIDOS Y NOMBRES	CARGO	UNIDAD / FISCALIA	EDIFICIO
CHACHO YEPEZ CELINDA KARINA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 4	LA MERCED
CHACON CHACON LAURA ESTELA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 9	LA MERCED
GALLEGOS MORETON ROSALINA MONSERRAT	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 6	LA MERCED
GONZALEZ GAME EMILI ELIZABETH	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 8	LA MERCED
GUEVARA PAREDES MARIA PIEDAD	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 3	LA MERCED
HOLGUIN RUIZ NOEMI MIREYA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 5	LA MERCED
MORAN ARREAGA NINA EVELYN	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 7	LA MERCED
PARADA VELOZ LOURDES VERONICA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 1	LA MERCED
SIGCHO JUNCO GLORIA MARIA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 10	LA MERCED
VILLARREAL CARDENAS TONSHAY JOSEFINA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO 2	LA MERCED
DIAZ ZAMBRANO EDUARDO ANTONIO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO SUR 3	LAS TERRAZAS - VALDIVIA SUR
PITA PAZMIÑO IRMA MERCEDES	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO SUR 2	LAS TERRAZAS - VALDIVIA SUR
SOLEDISPA CAMPOS MERCY CRISTINA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO SUR 1	LAS TERRAZAS - VALDIVIA SUR
BOLAÑOS MORENO JENNIFER GRACE	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO FLORIDA NORTE 1	UNIDAD JUDICIAL FLORIDA NORTE
MARIN PAREDES ALICIA DE LAS MERCEDES	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO FLORIDA NORTE 2	UNIDAD JUDICIAL FLORIDA NORTE
RUIZ BRIONES BLANCA CAROLINA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN VIOLENCIA DE GENERO FLORIDA NORTE 3	UNIDAD JUDICIAL FLORIDA NORTE

Fiscales de FEDOTI | Fiscales de Violencia de Género | Fiscales de Soluciones Rápidas | Fiscales de Patrimonio Ciudadan

APELLIDOS Y NOMBRES	CARGO	UNIDAD / FISCALIA	EDIFICIO	PISO
ACURIO QUEZADA KATIA ALEXANDRA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS SUR 3	LAS TERRAZAS - VALDIVIA SUR	2
ANDRADE MATUTE JACINTA MARIA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS SUR 4	LAS TERRAZAS - VALDIVIA SUR	2
ARMIJOS MORAN GIOCONDA AUXILIADORA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS SUR 5	LAS TERRAZAS - VALDIVIA SUR	2
ACOSTA CASTRO ROBERT DAVID	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS NORTE 2	MONTECRISTI	3
ALMEIDA VILLEGAS MARTIN FERNANDO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 4	MONTECRISTI	1
BUSTAMANTE LINDAO CARLOS GERMAN	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 1	MONTECRISTI	1
GAIBOR MUÑOZ MARCO ALEXANDER	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS NORTE 1	MONTECRISTI	3
HIDALGO VEGA WILFRIDO RUPERTO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 6	MONTECRISTI	3
LEON TENORIO VICTOR HUGO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 3	MONTECRISTI	1
LUNA QUINDE MICHELL ERIKA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 9	MONTECRISTI	3
MEDINA PINCAY LAURA DEL ROCIO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 8	MONTECRISTI	3
ROMERO JAEN WALTER JUNIOR	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 5	MONTECRISTI	3
TOALA CAÑARTE FREDDY HERIBERTO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 2	MONTECRISTI	1
VERA ARIAS ZOILA PRICILA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN SOLUCIONES RAPIDAS CENTRO 7	MONTECRISTI	3

Fiscales de FEDOTI | Fiscales de Violencia de Género | Fiscales de Soluciones Rápidas | Fiscales de Patrimonio Ciudadan

Fiscales por Unidad - cantón Guayaquil.xlsx

Abrir con

	A	B	C	D	E
	APELLIDOS Y NOMBRES	CARGO	UNIDAD / FISCALIA	EDIFICIO	PISO
	CAMPOS QUINTANA FRANCISCO GUSTAVO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 2	MONTECRISTI	1
	RODRIGUEZ ARBOLEDA NORMA CECILIA	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 1	MONTECRISTI	1
	CAICHE MEJILLON JORGE EDUARDO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 3	MONTECRISTI	4
	LOPEZ AVILA ALEX JAVIER	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 6	MONTECRISTI	4
	PULECIO MONTALVO NICOLAS ERNESTO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 9	MONTECRISTI	4
	SALTOS HAON FRANKLIN ARMANDO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 5	MONTECRISTI	4
	VELA ANDRADE NELSON DANIEL	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 8	MONTECRISTI	4
	VELASCO SOLIS JOFFRE ALFREDO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 7	MONTECRISTI	4
	ZAMBRANO BERMUDEZ GEOVANNI EDILBERTO	AGENTE FISCAL	FISCALIA ESPECIALIZADA EN PATRIMONIO CIUDADANO 4	MONTECRISTI	4

Fiscales de FEDOTI | Fiscales de Violencia de Género | Fiscales de Soluciones Rápidas | Fiscales de Patrimonio Ciudadan

Evidencia de entrevistas realizadas a los fiscales en sus respectivos despachos.


FGE
ASESORÍA DE LA
FISCALÍA PROVINCIAL


FGE
FISCALÍA
VIOLENCIA DE GÉNERO # 6
USO OBLIGATORIO DE
MASCARILLA
FGE
FISCALÍA
VIOLENCIA DE
GÉNERO # 6