74

Fecha de presentación: agosto, 2023
Fecha de aceptación: septiembre, 2023
Fecha de publicación: noviembre, 2023

DESAFIOS LEGALES

EN ECUADOR FRENTE A LOS DELITOS INFORMÁTICOS, IMPORTANCIA DE SU PREVENCIÓN

LEGAL CHALLENGES IN ECUADOR REGARDING COMPUTER CRIMES, IMPORTANCE OF ITS PREVENTION

Ingrid Joselyne Diaz Basurto[1]
Email: uq.ingriddiaz@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-2934-4010
Pablo Mariano Ojeda Sotomayor[1]
Email: uq.pabloos88@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-9082-3649
Cinthia Mariela Cajas Parraga[1]
Email: uq.cinthiacajas@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-2644-0074
Evelyn Paulina Cabrera Ripalda[1]
Email: dp.evelynpcr05@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-5772-6959
[1] Universidad Regional Autónoma de Los Andes, Puyo. Ecuador.

Cita sugerida (APA, séptima edición)

Diaz Basurto, I., J., Ojeda Sotomayor, P. M., Cajas Parraga, C. M & Cabrera Ripalda, E., P. (2023). Desafíos legales en Ecuador frente a los delitos informáticos, importancia de su prevención. ***Universidad y Sociedad 15***(6)746-754.

RESUMEN.

El estudio cualitativo de los delitos informáticos en Ecuador, basado en el Código Orgánico Integral Penal, revela una compleja interacción entre la legislación y la percepción de diversos actores sociales. En la presente investigación se realizaron entrevistas a, jueces, fiscales, abogados, personal bancario y la población general. Las entrevistas arrojan luz sobre la interpretación subjetiva de las leyes y la brecha de conocimiento en torno a los delitos cibernéticos. Se destaca la necesidad de una mayor concienciación y capacitación, especialmente entre el personal judicial y bancario para abordar eficazmente estos crímenes. Además, se evidencia la importancia de la adaptación constante de la legislación para enfrentar los desafíos cambiantes del ciberespacio, asegurando así una respuesta legal efectiva a las amenazas informáticas. Surge la necesidad de alertar a la población para evitar que sean víctimas de tales delitos.

Palabras clave: delitos informáticos, ciberseguridad, legislaciones, seguridad jurídica.

ABSTRACT.

The qualitative study of computer crimes in Ecuador, based on the Comprehensive Organic Penal Code, reveals a complex interaction between legislation and the perception of various social actors. In this investigation, interviews were conducted with judges, prosecutors, lawyers, banking personnel and the general population. The interviews shed light on the subjective interpretation of laws and the knowledge gap around cybercrime. The need for greater awareness and training is highlighted, especially among judicial and banking personnel to effectively address these crimes. Furthermore, the importance of constant adaptation of legislation to face the changing challenges of cyberspace is evident, thus ensuring an effective legal response to computer threats. The need arises to alert the population to prevent them from becoming victims of such crimes.

Keywords: computer crimes, cybersecurity, legislation, legal security.

INTRODUCCIÓN.

La evolución constante de las acciones cibernéticas ha generado nuevas conductas que desafían la legislación existente, creando una problemática global. Aunque los delitos informáticos han sido incluidos en figuras tradicionales, su naturaleza tecnológica demanda una regulación legal continua. Estos delitos, integrados en el crimen organizado, a menudo cuentan con complicidad interna, afectando la seguridad de la información de las organizaciones. La falta de una definición universal del delito informático refleja la dificultad de tipificarlo en los códigos penales, lo cual es evidente en la legislación ecuatoriana y en la mayoría de legislaciones (Acosta, et al. 2020).

El delito informático, definido como una acción antijurídica por vía informática con objetivos económicos, políticos o sociales, presenta desafíos significativos para la legislación. La falta de adaptación de las leyes a las nuevas formas delictivas en el ciberespacio genera una problemática global (Lobo, et al. 2023). Los constantes avances en las acciones cibernéticas complican aún más la regulación, exigiendo una respuesta legal constante. Los delitos informáticos, al desafiar la seguridad jurídica constitucional, requieren nuevas estrategias para proteger los derechos de las personas, sus bienes y pertenencias. La complejidad de regular la informática y la tecnología subraya la necesidad de investigaciones jurídicas para desarrollar mecanismos que aseguren la seguridad jurídica en este ámbito (Arcos-Argudo, et al. 2023).

Identificar los tipos de delitos informáticos es crucial para abordar las consecuencias personales, económicas y sociales de estos actos. La vulnerabilidad de la información personal y financiera destaca la importancia de conocer los riesgos al proporcionar datos a través de plataformas digitales, evitando así convertirse en víctimas de fraudes, extorsiones y chantajes (Vinelli, 2021). El principio constitucional de seguridad jurídica se ve afectado por la dificultad de regular y controlar los delitos informáticos, lo que impulsa la necesidad de desarrollar mecanismos que aseguren la protección de este principio ante las nuevas modalidades delictivas (Villón, et al. 2019).

El fácil acceso a la tecnología ha limitado la seguridad jurídica que las leyes pueden proporcionar, dado que las diversas formas de delinquir en el ciberespacio superan la capacidad normativa del estado ecuatoriano (Santacruz & Hermoza, 2019). La investigación científica se justifica por la creciente incidencia delictiva en el ámbito informático desde la integración de la informática en la vida diaria. Por lo que el objetivo de la presente investigación es conocer y profundizar en el análisis desde lo legal, de los delitos informáticos para garantizar el bienestar ciudadano. Además de realizar propuestas y reformas que pudieran garantizar un mejor tratamiento a estos actos. Así como su prevención en la población de la ciudad de Babahoyo.

MÉTODOS.

Se empleó una metodología de tipo mixta cuali-cuantitativa, con la finalidad de desarrollar una mejor comprensión del problema de investigación. Se obtuvo tanto información cerrada con el fin de medir actitudes hacia el objeto de estudio, como información abierta con el fin de analizar la diversidad de ideas acerca de la temática de estudio. A continuación se describen los métodos de nivel teórico empleados:

- Método histórico lógico: Lo lógico y lo histórico se complementan y vinculan mutuamente. Para poder descubrir las leyes fundamentales de los fenómenos, el método lógico debe basarse en los datos que proporciona el método histórico, de manera que no constituya un simple razonamiento especulativo. De igual modo lo histórico no debe limitarse sólo a la simple descripción de los hechos, sino también debe descubrir la lógica objetiva del desarrollo histórico del objeto de investigación. El método histórico-lógico se aplicó para realizar el estudio y análisis de la evolución histórica de la figura de delitos informáticos, para con ello, desarrollar una visión precisa de los fundamentos de crecimiento de este tipo de ilícitos a lo largo de la historia.
- Método analítico-sintético: A través del método analítico-sintético, se desarrollan dos procesos intelectuales, contrariados, que operan en conjunto, refiriéndose al análisis y la síntesis. El análisis se describe como el conjunto de procedimientos coherentes que permiten la descomposición del objeto de estudio, con el fin de estudiar todas sus partes por separado. En cuanto al proceso de síntesis, se desarrollará el proceso inverso al analítico, estableciendo un análisis de las partes previamente estudiadas (García, et al. 2018). El método analítico permitió realizar un análisis de la normativa legal, con relación a la normativa penal y tratados internacionales sobre los delitos informáticos. Así como de su influencia y su referencia al principio constitucional de seguridad jurídica.
- Método hipotético-deductivo: Este proceso inicia con una hipótesis desarrollada tomando como punto de partida principios, leyes o datos empíricos y mediante la aplicación de las reglas de la deducción. Se desarrollan predicciones que son verificadas de manera empírica, y si existen correspondencia con los sucesos, se comprueba la veracidad hallada en esa hipótesis utilizada como punto de inicio. Mediante la aplicación del método hipotético-deductivo se partió de una idea hipotética del estado del objeto de estudio

a través del análisis sobre los delitos informáticos y su relación al cumplimiento del principio constitucional de seguridad jurídica y mediante esta premisa se deduce la viabilidad y falencias del objeto de estudio.

Técnicas e instrumentos

Dentro de la presente investigación se aplicaron entrevistas a profesionales del derecho en ciudadanía en general, y personal activo dentro del sistema financiero bancario de la ciudad. Para obtener información concreta, real y cotidiana de carácter actualizada acerca de acontecimientos que hayan ocurrido dentro del área de investigación.

Fuentes de información:

Primarias:

1. Entrevistas realizadas a ciudadanía en general.
2. Entrevistas realizadas a profesionales del derecho.
3. Entrevistas realizada a personal activo del sistema financiero bancario de Banco Pichincha y Banco del Pacífico.

Dentro de la presente investigación se realizó un importante número de entrevistas principalmente a profesionales del derecho ciudadanía en general y personal activo dentro del sistema financiero bancario de la ciudad para obtener información concreta real y cotidiana de carácter actualizada acerca de acontecimientos que hayan ocurrido dentro del área de investigación.

Secundarias:

1. Información bibliográfica
2. Periódicos y noticieros virtuales.
3. Páginas de Internet.

Información obtenida y desarrollada dentro de la presente investigación científica se obtuvo a partir de diferentes textos y búsquedas bibliográficas revistas diarios y páginas de internet correctamente certificadas los cuales han servido para obtener datos históricos actuales y estadísticos para con ello obtener un trabajo de alta calidad y confiabilidad.

Población y muestra: para el desarrollo del trabajo investigativo se contará con la ayuda de varios profesionales del Derecho entre ellos: fiscales (2), abogados en libre ejercicio (20), ciudadanos (24), jueces con competencia en materia penal (4), empleados del sistema financiero (20), de ellos Empleados (12) y Directivos (8).

Fórmula para el cálculo de la muestra ver Ecuación 1

$$n = \frac{N^* Z_\alpha^2 \ p^* q}{d^{2*}(N-1) + Z_\alpha^{2*} \ p^* q} \quad (1)$$

Donde:

- N = Total de la población
- Zα= 1.96 al cuadrado (si la seguridad es del 95%)
- p = proporción esperada (en este caso 5% = 0.05)
- q = 1 – p (en este caso 1-0.05 = 0.95)
- d = precisión (en su investigación use un 5%).

Aplicación de la fórmula

N= 24 sociedad en general

N= 26 profesionales del derecho

N= 20 Personal activo del sistema financiero bancario

RESULTADOS Y DISCUSIÓN.

Como se mencionó en el epígrafe correspondiente a la metodología, el presente estudio desarrolló una búsqueda bibliográfica documental. De esta búsqueda se consideró oportuno mencionar aspectos que siguen a continuación, para brindar una mejor comprensión del tema. También se mostrarán los resultados de las entrevistas a los distintos actores de la sociedad que conformaron la muestra del presente estudio.

Principales conceptos de delito informático:

La concepción de la figura de delito ha estado íntimamente relacionada con las fases de desarrollo que ha tenido la sociedad a lo largo de la historia a causa de las distintas ideologías concebidas en cada una de las etapas de la humanidad. Dentro de la evolución histórica de la humanidad han existido innumerables concepciones sobre la figura del delito, siendo las más importantes las concebidas dentro del iusnaturalismo del siglo XX y el Iuspositivismo de finales del mismo siglo.

Todas las ramas desarrolladas del conocimiento humano han sido adecuadas para funcionar a través de sistemas informáticos, es decir, la ciencia, la tecnología, el ámbito profesional y hasta el ámbito personal han ido adecuando sus formas de funcionamiento a medios electrónicos y sistemas de información, ofreciendo el acceso sin limitaciones a grandes conjuntos de datos que en tiempos de antaño no podían ubicarse sino después de grandes búsquedas y selecciones minuciosas de información, en el cual el trabajo del hombre jugaba un papel determinante, mientras que las máquinas ofrecían un papel secundario y auxiliar (Macías-Lara et al., 2022).

Los autores Garzón Tapia & Vizuete Gallardo (2009), conciben que la figura jurídica del delito informático nace a partir de la evolución de las tecnologías informáticas y de las tecnologías de la información y comunicaciones (TIC). En un principio, las diferentes organizaciones gubernamentales internacionales decidieron que los delitos informáticos debían ser encuadrados en las figuras tradicionales reguladas. Sin embargo, la realidad fue, que la utilización de las tecnologías de la información y comunicaciones generaron un sin número de nuevas alternativas delictuales, que no se pudieron encuadrar en los delitos cotidianos prescritos dentro de las legislaciones, hecho que generó impunidad a este tipo de actividades y consecuencias altamente nocivas y dañinas para la sociedad.

Numerosos eruditos del derecho han hecho grandes esfuerzos para poder alcanzar una definición concreta acerca del delito informático, y aunque no se ha logrado un concepto que pueda globalizar lo que representa el delito informático, si se ha conseguido formular diferentes concepciones que respaldan a las características concretas de casos surgidos, como la presencia de una conducta en común: la aplicación de técnicas informáticas con la finalidad de obtener un resultado concreto. A pesar de que se han conseguido resultados notables a la hora de la concepción de una definición concreta acerca del delito informático, cada vez son más los debates que surgen sobre esta temática (Serrano, 2021).

Tipos de delitos informáticos:

Dentro de la categoría de delitos informáticos cabe destacar que existen diferentes formas del cometimiento de este tipo de ilícitos, las mismas que se agrupan en categorías muy importantes y diferentes como lo son: 1) fraude cibernético; 2) sabotaje cibernético; 3) el espionaje cibernético; y 4) accesibilidad ilegal a sistemas informáticos. Cabe destacar que no existe un orden de peligrosidad según su la presente referencia.

1. En el ámbito del fraude cibernético se mencionan las siguientes formas delictivas:

a) Falsificación de datos electrónicos: Se genera en el momento de la producción e introducción de datos digitales falsos en sistemas informáticos con la finalidad de desarrollar movimientos artificiales en las acciones y transacciones que puede desarrollar una empresa.

b) Vulneración de programas informáticos: Este tipo de delitos se conciben al momento de que una persona oculte programas de espionaje en medios informáticos ajenos, para poder generar nuevas acciones no autorizadas dentro de un sistema informático.

c) Phishing: este tipo de acción ilícita consiste en la obtención de datos personales por parte de la víctima, a través de la utilización de engaños como páginas falsas, con la finalidad de obtener identificaciones para poder acceder a cuentas bancarias, solicitar préstamos u obtener tarjeta de crédito a nombre de la víctima para hacer un mal uso de estas (Bascur & Sepúlveda, 2022).

2. En el ámbito del sabotaje Cibernético se encuentran las siguientes formas delictivas:

a) Bombas Lógicas: Un tipo de virus informático que destruye la estructura de funcionamiento básico de cualquier sistema informático.

b) Gusanos: Virus informático, que tiene la finalidad de infiltrarse en programas o redes informáticas para procesar modificar o destruir información digital.

c) Malware: Virus informático destinado a reproducirse dentro de un sistema informático, para ralentizarlo y destruirlo

d) Ciberterrorismo: Acciones de opresión en contra de un gobierno o sociedad a través de medios informáticos.

e) Incapacitación de servicio electrónico: Tiene la finalidad de qué el dispositivo electrónico objetivo desarrolle un consumo excesivo de memoria hasta que se produzca una sobrecarga en el sistema y lo dejé inhabilitado.

3. En el ámbito del Espionaje Cibernético se encuentran las siguientes formas delictivas:

a) Fuga de datos: Este delito consiste en propagar o hacer público diferentes tipos información de carácter confidencial de una persona o de una empresa.

b) Vulneración de derechos de autor: Está tipología delictual se relaciona directamente con la piratería informática a causa de qué consiste en el uso de manera ilegal de software sujeto a derechos de autor.

4. En el ámbito del acceso ilegal a sistemas informáticos:

a) Key Master: Herramienta informática que tiene la capacidad de acceso a cualquier tipo de archivo con la finalidad de alterar Su contenido borrar o copiar información

b) Intervención de líneas de comunicación: Alteración de líneas de telecomunicaciones que tiene la finalidad de extraer datos o conversaciones que circulan por esa línea de comunicación.

c) Piratería informática: Desarrollo de ataques hacia un sistema informático que se produce de manera externa Y qué interviene en contra de los sistemas de seguridad de un sistema de información (Bascur & Sepúlveda, 2022).

Características principales de los delitos informáticos

- Es una acción que posee estudios avanzados en la rama de la informática para su probatoria delictual.
- Son acciones que no necesitan desarrollarse desde el lugar donde se causan los daños, puesto que a través de los medios electrónicos se puede acceder al desarrollo del delito a la distancia.
- Este tipo de acciones son accesibles a cualquier tipo de persona puesto qué no necesitan de una inversión grande de capital simplemente es necesario un equipo tecnológico y el acceso internet.
- Este tipo de acciones son denominados delitos de guante blanco a causa de que los sujetos activos suelen ser personajes con un gran intelecto y preparación para ejecutarlos
- Al ser acciones de tan fácil acceso cada año Se incrementa el número de posibles agentes delictuales sobre este tipo de delitos.
- No existen leyes penales concretas que penalicen la comisión de este tipo de actos delictivos.
- Los procesos de resolución de este tipo de actos delictuales son de carácter lento, debido a la falta de leyes que regulen este tipo de conductas y a la falta de mecanismos procesales para tratar adecuadamente este tipo de actos.
- Este tipo de delitos también son accesibles a menores de edad puesto que no existen regulaciones sobre el uso de tecnologías de redes informáticas.
- Este tipo de delitos por lo general se desarrollan sin que la víctima se dé cuenta.
- La mayoría de casos sobre delitos informáticos zona cometidos normalmente por organizaciones criminales especializadas en informática las cuales tienen como objetivo perjudicar a instituciones y obtener beneficios tanto económicos como sociales (Mera & Gallegos, 2023).

Principio constitucional a la seguridad jurídica

La constitución del Ecuador representa la supremacía normativa dentro de la política ecuatoriana, es decir, que la constitución está por encima de cualquier otro tipo de normativa vigente dentro del estado ecuatoriano. En ella se albergan todos los derechos de los que gozan las personas miembros del estado ecuatoriano, así como la organización política, social y económica que se aplica dentro del territorio (Campos, 2019). La Constitución de la República del Ecuador del año 2008 estableció en base a los derechos y garantías de las personas miembros de la sociedad ecuatoriana el concepto de derecho a la seguridad jurídica, el cual consiste en la capacidad del Estado ecuatoriano de brindar un marco normativo capaz de salvaguardar los derechos de la sociedad, así como la creación de herramientas jurídicas que puedan ser aplicadas por autoridades competentes para llevar a cabo este fin (Ecuador. Asamblea Nacional Constituyente, 2008).

El tema de la seguridad jurídica está vinculado con el principio de legalidad. Pero el principio constitucional de seguridad jurídica en representación de un valor social y como un elemento representativo de una cultura jurídica va más allá de una simple referencia al principio legalidad. Puesto que este implica un derecho adquirido por el simple hecho de ser humano, es irrenunciable y de un nivel superior a cualquier otro derecho. Y el cual implica el desarrollo de un sistema normativo que pueda ser aplicado con una conducta judicial clara e impecable estable y eficaz (Mera & Gallegos, 2023).

La interceptación ilegal de datos

El delito de interceptación ilegal de datos consta en el artículo 230 del Código Orgánico Integral Penal (COIP). Este sanciona con tres a cinco años de pena privativa de libertad a quienes utilicen estos datos y los difundan. Otro delito que se comete por medios electrónicos es la utilización de adolescentes con fines sexuales o pornográficos, donde se propicia la inducción, promoción y facilitan la prostitución de una persona menor de edad. A estos actos, el COIP sanciona en el artículo 174, con una pena privativa de libertad de siete a 10 años. También está el robo de datos es cuando una persona duplica una página institucional como la de un banco o de una compañía de comercio electrónico y, sin advertir que es falsa, el usuario realiza alguna transacción (Ecuador. Asamblea Nacional, 2014).

Los ataques de las cibermafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3 183 delitos informáticos. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1 851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650

investigaciones a escala nacional. Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias con más casos. Gonzalo García, jefe de la Unidad de Ciberdelitos, dice que este tipo de hechos delictivos ocurren porque las personas tienen más acceso a Internet y redes sociales. Cifras oficiales muestran que el 79,21% de la población ecuatoriana tiene acceso a la web y alrededor de 15,8 millones de personas en el país tienen cuentas en las diferentes redes sociales.

Un informe de la Interpol (Policía Internacional) también menciona que "el mundo está más conectado digitalmente que nunca. Los delincuentes están aprovechando esa transformación en línea para atacar, a través de las redes y sistemas informáticos". Cinco tipos de estos ilícitos se han cometido con mayor frecuencia en el país. Estos son: la estafa en línea, violación a la intimidad, el acceso no consentido a un sistema informático, el ataque a la integridad de sistemas informáticos y la apropiación fraudulenta por medios electrónicos. Precisamente, para contrarrestar estos actos delictivos, la Policía ha ejecutado 38 operativos en dos años y medio. Además, en ese período, los uniformados han detenido a 39 personas que presuntamente cometieron ciberdelitos (Aparicio-Izurieta, 2022).

Resultados de la evaluación cualitativa de las entrevistas:

Entrevistas a los abogados:

1. El personal judicial evaluado, reflexionó sobre la Complejidad Jurídica de los delitos informáticos. Considerando cómo la legislación actual se enfrenta a la rápida evolución tecnológica.
2. Destacaron la necesidad de una mayor especialización en el campo legal para abordar de manera efectiva estos delitos, reconociendo la complejidad técnica de estos casos.
3. Reflejaron la importancia de la cooperación internacional en la lucha contra los delitos informáticos, reconociendo que muchos de estos casos trascienden las fronteras nacionales.
4. Se abordó la necesidad urgente de fortalecer las leyes que protegen los datos personales y la privacidad, dada la creciente cantidad de información sensible en línea.
5. Refieren que este tipo de delitos constituyen grandes desafíos específicos que se enfrentan al investigar los delitos informáticos, como la necesidad de peritos técnicos y la recopilación de evidencia digital. Además de la capacidad de la legislación para adaptarse rápidamente a las innovaciones tecnológicas y a nuevos métodos empleados por los delincuentes cibernéticos.
6. Se destaca la importancia de aumentar la conciencia pública sobre la ciberseguridad y los riesgos asociados con los delitos informáticos. Reflexionaron sobre el equilibrio necesario entre fortalecer la seguridad cibernética y garantizar la protección de los derechos individuales y la privacidad de los ciudadanos.

Entrevistas a los trabajadores del sistema bancario:

1. Los trabajadores bancarios en Babahoyo expusieron lo referente al impacto financiero directo de los delitos informáticos en los clientes, considerando pérdidas económicas y fraudes bancarios.
2. Mencionaron que los delitos informáticos respecto a la confianza del cliente con el sistema financiero pueden afectar la percepción que tienen los clientes sobre la seguridad de los servicios bancarios en la ciudad. Estos incidentes de delitos informáticos podrían afectar la reputación de la institución bancaria en Babahoyo, reconociendo la importancia de la imagen pública.
3. Los delitos informáticos podrían llevar a restricciones en el acceso a servicios financieros, especialmente si los clientes temen por la seguridad de sus cuentas. Consideran la necesidad de mejorar la educación financiera para ayudar a los clientes a comprender y prevenir los delitos informáticos, fortaleciendo así su capacidad para protegerse.
4. Señalan la preocupación por la seguridad de los datos personales de los clientes y cómo los delitos informáticos podrían comprometer esta información sensible. Consideran la necesidad de la colaboración entre el sistema bancario y las autoridades locales para abordar y prevenir los delitos informáticos. Reconociendo la importancia de un enfoque conjunto para la seguridad financiera en la ciudad.

Entrevistas y testimonios de personales naturales:

Testimonios de varias personas víctimas de delitos informáticos:

1. Pérdida de Ahorros: "Fui víctima de una estafa en línea y perdí una gran parte de mis ahorros. Aprendí la dura lección de ser más cauteloso con mis transacciones en línea".
2. Suplantación de Identidad: "Alguien suplantó mi identidad en línea y realizó compras fraudulentas. Fue una pesadilla desentrañar todo y demostrar que no era yo quien había realizado esas transacciones".
3. Falsa Oferta de Empleo: "Caí en una oferta de trabajo falsa en línea. Envié información personal y nunca recibí el trabajo. Ahora, tengo miedo de buscar empleo en línea".

4. Phishing Bancario: “Recibí un correo electrónico falso que parecía ser de mi banco. Ingresé mi información y mi cuenta bancaria fue vaciada”.
5. Ransomware en Negocio: “Mi pequeño negocio fue víctima de ransomware. Perdí el acceso a todos mis archivos y tuve que pagar una gran suma para recuperar la información”.
6. Fraude en Compras en Línea: “Compré un producto en línea y nunca llegó. Resultó ser un sitio falso”.
7. Robo de Datos Personales: “Mis datos personales fueron robados en un ataque cibernético. Ahora, estoy constantemente preocupado por posibles consecuencias y he tenido que tomar medidas extra para proteger mi identidad”

Entrevistas:

1. La población entrevistada reflexionó sobre la importancia de estar conscientes de los riesgos asociados con los delitos informáticos y las estafas en línea. Considerando que los delitos informáticos pueden dejar a las personas en una situación financiera vulnerable, con pérdidas de dinero que podrían afectar sus vidas cotidianas. Destacando la importancia de la educación en ciberseguridad para ayudar a las personas a identificar posibles estafas y proteger sus datos personales en línea.
2. Algunas de las personas entrevistadas manifestaron su temor a ser víctima de una estafa en línea. Aspecto que afecta el bienestar psicológico de la población. Atentando contra los principios de seguridad ciudadana y la política del “Buen vivir”.
3. Asumen la importancia de proteger sus propios datos personales y cómo las estafas en línea pueden comprometer esta información sensible. Y la necesidad de fomentar la denuncia de estos actos para contribuir a la prevención y persecución de estos actos ilegales.
4. Estas personas entrevistadas manifestaron falta de conocimientos respecto a la ciberseguridad y los delitos informáticos de manera general. Aspecto que resalta la necesidad de orientación a la población en este tema tan sensible y que ya ha afectado a muchos. Manifestaron la necesidad de adaptarse continuamente a las nuevas tendencias y tácticas utilizadas por los estafadores en línea, manteniéndose informados sobre las amenazas emergentes.

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 cuando entró en vigor el COIP hasta el 31 de mayo del 2015. En el COIP se sancionan los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros (Gutiérrez, et al. 2023).

Según el fiscal provincial de Pichincha, Wilson Toainga, las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor. El fiscal Edwin Pérez, especialista en delitos informáticos, indicó que en Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología. Por cuanto, la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país (Arcos-Argudo et al., 2023).

Un inconveniente para la investigación radica en que Ecuador no cuenta con convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información personal. Este aspecto ante las formalidades y la virtualidad de los procesos puede tardarse meses. Se considera oportuno que se pueda desarrollar una propuesta de reforma a la sección tercera, capítulo tercero, del título IV” infracciones en particular”, del Código Orgánico Integral Penal, con la intención de que a partir del artículo 234 de la norma referida se agreguen nuevas conductas consideradas como delitos informáticos.

Con el fin de fortalecer la aplicación del principio de seguridad jurídica prevista en la Constitución de la República del Ecuador, aquello sin perjuicio de las conductas penales en el marco de la tecnología e informática ya establecidas, como son los delitos de:

- Pornografía con utilizaciones de niños, niñas o adolescentes (Art. 103 COIP).
- Violación a la intimidad (Art. 178 COIP).
- Revelación ilegal de base de datos (Art. 229).
- Interceptación ilegal de datos (Art. 230 COIP)
- Transferencia electrónica de activo patrimonial (Art. 231 COIP)
- Delitos contra la información pública clasificada legalmente (Art. 233 COIP)
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones (Art. 234 COIP).

Esta propuesta iría dirigida de manera directa hacia la sociedad en general. Puesto que la legislación ecuatoriana debe dar pasos hacia adelante en los procesos de

legislación y regulación de delitos informáticos. Teniendo en cuenta que este tipo de actos ilícitos crecen con una mayor rapidez a lo que pueden reaccionar las leyes penales en la actualidad.

CONCLUSIONES.

El enfoque legal en los delitos informáticos es crucial para salvaguardar la privacidad de las personas y proteger la integridad de sus datos personales en un mundo cada vez más digitalizado. Es esencial para preservar la estabilidad financiera de individuos y empresas. Las regulaciones adecuadas pueden prevenir fraudes electrónicos, ataques a sistemas bancarios y otras amenazas que afectan directamente a la seguridad económica de la sociedad.

Fomentar un entorno legal sólido para abordar los delitos informáticos contribuye a mantener la confianza en las tecnologías digitales. La percepción de seguridad en línea es fundamental para la adopción y el desarrollo continuo de las innovaciones tecnológicas.

La atención legal a los delitos informáticos es esencial para mantener el orden social al garantizar que aquellos que violan la ley en el ciberespacio sean responsables de sus acciones. Esto promueve un entorno en el que la sociedad puede prosperar sin amenazas persistentes a través de medios electrónicos.

Se desarrollaron bases jurídicas y bibliográficas acerca de la presencia de los delitos informáticos en la legislación ecuatoriana. Llegando a la conclusión de que se enlistan una serie limitada de delitos informáticos. Este hecho que denota la necesidad de desarrollar y tipificar más conductas penalmente relevantes de los delitos a través de medios electrónicos y sistemas informáticos.

El ordenamiento jurídico ecuatoriano necesita la inclusión de nuevas figuras jurídicas que penalicen más acciones u omisiones desarrolladas a través de mecanismos informáticos, electrónicos y redes de información. Con la finalidad de abarcar la mayor cantidad posible de formas de atentar contra la integridad del estado o de la sociedad a través de la informática y con ello aplicar fortaleza al principio de seguridad jurídica.

REFERENCIAS BIBLIOGRÁFICAS.

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. ***Revista Venezolana de Gerencia, 25***(89), 351-368. https://www.redalyc.org/journal/290/29062641023/html/

Aparicio-Izurieta, V. V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. Sapienza: ***International Journal of Interdisciplinary Studies,*** ***3***(1), 1057-1063. https://pdfs.semanticscholar.org/98b5/7583d0852dac6edf7e13b5e9c84df4c350e7.pdf

Arcos-Argudo, M., Matute-Pinos, K., & Fernández-Mora, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. Revista ***Ibérica de Sistemas e Tecnologias de Informação***, (E60), 100-114. https://www.proquest.com/openview/d29c2f8f2bdc11ccd4644ff0be3d8b56/1?pq-origsite=gscholar&cbl=1006393

Bascur, G., & Sepúlveda, R. P. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. ***Revista de Estudios de la Justicia***, (37), 1-38. https://rej.uchile.cl/index.php/RECEJ/article/view/67885

Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. ***Revista Científica Hallazgos21, 4***(1), 100–111. https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Ecuador. Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. ***Registro Oficial No. 449***. Gobierno del Ecuador. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf.

Ecuador. Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento 180. Gobierno del Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

García Tamayo, R., Soler Lahittebignott, M. C. & Latorre Artega, S. (2018). La investigación científica y el método clínico para la formación del profesional de la salud. Biblioteca virtual de Derecho, Economía y Ciencias Sociales. https://www.eumed.net/2/libros/1703/investigacion-cientifica.html

Garzón Tapia, Pamela Natally y Vizuete Gallardo, Marco Fernando. (2009). El fraude informático: valoraciones técnico- jurídicas. (Tesis de grado, Universidad Técnica de Cotopaxi). http://repositorio.utc.edu.ec/handle/27000/139

Gutiérrez, G. A. S., García, N. A. Q., Alcívar, L. L. C., & Chancay, S. X. E. (2023). Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador. Polo del Conocimiento, 8(5), 1137-1153. https://mail.polodelconocimiento.com/ojs/index.php/es/article/view/5630

Lobo, M. M., Gil, S. V. H., & Aguirre, A. M. G. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. ***Revista de ciencias sociales, 29***(2), 356-372. https://dialnet.unirioja.es/descarga/articulo/8920556.pdf

Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q., Loor, J. J. M., Estupiñan-Troya, G., & Vizuete, J. D. R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. Sapienza: ***International Journal of Interdisciplinary Studies, 3***(2), 231-243. https://www.journals.sapienzaeditorial.com/index.php/SIJIS/article/download/324/199

Mera, J. M. R., & Gallegos, M. J. V. (2023). La categoría dogmático penal de la tipicidad, el principio de legalidad y los delitos informáticos en la legislación ecuatoriana: Ciberseguridad y criminalidad informática. ***Desafíos Jurídicos, 3***(4), 24-37.

Santacruz, H. B., & Hermoza, M. M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. ***Revista Ibérica de Sistemas e Tecnologias de Informação***, (E20), 391-400. https://www.proquest.com/openview/fc081b269b3464d67367cafb7a4b1d66/1?pq-origsite=gscholar&cbl=1006393

Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. ***Lucerna Iuris Et Investigatio***, (1), 29–47. https://doi.org/10.15381/lucerna.v0i1.18373

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2019). Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana. ***Revista Ibérica de Sistemas e Tecnologias de Informação***, (E17), 671-677. https://www.proquest.com/openview/b7f8919dbb75fa3e5f21552a48e94816/1?pq-origsite=gscholar&cbl=1006393

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. ***Ius Et Praxis, 53***(053), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995