Universidad Nacional de Loja

Facultad Jurídica, Social y Administrativa

Carrera de Derecho

Estudio jurídico y doctrinario sobre el ciber delito denominado phishing y la falta de normativa legal que regule los delitos informáticos.

Trabajo de Integración Curricular previo a la obtención del Título de Abogado.

AUTOR:

Andy Javier Iñahuazo López

DIRECTOR:

Dr. Freddy Ricardo Yamunaqué Vite, PhD.

Loja – Ecuador

2024

Educamos para Transformar

Certificación

Loja, 01 de marzo del 2023

Dr. Freddy Ricardo Yamunaqué Vite. Ph.D.
DIRECTOR DE TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **Estudio Jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta de normativa legal que regule los delitos informáticos,** previo a la obtención del Título de **Abogado**, de la autoría del estudiante **Andy Javier Iñahuazo López,** con **cédula de identidad** Nro. **1150594586**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa**.**

Dr. Freddy Ricardo Yamunaqué Vite. Ph.D.
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Andy Javier Iñahuazo López**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos o acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular, en el Repositorio Digital Institucional - Biblioteca Virtual.

Firma:

Cédula: 1150594586

Fecha: 16 de enero del 2024

Correo electrónico: andy.inahuazo@unl.edu.ec

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y publicación electrónica del texto completo del Trabajo de Integración Curricular.

Yo, **Andy Javier Iñahuazo López,** declaro ser el autor del presente Trabajo de Integración Curricular denominado: **"Estudio jurídico y doctrinario sobre el ciber delito denominado phishing y la falta de normativa legal que regule los delitos informáticos",** como requisito para optar por el Título de **Abogado**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 16 días del mes de enero del dos mil veinticuatro.

Firma:

Autora: Andy Javier Iñahuazo López.

Cédula: 1150594586

Correo: andy.inahuazo@unl.edu.ec

DATOS COMPLEMENTARIOS

Director del Trabajo de Integración Curricular: Dr. Freddy Ricardo Yamunaqué Vite. Ph.D.

Dedicatoria

El presente trabajo de investigación lo dedicó a mis Padres, José Emiliano Iñahuazo Jumbo y Dorys del Carmen López Sarango y a mis hermanos/as, quienes fueron pilar fundamental, motivándome a lo largo de la realización de esta investigación.

Andy Javier Iñahuazo López

Agradecimiento

Agradezco a la Universidad Nacional de Loja, a la Facultad Jurídica Social y Administrativa, al director de mi Trabajo de Integración Curricular Dr. Freddy Yamunaqué, quien, con su conocimiento y profesionalismo, supo brindarme las herramientas necesarias para culminar mi trabajo, del mismo modo, agradezco a la distinguida planta docente por haberme brindado los conocimientos necesarios a lo largo de mi formación profesional.

Por último, mi más sincero agradecimiento, a todas aquellas personas que de alguna u otra manera, fueron participes y me aportaron conocimiento para lograr satisfactoriamente, la culminación del presente trabajo de investigación.

"Considero más valiente al que conquista sus deseos, que al que conquista a sus enemigos, ya que la victoria más dura, es la victoria sobre uno mismo" -Aristóteles-

Andy Javier Iñahuazo López

Índice de contenidos

Portada……..…….i

Certificación ii

Autoría..... iii

Carta de autorización..... iv

Dedicatoria..... v

Agradecimiento vi

Índice de contenidos..... vii

1. Título 1

2.Resumen..... 2

2.1Abstract…..... 3

3.Introducción 4

4. Marco Teórico 6

4.1 Generalidades..... 6

4.1.1 Espectro Radioeléctrico..... 6

4.1.2 Internet..... 6

4.1.3 Tecnologías de las Información y Comunicación 7

4.1.4. TIC como herramientas para el fin delictivo: 8

4.2 Delito, Delito Informático y sus generalidades..... 9

4.2.1 Delito: 9

4.2.2 Teoría del delito..... 10

4.2.3 Delito Informático 12

4.3 Sujetos del Delito Informático 12

4.3.1 Sujeto Activo: 13

4.3.2 Sujeto Pasivo: 14

4.4 Bien Jurídico Protegido:.....14

4.5 Tipos de Delitos Informáticos 14

4.5.1. El Phishing.....17

4.5.2- Breve reseña histórica del Phishing.....19

4.5.3. Modus Operandi del Phishing.....19

4.6 Criminalidad 20

4.6.1. Criminalidad Informática 21

4.7 Importancia del Derecho Informático.....22

4.8 Derecho Informático 24

4.8.1. Vulneración del Bien Jurídico en delitos Informáticos 24

4.9 Bienes Jurídicos vulnerados en el delito informático de Phishing 25

4.9.1 Derecho a la Privacidad:.....25

4.9.2 Seguridad Jurídica:.....26

4.9.3. Tutela Judicial Efectiva 27

4.9.4. Principio de Legalidad 29

4.9.5. Interpretación de la norma 30

4.10Convenio de Budapest.....31

4.11Delitos Informáticos en Ecuador 33

4.12Criminalidad Informática en Ecuador 36

4.12.1. Datos proporcionados por fiscalía general del estado 38

4.12.2 Estafa…. 40

4.12.3 Suplantación de Identidad.....40

4.12.4 Apropiación fraudulenta por medios electrónicos 40

4.12.5 Acceso no consentido a un sistema informáticos 41

4.12.6 Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos 41

4.13 Derecho Comparado.....41

5. Metodología 45

5.1. Materiales utilizados. 45

Materiales de Oficina.....45

5.2. Métodos: 46

5.3. Técnicas.....47

6. Resultados..... 48

6.1 Resultados de las encuestas.....48

Gráfica 1 49

Gráfica 2 51

Gráfica 3 52

Gráfica 4 54

Gráfica 5 55

6.2 Resultados de las entrevistas:.....57

6.3 Estudio de Casos 64

7. Discusión 68

7.1Verificación de los Objetivos 68

7.2 Objetivo General. 69

7.3 Objetivos Específicos. 69

7.4 Fundamentación jurídica de la propuesta de reforma legal 71

8. Conclusiones: 72

9. Recomendaciones..... 73

9.1 Proyecto de Reforma al Código Orgánico Integral Penal.....73

10. Bibliografía..... 76

11. Anexos 78

Cuestionario Encuestas y Entrevistas. 78

Cuestionario de Entrevista. 80

Índice de tablas:

Gráfica 1 49

Gráfica 2 51

Gráfica 3 52

Gráfica 4 54

Índice de figuras:

Gráfica 1 49

Gráfica 2 51

Gráfica 3 52

Gráfica 4 54

Gráfica 5 55

Índice de anexos

Cuestionario Encuestas y Entrevistas. 78

Cuestionario de Entrevista. 80

Certificado de abstract ……..81

1. Título

“Estudio jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta denormativa legal que regule los delitos informáticos.”

2.Resumen

El presente trabajo de investigación titulado "Estudio jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta de normativa legal que regule los delitos informáticos", tiene como objetivo realizar un análisis profundo a la legislación ecuatoriana, así como también a las normas existentes en el ámbito de delitos informáticos, además de resaltar la trascendencia e importancia que merecen los delitos informáticos en la sociedad actual.

En particular, el presente trabajo, se enfoca en el delito informático de Phishing, el cual consiste en la obtención de manera fraudulenta de información de carácter confidencial, como contraseñas, datos financieros u otra información personal o sensible, por medio del uso de las tecnologías de la información y comunicación. Así mismo se analiza como esté afecta y vulnera múltiples derechos constitucionales que son fundamentales para los ciudadanos.

El Ecuador al ser un Estado que se fundamenta en el respeto y garantía de los derechos, tiene el deber y obligación de desarrollar las herramientas necesarias para prevenir y combatir las vulneraciones a los derechos de los ciudadanos, por tanto, el sistema jurídico ecuatoriano deberá implementar instrumentos eficaces, como lo son, la actualización constante de normas jurídicas, que busquen la tipificación y sanción a las nuevas formas de delinquir, en este caso la de los delitos informáticos, que se desarrollan a la par con el avance de las tecnologías y que están en constante evolución.

Para el desarrollo del presente trabajo de investigación se implementó el uso de diferentes métodos y técnicas como son; el análisis e interpretación de textos y normas jurídicas, así como también, entrevistas y encuestas, a fin de obtener información de carácter relevante para la presente investigación.

Del mismo modo se resuelve y verifica los objetivos planteados y se concluye con una propuesta de reforma al Código Orgánico Integral Penal, con el fin de reforzar el derecho a la seguridad jurídica y al no estado de indefensión en el sentido de delitos informáticos.

Palabras claves: Ciberdelito, Phishing, Vulnerabilidad, Seguridad Jurídica, Delitos Informáticos.

2.1Abstract

The present research work entitled “Estudio jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta de normativa legal que regule los delitos informáticos” aims to carry out a deep analysis of Ecuadorian legislation, as well as the existing rules in the field of computer crimes, in addition to highlighting the transcendence and importance that computer crimes deserve in the current society.

Particularly, this research work focusses on the computer crime of Phishing which consist of fraudulently obtaining confidential information, such as passwords, financial data or other personal or sensitive information, through the use of information and communication technologies. It also analyzes how this affects and violates multiple constitutionals rights thatare fundamental for citizens.

Ecuador, being a state that is based in the respect for and guarantee of rights, has the duty and obligation to develop the necessary tools to prevent and combat violations of citizens’ rights. Therefore, the Ecuadorian legal system must implement effective instruments, such as the constant updating of legal norms which seek the classify and sanction new forms of crime, in this case computer crimes, which develop in parallel with theadvancement of technologies which are in constantly evolving.

For the development of this research work, different methodologies and techniques were implemented such as the analysis and interpretation of texts and legal norms, as well as interviews and surveys, in order to obtain relevant information for this research.

In the same way, the proposed objectives are resolved and verified, and a proposal for reform of the Codigo Organico Integral Penal is concluded with the aim of strengthening the right to legal security and the non-state of defenselessness in the sense of computer crimes.

Key words: Cybercrime, Phishing, Vulnerability, Legal Security, Computer Crimes.

3.Introducción

El desarrollo de la presente investigación titulada "Estudio jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta de normativa legal que regule los delitos informáticos" está enfocado en el análisis del delito informático Phishing, en su contexto, estructura, bien/es jurídicos que vulnera, así mismo como en el empleo indispensable de las tecnologías de la información y comunicación, como medio o fin para la consumación de los delitos informáticos.

Durante los últimos años, hemos sido testigos de cambios sin precedentes en la forma en que nos comunicamos con el mundo debido al avance constante de las tecnologías de la información y la comunicación. Estos cambios han traído eficiencia, conectividad y accesibilidad, aportando numerosos beneficios a nuestra vida diaria. Pero, como suele ocurrir con los grandes avances, también trae consigo nuevos desafíos, particularmente en el ámbito de la ciberseguridad.

En este contexto, la presente investigación pretende estudiar y analizar un aspecto importante de esta revolución tecnológica: el delito informático phishing el cual consiste en engañar a las personas por medio del uso de Tecnologías de la Información y Comunicación, para obtener información confidencial, como contraseñas, números de tarjetas de crédito o detalles de cuentas bancarias. Los ciberdelincuentes que realizan phishing suelen hacerse pasar por entidades de confianza, como bancos, empresas u organizaciones gubernamentales, y envían mensajes engañosos a través de correos electrónicos, mensajes de texto o incluso redes sociales, lo cual se ha convertido en una de las amenazas más graves y una de las más empleadas por los ciber delincuentes.

A través de su análisis exhaustivo, este estudio revela no sólo la naturaleza compleja del phishing, sino también su impacto global. Este delito cruza fronteras, afecta tanto a personas como a empresas y viola derechos fundamentales como la privacidad, la propiedad, la seguridad informática y la confianza en los medios digitales.

Una parte importante de este estudio se centra en la falta de disposiciones legales efectivas y específicas para combatir el cibercrimen en el contexto ecuatoriano. A medida que los ciberdelincuentes continúan desarrollando sus métodos y estrategias, está claro que se necesita una respuesta legal fuerte y moderna para garantizar que las autoridades puedan perseguir y castigar efectivamente a quienes cometen delitos en línea.

En este contexto, el estudio también incluye datos estadísticos actualizados que muestran los altos índices de criminalidad asociados a los delitos informáticos en Ecuador. Estas estadísticas proporcionan una imagen clara y relevante de la magnitud del problema y de la urgente necesidad de abordar estas cuestiones desde una perspectiva jurídica, del mismo modo, esta investigación proporciona un análisis detallado de las características, métodos y consecuencias del phishing, así como de los vacíos legales que dificultan perseguir y castigar el phishing y otros delitos informáticos, a fin de contribuir a mejorar la comprensión de los ciberdelitos y sugerir medidas específicas para prevenirlo. A través de estadísticas de vanguardia y un enfoque interdisciplinario, se pretende arrojar luz sobre cuestiones críticas en el entorno legal y tecnológico actual. Se señala también, la necesidad de establecer leyes claras y efectivas que permitan a las autoridades investigar y procesar a los responsables de estos delitos, haciendo hincapié en mejorar la cooperación internacional y la implementación de medidas preventivas, para garantizar una respuesta efectiva y coordinada a nivel mundial.

De esta manera queda expuesto el presente trabajo de investigación, con el ánimo de que el presente trabajo sirva de guía útil para estudiantes y profesionales del Derecho, convirtiéndose en una fuente de consulta y conocimiento en la lucha contra los delitos informáticos, Así mismo, se espera que sus hallazgos fomenten el debate sobre la importancia de una regulación efectiva con el fin de garantizar el derecho constitucional de las personas a la seguridad jurídica, promoviendo una legislación penal sólida y actualizada que aborde adecuadamente los delitos informáticos en la era digital.

4. Marco Teórico

4.1 Generalidades

Para entrar en contexto con la presente investigación es importante resaltar todo lo relaciona al medio por el cual se originan estas nuevas figuras delictivas, ya que el uso de dichos medios es indispensable para concretar o consumar el hecho penalmente relevante, el cual es objeto del presente estudio como lo son los delitos informáticos y en específico el delito informático de Phishing.

4.1.1 Espectro Radioeléctrico

Para dar un sentido de definición al Espectro Radioeléctrico, eh tomado como referencia la definición dada por la Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), la cual menciona que: "El espectro radioeléctrico constituye un subconjunto de ondas electromagnéticas u ondas hertzianas fijadas convencionalmente por debajo de 3000 GHz, que se propagan por el espacio sin necesidad de una guía artificial. A través del espectro radioeléctrico es posible brindar una variedad de servicios de telecomunicaciones que tienen una importancia creciente para el desarrollo social y económico de un país" (ARCOTEL, 2015)

En base a este concepto podemos entender por su definición técnica, la cual indica que, el Espectro Radioeléctrico está constituido por ondas electromagnéticas, entendido en el sentido de que estas ondas no son física, ni apreciables al ojo humano, pero están presentes en el espacio, del mismo modo, nos demuestra la importancia que tiene el Espectro Radioeléctrico ya que, es un medio indispensable para lograr las telecomunicaciones, entendido por esto, a la telefonía, radio, televisión, Wifi, entre otras, lo cual es clave para el desarrollo social y económica de nuestro país.

El Art.313 de la Constitución de la Republica del Ecuador señala que; "El estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficacia" (Constitución de la Republica del Ecuador, 2008). Este artículo es importante ya que muestra como el estado ecuatoriano tiene el derecho de administrar los sectores estratégicos, en esto cabe el espectro radioeléctrico ya que, en la citada norma suprema se determina que este, es uno de los considerados como sector estratégico, por ende, le corresponde al estado no solo el derecho sino también el deber de regular, controlar y gestionar dicho sector.

4.1.2 Internet

Para entender el significado de este, me ha sido necesario tomar como base al concepto dado por la Real Academia de la Lengua Española, la cual señala que Internet es una "Red Informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación" (Real Academia de la lengua Española, 2023). Dicho de este modo, señala que Internet no necesariamente se refiere a una sola cosa, sino más bien, a un conjunto de redes informáticas de computadoras interconectadas entre sí, que juntas crean un organismo descentralizado, es decir, no tiene un control central que disponga su funcionamiento.

En la obra titulada "Internet y el Derecho", el autor Antonio Pérez, señala que "Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia" (Pérez, 1998).

Esto nos dice que el Internet se ha constituido como un elemento primordial para el desarrollo social y económico mundial, de modo que logra que los usuarios interactúen entre sí, intercambiando cualquier tipo de información, desde cualquier parte del mundo y sin barreras ni limitaciones que lo impidan, esto a su vez permite el desarrollo comercial y por consiguiente el desarrollo económico de las naciones, al permitir que se realice acciones o transacciones que antes solo eran posibles de manera física.

El Art. 88.1 de La Ley Orgánica de Telecomunicaciones señala que: "Todas las personas tienen el derecho a participar en la sociedad de la información. El Estado garantizará el acceso universal al servicio público de internet, de conformidad con la Constitución de la República" (Ley Orgánica de Telecomunicaciones, 2015). El presente artículo establece que todos los ecuatorianos tenemos el derecho a participar dentro de la sociedad de la información, esto refleja el reconocimiento e importancia de la inclusión digital y subraya queel acceso a Internet y a los servicios relacionados es esencial para el ejercicio de otros derechos y para la aplicación activa en la sociedad.

4.1.3 Tecnologías de las Información y Comunicación

Es importante destacar en qué consisten las Tecnologías de la Información y Comunicación, esto a fin de comprender su impacto y como estas desempeñan un papel fundamentas en la actual sociedad moderna.

Tomando como referencia el estudio realizado por Roberto Baelo e Isabel Cantón

en su obra titulada “Las tecnologías de la información y la comunicación en la educación superior”, en la que citan al autor Matinez Sánchez en su distinción realizada al conceptualizar a las TIC “podemos entender por nuevas tecnologías a todos aquellos medios de comunicación y de tratamiento de la información que van surgiendo de la unión de los avances propiciados por el desarrollo de la tecnología electrónica y las herramientas conceptuales, tanto conocidas como aquellas otras que vayan siendo desarrolladas como consecuencia de la utilización de estas mismas nuevas tecnologías y del avance del conocimiento humano” (Roberto Baelo, Isabel Cantón, 2009).

En otras palabras, las Tecnologías de la Información y Comunicación abarcan todo lo que como resultado se da, de la fusión de avances tecnológicos y creatividad conceptual, y esto incluye tanto tecnologías que ya conocemos como aquellas que aún no han sido desarrolladas, pero que surgirán a medida que avance el conocimiento y la innovación. Esta definición también, proporciona una introducción general a las TIC y es importante enfatizar que las TIC abarcan una amplia gama de tecnologías que han cambiado la forma en que vivimos, trabajamos y nos comunicamos en la sociedad moderna.

Es claro indicar que, así como se dan distintos avances en lo tecnológico, también se dan en lo social y a esto hago referencia a que, así como la tecnología ha avanzado y evolucionado, a la par, también lo han hecho las formas de delinquir, ya que, gracias a estos avances, los ahora denominados delitos informáticos, no necesaria mente son perpetrados de manera física, sino que usan estas herramientas sea como medio o fin para delinquir, vulnerando así, los derechos de las personas.

4.1.4. TIC como herramientas para el fin delictivo:

Las nuevas herramientas digitales han sofisticado los delitos tradicionales. Para robar dinero, por ejemplo, ya no hay que robar un banco. Inclusive, la tecnología ha permitido ataques cibernéticos que jamás nos hubiéramos imaginado. El cibercrimen no es una amenazadel futuro para la que nos debemos preparar. Es una amenaza del presente para la que no estamos preparados (Banco Interamericano de Desarrollo, 2018).

En base al presente concepto se destaca la creciente sofisticación de los delitos tradicionales debido a las herramientas digitales que refleja la inminente realidad del cibercrimen en el mundo actual. Por tanto, es menester, analizar lo que trae consigo esta evolución delictiva.

Las nuevas tecnologías han permitido que los delincuentes puedan adaptarse y evolucionar a partir de los métodos tradicionales, tomando como ejemplo el propuesto en el concepto analizado, que, para cometer un delito en relación al dinero, ya no es necesario atacar físicamente a la víctima, ya que los ahora denominados ciberdelincuentes pueden realizarlo de forma remota a través de transacciones electrónicas fraudulentas, esto gracias a las herramientas digitales o tecnologías de la información y comunicación.

-Ataques cibernéticos: Los avances en la tecnología han dado lugar a ataques cibernéticos sofisticados que pueden afectar a personas, empresas e incluso gobiernos. Los delincuentes informáticos pueden ingresar a los sistemas informáticos para robar datos confidenciales, cometer fraude, interrumpir servicios y causar daños graves. Detectar y monitorear estos ataques puede resultar difícil debido a su complejidad y a la capacidad de los delincuentes de ocultar sus identidades en línea.

-Una amenaza actual: A pesar de la percepción general de que el cibercrimen es una amenaza del futuro, el cibercrimen ya es un problema complejo y urgente presente ya en nuestra sociedad. Las organizaciones y las personas están constantemente bajo ataque en línea. Los ciberdelincuentes aprovechan las vulnerabilidades de la seguridad digital para cometer delitos como robo de identidad, fraude financiero y propagación de malware. No prepararse adecuadamente para estas amenazas puede tener graves consecuencias para las víctimas y la propiedad.

-La necesidad de estar preparados: Dada la naturaleza actual y real del cibercrimen, es esencial que las empresas, los gobiernos y los individuos estén adecuadamente preparados. Esto a su vez incluye, que las legislaciones se actualicen constantemente a la par de los avances tecnológicos, ya que el deber de cada estado es garantizar, la seguridad jurídica a sus ciudadanos.

4.2 Delito, Delito Informático y sus generalidades

Para lograr abordar este tema de forma correcta es menester desarrolla una conceptualización precisa a lo que se denomina delito, así como también a los elementos que lo conforman.

4.2.1 Delito:

La definición que nos expone el autor Guillermo Cabanellas de la obra Diccionario Jurídico Elemental acerca del delito es que: “Etimológicamente, la palabra

delito proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena. En general, culpa, crimen, quebrantamiento de una ley imperativa. AGOTADO. El que además de consumado ha conseguido todos los objetivos que el autor se proponía y cuantos efectos nocivos podía producir el acto delictivo. CASUAL. Considerado subjetivamente, el que surge de modo repentino por un estímulo pasional, por una oportunidad tentadora para nimos débiles" (Cabanellas, 1993).

Este concepto claramente ofrece dos perspectivas sobre el término "delito". La primera es que Etimológicamente, esta palabra se deriva del latín "delictum", la cual se refiere al acto jurídico y doloso castigado con una pena. Dicho de otro modo y en un contextogeneral, el delito implica culpa, crimen o violación de una ley imperativa.

Del mismo modo el término "agotado" al que refiere en dicha conceptualización, es usado para describir un delito que ha sido consumado y que ha alcanzado todos los objetivos propuestos por el autor, incluyendo así también, todos los efectos nocivos que el acto delictivo pudo producir. En el caso del término "casual", refiere a que un delito surge de manera repentina a causa de un estímulo pasional o a una oportunidad tentadora, esto especialmente se genera en individuos con una voluntad débil.

El delito supone varias conceptualizaciones en base a diversos autores, quienes han proporcionado diversas definiciones; sin embargo, todas convergen en una idea fundamental:"El delito se refiere a cualquier comportamiento humano o conducta, típica, antijuridica y culpable". Esto implica que, para considerar a una conducta humana como delito, se debe verificar que esta cumpla con ciertas características y elementos, que, de no verificarse, no sepodría denominar o catalogar a una conducta como delito.

Por lo tanto, es de suma importancia entender, en qué consisten estos elementos que diferencian a la conducta humana, como delito o no y para ello conceptualizare estos elementos de forma resumida y detallada.

4.2.2 Teoría del delito

El profesor Raúl Zaffaroni en su obra Manual de Derecho Penal, describe a la teoría del delito como: "La teoría del delito, como sistema de filtros que permite abrir sucesivos interrogantes acerca de una respuesta habilitante de poder punitivo por parte de las agencias jurídicas, constituye la más importante concreción de la función reductora del derecho penal en cuanto a las leyes penales manifiestas" (Zaffaroni, 2006).

El concepto propuesto por el maestro Zaffaroni, describe a la teoría del delito

comoun marco conceptual complejo e importante en el campo del derecho penal, el cual es propuesto como un sistema de filtrado que permitiría a las autoridades judiciales formularse preguntas detalladas y rigurosas antes de imponer sanciones penales.

En esencia, esta teoría es una herramienta fundamental del derecho penal, en el sentido en que actúa como un mecanismo para evaluar y justificar el ejercicio del poder punitivo por parte del Estado, es así que el derecho penal juega un papel importante en el establecimiento de los límites y salvaguardias del sistema legal, esto ya que limita la actuación de los ciudadanos en busco de la armonía y control social y fortalece la integridad del sistema legal penal.

Para describir cada uno de los elementos de la teoría del delito, he revisado y analizado varios textos, así como también material audiovisual, en los que se explica cada uno de ellos, es así que he logrado desarrollar conceptos de fácil comprensión para el lector.

Conducta: La conducta es el primer paso para determinar si un acto es un delito, lo que se define como, aquel comportamiento voluntario de una persona, sea por acción u omisión. Esta acción u omisión debe ser consciente y libre. Es decir, los individuos deben controlar su comportamiento y comprender lo que están haciendo. Una acción puede ser positiva, como robar algo, o negativa, como no ayudar a alguien en peligro cuando legalmente se lo exige.

Tipicidad: La tipicidad se refiere a la coherencia entre el comportamiento de una persona y los elementos descritos en la ley para un delito en particular. Cada delito se define por un conjunto de factores que deben cumplirse para que la conducta se considere típica. Si el comportamiento de una persona reúne todos los elementos de un delito, ese comportamiento se considera típico y puede considerarse un delito.

Antijuridicidad: Se refiere al conflicto entre un acto y el ordenamiento jurídico existente. Si bien un acto puede ser típico, es decir, acorde con lo descrito en el tipo penal, no puede ser considerado delito si existe una justificación que lo legitime. Esto puede ser; razones justificables, como la legítima defensa o el cumplimiento de una obligación legal, pueden anular la ilegalidad del acto. Esto significa que, aunque el comportamiento es común,no se considera un delito.

Culpabilidad: La culpa se refiere a la culpa moral y psicológica de una persona que ha cometido un acto culposo. Esto significa que el individuo comprende que sus acciones sonilegales y tiene la capacidad de actuar según ese entendimiento. La culpa es

la libertad y la capacidad de una persona de elegir no cometer un delito. Una persona sólo puede ser declarada culpable si tenía la capacidad de comprender el significado y las consecuencias de sus actos en el momento de cometer el delito.

En base a los conceptos dados, se puede entender que para que se configure a una conducta como delito esta debe cumplir con los elementos antes descritos y que a falta de uno de ellos este acto dejaría de configurarse como delito, por lo que no tendría por qué ser penalmente relevante.

4.2.3 Delito Informático

El delito informático es cualquier uso ilegal, delictivo, inmoral o no autorizado de dispositivos electrónicos e Internet, con el objetivo de invadir, destruir o dañar la propiedad de partidos u organizaciones**.** También conocido como ciberdelito, cubre un amplio abanico de acciones ilícitas de diferente naturaleza. El factor común es la tecnología de la información, ya sea un medio o un fin en sí mismo (Revista Seguridad 360, 2021).

Haciendo alusión a dicho concepto se entiende que el delito informático, también es conocido como ciberdelito, y este se refiere a cualquier actividad ilegal, delictiva o no autorizada relacionada con el uso de dispositivos electrónicos e Internet, es decir que emplea a las tecnologías de la información y comunicación para perpetrarlo. El objetivo principal de los delitos informáticos es invadir, destruir o dañar la propiedad de una persona, empresa u organización, además, es de naturaleza diversa y puede incluir una amplia gama de actividades ilegales. Lo que tienen en común estas actividades, es el uso de la tecnología de la información y comunicación, que puede ser tanto una herramienta como un fin en sí mismo, esto a su vez, es aprovechado por los ciberdelincuentes, ya que, utilizan la tecnología para explotar vulnerabilidades en sistemas y redes informáticas para obtener acceso no autorizado, robar información confidencial o dañar sistemas informáticos.

4.3 Sujetos del Delito Informático

El Dr. Santiago Acurio del Pino en su obra “Delitos informáticos: Generalidades” señala que, en derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o

varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo (Acurio Del Pino, 2016).

Este párrafo destaca la importancia de dos sujetos en el derecho penal: el sujeto activo, que comete el delito, y el sujeto pasivo, que sufre las consecuencias. Ambos pueden ser personas naturales o jurídicas. Además, subraya que el bien jurídico protegido determina la identidad y posición de los sujetos en relación con el delito. Es crucial entender quién es el sujeto pasivo, que puede diferir del perjudicado, incluso involucrando a terceros. El ofensor, al lesionar el bien protegido, se convierte en el sujeto activo del delito.

4.3.1 Sujeto Activo:

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos (Acurio Del Pino, 2016).

Esta sección describe las características de las personas que cometen delitos cibernéticos. A diferencia de los delincuentes comunes, el sujeto activo de los delitos informáticos tiene habilidades especiales para manipular sistemas informáticos. También en ocasiones, suelen ocupar puestos estratégicos en entornos laborales donde se maneja información sensible. Es importante tener en cuenta que estas personas pueden tener altos conocimientos de informática incluso si no trabajan en un campo relacionado. Esto indica queel conocimiento técnico es una característica distintiva entre este tipo de delincuentes.

Estas habilidades especializadas pueden permitirles cometer delitos informáticos, lo que subraya la necesidad de medidas de seguridad adecuadas para proteger la información confidencial en eltrabajo y en línea.

4.3.2 Sujeto Pasivo:

En primer término, tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros (Acurio Del Pino, 2016).

Dicho de este modo, el sujeto pasivo del delito informático, pueden ser personas o instituciones como agencias de crédito o gobiernos que utilizan sistemas informáticos automatizados. Estos sistemas, que a menudo están conectados a otros sistemas, son vulnerables a acciones maliciosas por parte de actores activos con habilidades de manipulación de tecnologías de la información. La complejidad y escala del delito cibernético resalta la importancia de la protección de la información y la necesidad de medidas de seguridad sólidas tanto para individuos como para instituciones.

4.4 Bien Jurídico Protegido:

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales (Acurio Del Pino, 2016).

El concepto propuesto enfatiza la importancia de los "objetos jurídicos" en el derecho penal. Esto se refiere al daño o destrucción de un bien, debido a las acciones de un sujeto involucrado en un delito. Esto es muy importante para comprender el delito porque representa la razón de ser de un delito. Aunque no suele estar claramente establecida en los delitos penales, la forma jurídica es fundamental para determinar qué bienes o intereses pretende proteger la ley. La preservación de dichos bienes o intereses será una consideración clave al evaluar si la conducta en cuestión constituye un delito y, de ser así, qué tipo de delito se ha cometido. En cuestión, el propósito de la ley es central para comprender el propósito del delito y su impacto en la sociedad.

4.5 Tipos de Delitos Informáticos

El autor Jesús Loredo, en su obra "Delitos Informáticos", menciona que: "Los delitos informáticos abarcan una gran variedad de modalidades como se mencionan en la

web de la interpol y se enlista a continuación: Ataques contra sistemas y datos informáticos usurpación de la identidad Distribución de imágenes de agresiones sexuales contra menores estafas a través de internet intrusión en servicios financieros en línea Difusión de virus Botnets (redes de equipos infectados controlados por usuarios remotos) Phishing (adquisición fraudulenta de información personal confidencial)" (Jesús Loredo, 2013).

El autor nos muestra distintas modalidades de delitos informáticos, el cual basa esta información a lo descrito por la Interpol, estas modalidades incluyen ataques contra sistemas y datos informáticos, donde los delincuentes pueden intentar filtrarse en sistemas para acceder, robar o manipular información sensible y de carácter confidencial, también se menciona la usurpación de identidad, que implica el uso no autorizado de la información personal de otra persona para cometer fraudes u otros delitos en línea.

Por su parte, el auto Marco Saltos en su artículo denominado "Análisis conceptual deldelito informático en Ecuador", comenta que "Las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:

Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Fraude efectuado por manipulación informáticas de los procesos de cómputo.

Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

La Bomba lógica o cronológica; la cual exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas Informáticos o Hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

Reproducción no autorizada de programas informáticos de protección legal; lacual trae una pérdida económica sustancial para los propietarios legítimos" (Saltos Salgado, 2021).

El amplio espectro de actividades delictivas en el ámbito digital que ha delineado, basándose en las definiciones de las Naciones Unidas, subraya la complejidad y la diversidad del delito informático en la era digital actual, es así que, estas características demuestran cómo los ciberdelincuentes han desarrollado formas sofisticadas y especializadas de cometer delitos en línea.

El fraude informático, incluido el robo de datos y la manipulación de software, se ha convertido en un delito común que afecta tanto a personas como a organizaciones.

La falsificación y alteración de datos almacenados electrónicamente indican que las computadoras se han convertido en herramientas para crear documentos falsos.

Destruir su computadora mediante acciones como la eliminación no autorizada de datos tiene como objetivo interrumpir el funcionamiento normal del sistema, y los virus y gusanos son programas maliciosos que pueden infiltrarse en otros programas y causar dañosgraves.

- La creación de bombas lógicas o de tiempo pone de relieve el nivel de conocimientos técnicos necesarios para cometer determinados delitos cibernéticos.
- El acceso no autorizado por parte de piratas informáticos a servicios o sistemas informáticos abarca desde la simple curiosidad hasta el sabotaje y el espionaje, lo que

refleja la variedad de motivaciones detrás de estos delitos.

- Además, la copia no autorizada de programas informáticos no sólo constituye una violación de los derechos de autor, sino que también causa graves pérdidas económicas a los propietarios legales de los programas.

Estas características resaltan la necesidad urgente de una legislación sólida y medidasde seguridad cibernética para proteger tanto a las personas como a las empresas de diversas formas de delitos cibernéticos. Además, se enfatiza la importancia de la cooperación internacional y el intercambio de información para responder eficazmente a las amenazas transnacionales.

4.5.1. El Phishing

El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusiónal intento de hacer que los usuarios "muerdan el anzuelo". A quien lo practica se le llama phisher. También se dice que el término phishing es la contracción de password harvesting fishing (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que la escritura 'ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua forma de hacking telefónico conocida como phreaking (Coldono, 2022).

El origen del término phishing, de la palabra inglesa "fishing", pone de relieve el carácter engañoso de esta actividad. La analogía de la pesca es el intento de un atacante de "atraer" a un usuario, animándolo a morder el anzuelo y revelar información confidencial como contraseñas, números de tarjetas de crédito o información financiera confidencial. Las actividades de phishing incluyen una variedad de técnicas engañosas diseñadas para engañara los usuarios haciéndoles creer en comunicaciones fraudulentas que parecen legítimas.

El uso de \'ph\' en lugar de \'f\' en palabras relacionadas con la informática como phreaking (una forma de piratería telefónica) es común entre los piratas informáticos y se ha convertido en parte de la jerga digital, estas comunicaciones de phishing demuestran la paciencia, la astucia y la tenacidad de los ciberdelincuentes que intentan "pescar" información valiosa.

En cuanto a un posible acrónimo de "pesca de contraseñas", cabe señalar que la comunidad de habla inglesa ha adoptado el término phishing para describir específicamente este tipo de fraude en línea. El vínculo de "pesca de contraseñas" tiene sentido dada la naturaleza de la actividad, pero probablemente sea una declaración

retrospectiva destinada a simplificar la terminología existente.

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia (Malwarebytes, 2022).

En un contexto legal, en base al concepto citado anteriormente, el phishing se considera un delito cibernético que utiliza el robo de identidad para engañar a las personas para que proporcionen información confidencial, como contraseñas y números de tarjetas de crédito. Estas prácticas suelen llevarse a cabo a través de correos electrónicos o mensajes de texto fraudulentos enviados desde fuentes confiables como bancos, colegas o agencias gubernamentales. Estos mensajes suelen contener amenazas o advertencias diseñadas para asustar a las víctimas para que revelen información confidencial o hagan clic en enlaces maliciosos, por tanto, es fundamental que las personas estén conscientes de los riesgos asociados con el phishing y tomen medidas para proteger su información confidencial.

En contexto, se indica que el objetivo del phishing es obtener datos confidenciales de los usuarios para utilizarlos en actividades delictivas, con el fin de afectar el patrimonio de otras personas. Se menciona que la persona que comete este delito se conoce como "phisher", además, se hace referencia a la importancia de estar atentos a las señales de actividad sospechosa en línea para evitar caer en este tipo de engaños. La intención detrás de este engaño es llevara las personas a divulgar información personal y confidencial, como números de cuenta bancaria, contraseñas o información de tarjetas de crédito.

El phishing, por tanto, es una actividad ilegal que puede causar graves perjuicios a las víctimas de esta modalidad de delitos cibernéticos, incluyendo la pérdida de datos personales y financieros, el robo de identidad, y la exposición a otras formas de fraude y delitos cibernéticos.

4.5.2- Breve reseña histórica del Phishing

Las primeras personas que expusieron el concepto del phishing, fueron Jerry Félix y Chris Hauck en una conferencia de Interex celebrada en el año 1987 debido a un documento presentado que se llamaba *"Sistema de Seguridad: La perspectiva de un Hacker"*. El phishing comenzó a ser practicado a mediados de la década de los 90. La primera empresa que sufrió estos ataques fue American Online (AOL); era la principal proveedora de servicio de internet en el país. Esto captó la atención de los ciberdelincuentes. En esa época, por medio de algoritmos, se creaban tarjetas de crédito falsas con las que era fácil obtener una suscripción gratis a este servicio. Una vez la compañía de internet descubrió esto, creó una herramienta llamada AOHell, que bloqueaba todos los ataques de una manera más automatizada. En vista de eso, los ciberdelincuentes se hacían pasar por empleados de AOL y empezaron a enviar mensajes a los usuarios de esta empresa a través del servicio de mensajería instantánea, donde solicitaban su contraseña para "solventar un problema". La compañía se aseguraba de mantener a sus usuarios informados sobre estas estafas; al final de la mensajería instantánea salía un aviso que decía: "Nadie que trabaje en AOL le pedirá su contraseña o información de facturación". La empresa de internet logró librarse de todos estos ataques a sus usuarios legítimos en el año 1997 (Enciso, 2021).

El hecho de que los ciberdelincuentes hayan evolucionado y adaptado para hacerse pasar por empleados de AOL demuestra la naturaleza inteligente y engañosa del phishing, que solicita las contraseñas de los usuarios a través de mensajes instantáneos, siendo el phishing una amenaza persistente en el mundo digital y cómo las empresas y usuarios han tenido que evolucionar para protegerse contra estas tácticas cada vez más sofisticadas.

Además, la precaución de AOL al notificar a los usuarios sobre estas estafas y advertir contra el intercambio de información confidencial resalta la importancia de la concientización del usuario para prevenir el phishing.

4.5.3. Modus Operandi del Phishing

El fenómeno del phishing ha evolucionado significativamente con el tiempo, lo que hallevado al desarrollo de roles profesionales para quienes participan en esta actividad delictiva. Esta especialización ha creado un grupo de trabajo altamente coordinado y eficiente en la implementación de ataques de phishing. Esta división del trabajo ha dado

lugar a una estructura organizativa que permite a los delincuentes llevar a cabo sus actividades de una manera más eficiente y sofisticada.

Dentro de esta dinámica y en base al estudio y postulados de algunos autores, eh tomado pertinente conceptualizar, 3 categorías principales que demuestran de mejor forma ordenada, el modus operandi en el delito de Phishing.

Mensajeros: Aquel responsable del envío masivo de correos electrónicos o mensajes de texto con contenido engañoso. Estos mensajes están destinados a mostrar los nombres de organizaciones confiables, como bancos, corporaciones y agencias gubernamentales. El objetivo es convencer a las víctimas de que revelen información confidencial, como contraseñas o datos financieros.

Recopiladores / Relectores: Los recolectores tienen la tarea de crear sitios web falsos o fraudulentos que redirigen a los destinatarios de los correos electrónicos de mensajes. Estos sitios web están diseñados para parecerse a plataformas legítimas, convenciendo a las víctimas de que están interactuando con un servicio real. Cuando las víctimas ingresan información en estos sitios, los recopiladores recopilan datos confidenciales y los almacenan para su uso posterior

Cajeros: Se considera así a aquel, encargado de la toma de información recopilada por los recolectores y la utilizan para realizar diversas actividades ilegales. Esto puede incluirla creación de tarjetas de crédito falsas, el envío de dinero fraudulento, la compra de bienes y servicios en línea y la venta de información robada en el mercado negro.

La fragmentación de roles en las actividades de phishing refleja la sofisticación y complejidad de este tipo de delito. También destaca la necesidad de mejorar las medidas de prevención y seguridad para contrarrestar este tipo de actividades delictivas y proteger a los usuarios de Internet de posibles ataques de phishing.

4.6 Criminalidad

Cabanellas describe a la criminalidad en su obra “Diccionario Jurídico Elemental” como: “calidad o circunstancia por la cual es criminal una acción. También, volumen total deinfracciones o proporción en que se registran los crímenes en general, y las varias clases de crímenes en particular, en una sociedad o región determinada y durante cierto espacio de tiempo” (Cabanellas, 1993).

El presente concepto hace referencia a dos aspectos básicos en el ámbito del derecho penal: la calidad o circunstancias que conducen a la sanción de un hecho, el

número total de delitos y el ritmo con el que se registran los distintos tipos de delitos en una sociedad o regiónen cierto periodo de tiempo.

La primera visión enfatiza la importancia de las características o circunstancias específicas que hacen que un acto sea un delito. En el derecho penal existen diferentes elementos que determinan que un acto es delito, los cuales ya fueron explicados anteriormente, pero a modo de indicación, estos elementos son: Conducta, Tipicidad, Antijuridicidad, Culpabilidad.

Desde la segunda perspectiva, se refiere al número total de delitos y la proporción de diferentes delitos ocurridos en una sociedad o región determinada en un período de tiempo determinado. Estos análisis estadísticos son esenciales para comprender la dinámica del crimen en la sociedad, permitiendo a las autoridades y a los expertos en políticas criminales tomar decisiones informadas para prevenir y combatir el crimen.

4.6.1. Criminalidad Informática

El Dr. Santiago Acurio del Pino, en su obra "Delitos Informáticos", al hacer referenciaal concepto de Criminalidad Informática, cita a Baón Ramírez, quien define la criminalidad informática como: "la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad)" (Acurio Del Pino, 2016, pág. 10).

El presente concepto ofrece un enfoque integral que tiene en cuenta tanto la naturalezadelictiva del acto como la importancia del vínculo entre tecnología informática y delito. Este enfoque contribuye a la contextualización y mejor comprensión del fenómeno en el marco deprincipios jurídicos tradicionales adaptados a la era digital.

En este contexto, es muy importante analizar los factores clave relacionados con el concepto de criminalidad informática. En primer lugar, se destaca que la criminalidad informática se refiere a la realización de hechos que cumplen con los requisitos que definen elconcepto de delito. Esta afirmación sugiere que, a pesar de la naturaleza virtual de los delitos informáticos, sigue siendo un acto que reúne los elementos criminales tradicionales de conducta, culpabilidad, y la lesión o amenaza de lesión a un bien jurídico protegido. La definición también incluye la idea de utilizar elementos informáticos como herramientas paracometer delitos. Esto indica que el mero uso de tecnología informática para cometer un delito no lo convierte automáticamente en un delito informático. Más

bien, se centra en la relación instrumental entre los elementos informáticos y la actividad delictiva, enfatizando la importancia de cómo se utiliza la tecnología para llevar a cabo actividades ilícitas.

La definición también incluye la vulneración de los derechos del titular de un elemento informático, ya sea hardware o software, que convierte al elemento informático en objeto de un delito penal. Esto demuestra la dualidad de la criminalidad informática, visto tanto en el abuso de la tecnología como herramienta delictiva como en la violación de derechos asociados a la tecnología.

4.7 Importancia del Derecho Informático

La autora Victoria Rodríguez en su obra "Derecho Informático", establece que, "La informática jurídica o Ius-cibernética, es la información al servicio del Derecho, como instrumento idóneo para optimizar la labor de los operadores jurídicos. Son sus ramas la informática documental, de gestión y decisional" (Rodriguez, 2007, pág. 17).

La idea que plasma la autora en su libro "Derecho Informático" es la base para comprender la intersección de la tecnología de la información y el derecho. Para describir el papel de la información en los servicios jurídicos, la autora introduce los términos "informática jurídica" o "ius-cibernética". Este concepto representa una sinergia entre el mundo jurídico y las tecnologías de la información al utilizar la información como herramienta para incrementar la efectividad y eficiencia de los profesionales del derecho, conocidos como operadores jurídicos. Los autores mencionan tres áreas principales de la informática jurídica: informática documental, informática de gestión e informática de decisiones. Estas tres áreas son importantes para optimizar las actividades legales y mejorar la toma de decisiones legales, es por ello cual son representadas a continuación:

"Informática Jurídica Documental: Es la ciencia que estudia el uso de procedimientos cibernéticos para el tratamiento, almacenado y recuperación de información jurídica, así como el empleo y control de esos procedimientos por parte del Estado y de los particulares" (Rodriguez, 2007, pág. 7). El concepto incluye un conjunto de prácticas y herramientas con los principales objetivos de mejorar la gestión de la información jurídica, agilizar los procedimientos legales y garantizar el cumplimiento de los requisitos legales y éticos en la era digital. Se centra en la investigación y aplicación de la tecnología de la información para gestionar eficazmente la información jurídica, incluido el procesamiento, el almacenamiento y la recuperación. También aborda el

control y regulación del uso de estos procedimientos tecnológicos tanto por parte de autoridades públicas como de particulares en un contexto legal. En otras palabras, tiene como objetivo utilizar tecnologías digitales para mejorar la gestión de la información jurídica y garantizar que el uso de esta información cumpla con los estándares legales y éticos necesarios.

Informática Jurídica de gestión: Además de la simple recopilación y archivo de datos jurídicos, la informática sirve como herramienta de apoyo administrativo para facilitar la realización de trámites, por ejemplo, en las mesas de entradas de los juzgados, seguimientode expedientes y en la gestión de los estudios de abogados con aplicaciones que incluyen el procesamiento de textos y el control integral del caso llevado (Rodriguez, 2007, pág. 18).

En base a este concepto, se entiende que la Informática Jurídica de Gestión, se enfocaen brindar herramientas tecnológicas para ayudar con la gestión administrativa y culminaciónde procesos legales. Esto incluye la automatización de las operaciones de las oficinas judiciales, el seguimiento de casos, la gestión de bufetes de abogados y más. En un mundo cada vez más digital, la informática de gestión jurídica desempeña un papel clave en la modernización de los sistemas jurídicos, mejorando la productividad y la precisión en el manejo de asuntos legales al tiempo que garantiza el cumplimiento de los estándares legales yéticos.

Informática Jurídica decisional: Se vincula con la llamada "Inteligencia Artificial"a partir de cierta información ayudan a tomar decisiones y resuelven problemas mediante la simulación del razonamiento humano. Están compuestos de un banco de datos que permite elcálculo lógico sobre ellos, aplicando los esquemas del razonamiento. Mediante el motor de inferencia el sistema es capaz de tomar dos (2) informaciones de la base (premisas) y obteneruna conclusión lógica (Rodriguez, 2007, pág. 18).

Del mismo modo, el presente se entiende como el enfoque en utilizar tecnología para simular el razonamiento humano para respaldar la toma de decisiones y la resolución de problemas legales. Básicamente, estos sistemas utilizan una base de datos de información jurídica y utilizan un marco de razonamiento lógico para procesarla. En el corazón de estos sistemas hay algo llamado "motor de inferencia". Este motor es un componente clave que permite a la informática de decisiones jurídicas utilizar información de bases de datos, también conocidas como premisas, y sacar conclusiones lógicas de ella, ya que utiliza inteligencia artificial para respaldar la toma de decisiones y

la resolución de problemas legales.

4.8 Derecho Informático

"El Derecho informático, es el conjunto de normas y principios jurídicos que tienen por objeto reglar las relaciones jurídicas emergentes de la actividad informática" (Rodriguez, 2007). Este concepto de derecho informático se refiere a un conjunto de normas y principios jurídicos desarrollados específicamente para regular las relaciones jurídicas que surgen como resultado de las actividades informáticas. Esta área del derecho ha adquirido importancia en la era digital porque aborda una amplia gama de cuestiones jurídicas relacionadas con las tecnologías de la información y la comunicación. En eso radica su importancia ya que la legislación en base a las TIC, desempeña un papel clave para garantizar que dichas actividades cumplan con los requisitos legales y éticos y protejan los derechos y obligaciones de las partes. Esto incluye cuestiones relacionadas con la seguridad cibernética, la privacidad en línea, los derechos de propiedad intelectual digital y la responsabilidad por actividades cibernéticas, etc. Además, el derecho informático debe adaptarse constantemente a medida que avanza la tecnología y surgen nuevas cuestiones legales.

4.8.1. Vulneración del Bien Jurídico en delitos Informáticos

El autor Hugo Bayardo, en su obra "Los delitos Informáticos y su tipificación en la legislación penal ecuatoriana", señala que "Dogmáticamente se considera las formas típicas de afectación de un bien jurídico son la lesión o la puesta en peligro (Luzón, 2012). Por ello es que, para que exista un delito informático, es necesario que exista un bien jurídico lesionado o puesto en peligro por la conducta del sujeto activo. Es decir, las acciones dolosas que van encaminadas al fraude, al daño, la transferencia electrónica del activo patrimonial, la interceptación ilegal de datos, etc. lesionan o ponen en peligro electrónica del activo patrimonial, la interceptación ilegal de datos, etc. lesionan o ponen en peligro" (Hugo Bayardo Santacruz, 2019).

La afirmación citada por Hugo Bayardo en su obra, es válida y se aplica en el ámbito de los delitos informáticos, ya que es en realidad necesario que para que se genere un delito debe haberse vulnerado un bien jurídico. En el caso de los delitos informáticos en Ecuador, tales como fraude, daño, transferencia electrónica indebida de activos patrimoniales, interceptación ilegal de datos y otros actos similares, es esencial que exista un bien jurídico lesionado o puesto en peligro para que se configure el delito. Esto significa que las acciones dolosas que implican estos delitos deben causar un perjuicio

tangible o poner en riesgo la integridad de los activos o datos involucrados.

En el contexto digital, los bienes jurídicos pueden incluir la integridad y confidencialidad de la información, la privacidad de las personas, la seguridad de las transacciones electrónicas y otros aspectos relacionados con la tecnología de la información.

Cuando un sujeto activo lleva a cabo acciones fraudulentas, dañinas o ilícitas que afectan estos bienes jurídicos, se considera que ha lesionado o puesto en peligro dichos bienes, lo que constituye la base para la imputación de un delito informático.

La aplicación de esta comprensión dogmática es esencial para garantizar la justicia y la seguridad jurídica en los casos de delitos informáticos en Ecuador. En última instancia, el enfoque basado en el bien jurídico asegura que las personas sean responsables de sus acciones y que se protejan los derechos y la integridad de las partes afectadas por los delitos informáticos.

4.9 Bienes Jurídicos vulnerados en el delito informático de Phishing

En el contexto de la legislación penal ecuatoriana, el bien jurídico vulnerado en el delito de phishing está relacionado con la seguridad y la confianza en los sistemas informáticos, así como la protección de la privacidad y la integridad de la información personal y financiera de los ciudadanos. En este sentido es de importancia relevante el realizar un análisis exhaustivo de estos aspectos en el contexto de la legislación penal de Ecuador:

4.9.1 Derecho a la Privacidad:

El Código Orgánico integral penal, en su sección sexta "*Delitos contra el derecho a laintimidad personal y familiar*" tipifica lo referente a Violación a la intimidad.

"**Art 178.- Violación a la intimidad**. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014).

En el contexto de la ley ecuatoriana. Sujeto a esta cláusula, acceder, retener, revisar, almacenar, registrar, reproducir, distribuir o publicar datos personales, mensajes de datos, voz, audio y video, correspondencia postal, información en soporte informático, mensajes personales. sin consentimiento o autorización legal, este hecho se castiga con

pena privativa de libertad de uno a tres años.

El phishing invade el derecho a la privacidad de las personas, un derecho protegido por la Constitución de Ecuador. Los ciudadanos tienen derecho a proteger su información personal y a mantenerla fuera del alcance de terceros no autorizados. La obtención no autorizada de datos a través del phishing representa una violación directa de este derecho fundamental.

4.9.2 Seguridad Jurídica:

El Art. 82 de la Constitución de la Republica del Ecuador, revela "El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes" (Constitución de la Republica del Ecuador, 2008).

Este artículo, establece el derecho fundamental a la seguridad jurídica, lo cual se basa en dos principios fundamentales: el respeto a la Constitución y la existencia de normasjurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Primero, el respeto a la constitución significa que todas las leyes, reglamentos y acciones gubernamentales deben ser consistentes con los principios y derechos establecidos en la Constitución ecuatoriana. Esto asegura que las normas y políticas del país sean consistentes con los valores y derechos fundamentales consagrados en la constitución del país.

En segundo lugar, los requisitos en materia de primacía, claridad, apertura de las normas jurídicas y su aplicación por parte de las autoridades competentes son muy importantes para garantizar la seguridad jurídica. La preferencia sobre las reglas significa que las leyes y regulaciones deben establecerse antes de que ocurra el comportamiento que regulan. Esto da confianza a los ciudadanos y les permite conocer de antemano las consecuencias jurídicas de sus actos

La claridad en las regulaciones significa que deben estar redactadas de manera clara y clara para que los ciudadanos puedan comprender fácilmente sus derechos y obligaciones. La apertura de un estándar significa que el estándar está abierto y accesible al público en general, de modo que todos tengan acceso a información sobre las leyes y regulaciones de su país. Por consiguiente, la seguridad jurídica se logra cuando los ciudadanos confían en que las autoridades aplicarán la ley de manera consistente y justa, sin discriminación ni arbitrariedad.

En este sentido, el derecho a la seguridad jurídica en Ecuador se fundamenta en el

respeto a la Constitución, que establece las bases para la organización y funcionamiento del Estado y garantiza los derechos y libertades fundamentales de los ciudadanos. Además, se fundamenta en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

La claridad y publicidad de las normas jurídicas en Ecuador es garantizada por la obligación del Estado de publicar todas las normas jurídicas en el Registro Oficial y en la página web oficial del Estado. Asimismo, la Constitución establece que todas las normas jurídicas deben ser generales, es decir, aplicables a todas las personas en igualdad de condiciones.

Por otra parte, el acceso a la justicia es un elemento fundamental del derecho a la seguridad jurídica en Ecuador. La Constitución garantiza el derecho a la tutela judicial efectiva y a un debido proceso, lo que implica que todas las personas tienen derecho a un acceso efectivo a la justicia y a un proceso justo e imparcial, en el que se respeten sus derechos fundamentales.

En cuanto a la independencia y transparencia de la función judicial, la Constitución deEcuador establece que los jueces y juezas deben actuar con imparcialidad y objetividad, sin recibir órdenes o presiones de ningún tipo. Además, se establece la obligación de los jueces y juezas de dar a conocer públicamente sus decisiones y de justificarlas de manera clara y motivada.

De la ligera conceptualización que la Constitución infiere sobre la seguridad jurídica, se puede concluir que ésta es la tutela y confianza de que el Estado respetará todos los derechos de sus administrados, el derecho a la libertad, a la propiedad privada, a la libertad de expresión, al debido proceso, entre otros, precisamente por la existencia de una norma pública previa que impone, permite o prohíbe, y a la cual no únicamente debe adecuar su acción el poder público, sino que además debe inexorablemente aplicarla. (Vallejo, 2010)

Dicho de este modo, en Ecuador el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes. Esto implica garantizar la claridad y publicidad de las normas jurídicas, el acceso a la justicia, el debido proceso y la independencia y transparencia de la función judicial.

4.9.3. Tutela Judicial Efectiva

La tutela judicial efectiva, constituye un derecho fundamental, tipificado en la

Constitución de la República del Ecuador:

"Art. 75.- Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley" (Constitución de la Republica del Ecuador, 2008).

Por consiguiente, la tutela judicial efectiva es un derecho fundamental que se encuentra

reconocido en la Constitución de la República del Ecuador y en diversos instrumentos internacionales de derechos humanos ratificados por el país. Este derecho se refiere al acceso a la justicia de manera oportuna y efectiva, y la garantía de que las personas puedan ejercer sus derechos y obtener una protección adecuada por parte del Estado.

En Ecuador, la tutela judicial efectiva se encuentra garantizada por un conjunto de normas y procedimientos que permiten a las personas acceder a la justicia de manera ágil y eficiente. La Constitución establece que toda persona tiene derecho a la tutela judicial efectiva, la cual se garantiza mediante la protección de los derechos fundamentales, la prevención y la solución de conflictos, y la reparación integral de los daños.

Entre las principales medidas que garantizan la tutela judicial efectiva en Ecuador se encuentran las siguientes:

Acceso a la justicia: La Constitución garantiza el derecho a la justicia y establece que el acceso a ella debe ser gratuito, integral y efectivo. Además, se han implementado diversos mecanismos de acceso a la justicia para personas en situación de vulnerabilidad, como la Justicia Gratuita, la Defensoría del Pueblo y la fiscalía general del Estado.

Independencia judicial: El sistema judicial en Ecuador es independiente y se encuentra separado de los demás poderes del Estado. Esto garantiza que las decisiones judiciales se tomen de manera imparcial y sin influencias externas.

Debido proceso: Las personas tienen derecho a un debido proceso, lo que implica que deben ser notificadas adecuadamente de los procedimientos judiciales, contar con un abogado defensor, presentar pruebas y alegatos, y recibir una resolución judicial fundamentada.

Tutela de los derechos fundamentales: El sistema judicial en Ecuador se encuentra obligado a proteger los derechos fundamentales de las personas, lo que implica

que las decisiones judiciales deben ser compatibles con los derechos humanos y las garantías constitucionales.

Recursos judiciales: Las personas tienen derecho a presentar recursos judiciales ante las decisiones judiciales que consideren violatorias de sus derechos o perjudiciales para sus intereses.

Resolución de conflictos: El sistema judicial en Ecuador cuenta con diversos mecanismos de resolución de conflictos, como la mediación, el arbitraje y la conciliación, que permiten resolver conflictos de manera extrajudicial y en un plazo más corto que los procedimientos judiciales.

4.9.4. Principio de Legalidad

Este principio es de suma importancia en el desarrollo de la presente investigación, ya que va directamente relacionado con el debido proceso que debe desarrollarse al momento en el que se configura una conducta antijurídica, siempre y cuando esta conducta este tipificada en la norma legal.

Por tanto, podemos identificar que este principio es contemplado en la CRE, en el art.76, numeral 3 en el cual expresa que:

"Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada Procedimiento" (Constitución de la Republica del Ecuador, 2008).

El principio constitucional mencionado es una garantía fundamental para las personas, ya que impide que se les juzgue o sancione por conductas que no están previamente tipificadas como delitos o infracciones en la ley. Esto implica que cualquier conducta que pueda ser sancionada debe estar claramente establecida en la ley y cumplir con los requisitos establecidos para ser considerada una infracción penal, administrativa o de otra naturaleza.

Además, este principio constitucional establece la obligación de que cualquier juzgamiento o sanción sea realizada únicamente por un juez o tribunal competente, es decir, aquellos que tienen la autoridad y el conocimiento necesario para resolver el caso de manera justa e imparcial. Asimismo, se establece la obligación de seguir el debido proceso legal, lo que implica que se deben respetar las formalidades y garantías procesales para proteger los derechos de la persona involucrada en el proceso.

La Corte Constitucional de Transición que, en materia penal, juega un papel primordial el principio de estricta legalidad, que constituye una norma meta legal dirigida al legislador, a quien prescribe una técnica específica de calificación penal idónea para garantizar la taxatividad de los presupuestos de la pena, la decibilidad de la verdad de su enunciación, ya que el principio de mera legalidad es una norma dirigida a los jueces, a los que se ordena que consideren delito cualquier acto calificado por tal por la ley (Falconí, 2012).

Dicho de otro modo, el principio de estricta legalidad juega un papel central en los casos penales. Este principio establece que sólo los actos prescritos por la ley pueden considerarse delictivos. En otras palabras, los actos que constituyen un delito deben estar claramente definidos y distinguidos por la ley. El texto señala que el principio de estricta legalidad es una norma metajurídica dirigida a los legisladores. Esto significa que la legislatura debe promulgar leyes claras y específicas que definan qué comportamiento es un delito y prescriban las sanciones asociadas. El objetivo de este principio es garantizar la claridad jurídica, de modo que los ciudadanos sepan de antemano qué acciones están prohibidas y qué consecuencias jurídicas se derivarán de realizarlas.

Además, esta interpretación de Falconí, se refiere al principio de legalidad, es decir, a las reglas para los jueces. Este principio establece que los jueces tienen el deber de considerarcomo delito cualquier acto previsto por la ley. Es decir, los jueces no tienen la facultad de interpretar el derecho penal de manera amplia ni de cometer delitos por sí mismos. Su funciónes hacer cumplir estrictamente las leyes existentes y las definiciones de delitos establecidas por el poder legislativo.

Además, establece la obligación de que cualquier juzgamiento o sanción sea realizadaúnicamente por un juez o tribunal competente y con el debido proceso legal, lo que protegelos derechos de la persona involucrada en el proceso.

4.9.5. Interpretación de la norma

El Código Orgánico Integral Penal, expresa que, para la interpretación de las normas dentro del Código, se debe cumplir con algunas reglas que son:

La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos.

Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma.

Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos (Código Orgánico Integral Penal, 2014).

En el primer inciso, señala que la interpretación de las disposiciones del Código Penal se hará de conformidad con la Constitución de la República del Ecuador y los instrumentos internacionales de derechos humanos. Esto significa que la interpretación del derecho penal debe respetar los principios y derechos fundamentales consagrados en la Constitución del Ecuador y en los tratados internacionales de derechos humanos ratificados por el Ecuador.

El segundo inciso, muestra que los tipos de delitos y penas se interpretan de forma estricta, es decir, según el significado literal de los criterios. Esto significa que los delitos y penas previstos en el derecho penal no pueden interpretarse de manera amplia o integral. Las interpretaciones deben ser coherentes con lo claramente establecido en el texto de la ley y evitar interpretaciones amplias que puedan ampliar el alcance del delito o pena. Prohibición de semejanza de origen delictivo:

Finalmente, el tercer inciso prohíbe el uso de semejanzas para crear nuevos delitos, esto significa que los delitos no pueden identificarse en comparación con situaciones similares. Además, no pueden utilizarse analogías para ampliar los límites de las presunciones legales que permiten el uso de sanciones o medidas preventivas, ni para establecer la especificidad o limitaciones de derechos. En otras palabras, las leyes penales deben ser precisas y específicas, y no pueden crearse delitos o penas similares.

Estas disposiciones establecen los principios básicos para la interpretación normativa de la ley orgánica penal integral del Ecuador, así como también, aseguran la legitimidad y protección de los derechos de los delincuentes al garantizar que la ley penal se interprete de conformidad con la Constitución y los derechos humanos, se aplique estrictamente y no se extienda libremente por analogía

La interpretación de la norma es una tarea que corresponde principalmente a los jueces y tribunales, quienes tienen la responsabilidad de aplicar las normas en los casos concretos que se presentan ante ellos. Para llevar a cabo esta tarea, los jueces y tribunales deben tener en cuenta diversos factores, como el texto de la norma, su contexto histórico ysocial, y la jurisprudencia y doctrina que se han generado en torno a ella.

4.10 Convenio de Budapest

El Convenio de Budapest sobre Ciberdelincuencia es un tratado internacional creado en el año 2001 e impulsado por el Consejo de Europa, con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet. (Digitales, 2022).

El Convenio de Budapest es un tratado internacional que tiene como objetivo armonizar las leyes nacionales de los países miembros en materia de delitos informáticos y ciberdelincuencia. Fue desarrollado por el Consejo de Europa y entró en vigor en el año 2004. Este convenio se ha convertido en un instrumento fundamental para combatir la ciberdelincuencia en todo el mundo, ya que proporciona un marco legal claro y sólido para los países miembros.

El convenio supone en cierto modo la plasmación positivizada de muchas de las ideas aquí vertidas, la mayor maximización de la cooperación en materia de delitos informáticos existente hoy en día en el plano internacional. En efecto, se trata del primer y único instrumento internacional existente hasta la fecha en esta materia, y su auténtica importancia se hará manifiesta a lo largo de este capítulo. Referente a los Estados que forman parte del mismo, a día de hoy tan sólo treinta Estados han ratificado el Tratado, de un total de cuarentay seis firmas (Díaz, 2010).

Este enunciado señala que el Convenio de Budapest, es único y el primer y único documento internacional en el ámbito del cibercrimen hasta la fecha. Esta declaración resalta la originalidad y la importante relevancia del Convenio. Además, que, dicho convenio incluye una serie de disposiciones que buscan proteger la seguridad de los sistemas informáticos, la privacidad de los datos y la propiedad intelectual en línea. Establece medidas preventivas y punitivas para delitos informáticos, como el acceso no autorizado a un sistema informático, la interceptación de datos y la interferencia en la integridad de datos informáticos. Cabe recalcar que actualmente cuenta con más de 60 países como firmantes. Al unirse al Convenio de Budapest, los países se comprometen a cooperar en la investigación y el enjuiciamiento de los delitos relacionados con la tecnología de la información, que son importantes en un mundo cada vez más interconectado.

Está abierto a la adhesión de cualquier Estado que quiera formar parte de él y se ha convertido en un marco de referencia mundial para combatir la ciberdelincuencia. Es menester indicar que el Convenio de Budapest, es un tratado internacional muy

importante que incluye disposiciones específicas para abordar los delitos informáticos y la ciberdelincuencia en todo el mundo. Proporciona un marco legal sólido para la prevención, investigación y enjuiciamiento de la ciberdelincuencia, y establece un marco para la cooperación internacional en este ámbito. Este tratado sigue siendo relevante y necesario en la actualidad, ya que la ciberdelincuencia sigue siendo una amenaza para la seguridad y la privacidad en línea en todo el mundo.

Para Ecuador la adhesión a este convenio le brindaría acceso a herramientas y recursos compartidos por los signatarios, fortaleciendo su capacidad para responder a las amenazas cibernéticas y proteger la seguridad de sus ciudadanos y su infraestructura crítica. La participación en este acuerdo contribuirá a la armonización de la legislación ecuatoriana con los estándares internacionales, creando un entorno seguro y confiable para lasociedad y la economía digital del país.

4.11 Delitos Informáticos en Ecuador

En el Ecuador, la tipificación de conductas relacionadas con el uso de medios informáticos es relativamente nueva, si se tiene en cuenta que las legislaciones que se dieron en otros países tras el primer virus informático reportado por IBM en el año de 1984. El antecedente más próximo se remonta al año 2002 con la expedición de la *Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos*. Dicha ley, apelando a la importancia delos sistemas de información y de redes electrónica, se encaminó a regular un ámbito que todavía se encontraba ignorado (Hugo Bayardo Santacruz, 2019, pág. 4).

Dicho de otro modo, el Ecuador no contaba con una legislación específica en esta materia. Un paso importante en el desarrollo legislativo de la ciberseguridad nacional fue la promulgación de la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos". Esta ley fue un paso importante hacia la regulación de una industria que hasta entonces había sido descuidada. La Ley tiene como objetivo regular el comercio electrónico, así como establecer un marco legal para las firmas electrónicas y la comunicación de datos. En un mundo cada vez más digital, se ha vuelto esencial establecer regulaciones que garanticen la seguridad y confiabilidad de las transacciones electrónicas y protejan los datos yla información de los ciudadanos y las empresas.

La promulgación de esta ley representa un importante paso adelante en el reconocimiento por parte del Ecuador de la necesidad de protegerse contra el cibercrimen y la ciberseguridad. Sin embargo, es importante señalar que, a pesar de este importante paso, la ley en esta área debería seguir evolucionando para abordar nuevas amenazas y

desafíos tecnológicos en constante cambio. La ciberseguridad es una preocupación creciente para las autoridades y los ciudadanos, y es importante que las leyes sigan evolucionando para proteger los intereses públicos y privados en el ámbito digital.

A partir de la vigencia del Código Orgánico Integral Penal (COIP), esto es, desde el 10 de agosto de 2014, el número de conductas relacionadas con los delitos informáticos se incrementan. Destaca el hecho de que dentro de la sistemática del COIP no se contemplan delitos que lleven expresamente la denominación de delitos informáticos. Sin embargo, existen conductas punibles que dogmáticamente pueden ser considerados como delitos informáticos (Hugo Bayardo Santacruz, 2019, pág. 5).

Esto señala un punto importante en el desarrollo del marco legal ecuatoriano en relación con los delitos informáticos. Es interesante notar que, a diferencia de algunos otros países que han adoptado leyes específicas para delitos informáticos, en el caso del Ecuador, estas conductas están integradas en la legislación penal general sin una designación específicacomo "delitos informáticos".

Este enfoque muestra una adaptabilidad de la ley ecuatoriana para abordar los desafíos tecnológicos y las amenazas cibernéticas en un contexto legal más amplio. La ausencia de una denominación específica no impide que las acciones cometidas en el ámbito digital sean consideradas como delitos informáticos, aunque a mi criterio, debería haber un título o capitulo que los integre de manera específica.

En cuanto a la caracterización de conductas punibles como delitos informáticos desdeuna perspectiva dogmática, esto implica una evaluación profunda de las acciones y su relación con la tecnología. Los delitos informáticos pueden incluir actividades como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de datos, la difusión demalware, el fraude en línea y el phishing, entre otros. Estas acciones son interpretadas por los jueces y punibles en base a otros delitos ya tipificados y que vulneran aquellos derechos, como el derecho a la privacidad, la integridad de los datos y la confidencialidad.

Es relevante destacar que, en el contexto de un mundo cada vez más digitalizado, la adaptación y expansión de las leyes para abordar los delitos informáticos son esenciales para preservar la seguridad y la confianza en el entorno en línea.

De los delitos informáticos que se encuentran tipificados en la normativa penal, son representados en el siguiente cuadro descriptivo, a modo didáctico, a fin de un mejor entendimiento:

Delitos Informáticos Tipificados en el COIP		
Articulo	Delito	Pena
Art.103	Pornografía con utilización de niñas, niños y adolescentes.	13 a 16 años Agravante: 16 a 22 años
Art.173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	1 a 3 años Agravante: 3 a 5 años
Art.174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.	7 a 10 años
Art. 178	Violación a la intimidad.	1 a 3 años
Art. 190	Apropiación fraudulenta por medios electrónicos.	1 a 3 años
Art. 191	Reprogramación o modificación de información de equipos terminales móviles.	1 a 3 años
Art. 192	Intercambio, comercialización o compra de información de equipos terminales móviles.	1 a 3 años
Art. 193	Reemplazo de identificación de terminales móviles.	1 a 3 años
Art. 194	Comercialización ilícita de terminales móviles.	1 a 3 años
Art. 195	Infraestructura ilícita	1 a 3 años
Art. 229	Revelación ilegal de base de datos	1 a 3 años Agravantes: 3 a 5 años

Imagen: (1) Delitos Informáticos Tipificación en el COIPElaborado por el Autor

Art. 229	Revelación ilegal de base de datos	1 a 3 años Agravantes: 3 a 5 años
Art. 230	Interceptación ilegal de datos	3 a 5 años
Art. 231	Transferencia electrónica de activo patrimonial	3 a 5 años
Art. 232	Ataque a la integridad de sistemas informáticos	3 a 5 años Agravante: 5 a 7 años
Art. 233	Delitos contra la información pública reservada legalmente.	5 a 7 años Atenuante: 3 a 5 años Agravante: 7 a 10 años
Art. 234	Acceso no consentido a un sistema informático o de telecomunicaciones.	3 a 5 años
Art. 298 (numerales 8, 9 y 10)	Defraudación tributaria	Numeral 1 al 11: 1 a 3 años Numeral 12 al 14: 3 a 5 años Numeral 15 al 17: 5 a 7 años Numeral 18, 19 y 20: 5 a 7 años

Imagen: (2) Delitos Informáticos Tipificación en el COIPElaborado por el Autor

La figura presentada representa un avance significativo en la comprensión y definición de los diferentes tipos de delitos informáticos y las respectivas sanciones descritas en el Código Orgánico Integral Penal (COIP) del Ecuador. Esta herramienta visual le brinda al lector, una imagen clara y concisa de las diferentes categorías de

delitos cibernéticos. La figura no sólo clasifica los delitos cibernéticos, sino que también proporciona información detallada sobre las sanciones para cada tipo de delito.

4.12 Criminalidad Informática en Ecuador

Desde la Fiscalía General del Estado se han creado unidades especializadas para combatir este tipo de criminalidad. La Unidad de Patrimonio Ciudadano se encarga de atender este tipo de defraudaciones. Sin embargo, la falta de fiscales hace que se acumulen las causas y que las investigaciones no prosperen. En la mayoría de los casos, las investigaciones se estancan en la fase de indagación previa por la falta de evidencias, lo que origina el archivo de las causas y consecuentemente el aumento de la impunidad (Hugo Bayardo Santacruz, 2019, pág. 6).

El texto destaca un aspecto crucial en la lucha contra la ciberdelincuencia en Ecuador: la existencia de unidades especializadas dentro de la fiscalía general del Estado dedicadas a combatir este tipo de criminalidad. En este caso, la Unidad de Patrimonio Ciudadano tiene la responsabilidad de abordar defraudaciones y delitos informáticos en el país. Sin embargo, a pesar de estos esfuerzos, el sistema se enfrenta a desafíos significativos que obstaculizan la efectividad de las investigaciones y la persecución de los delincuentes cibernéticos.

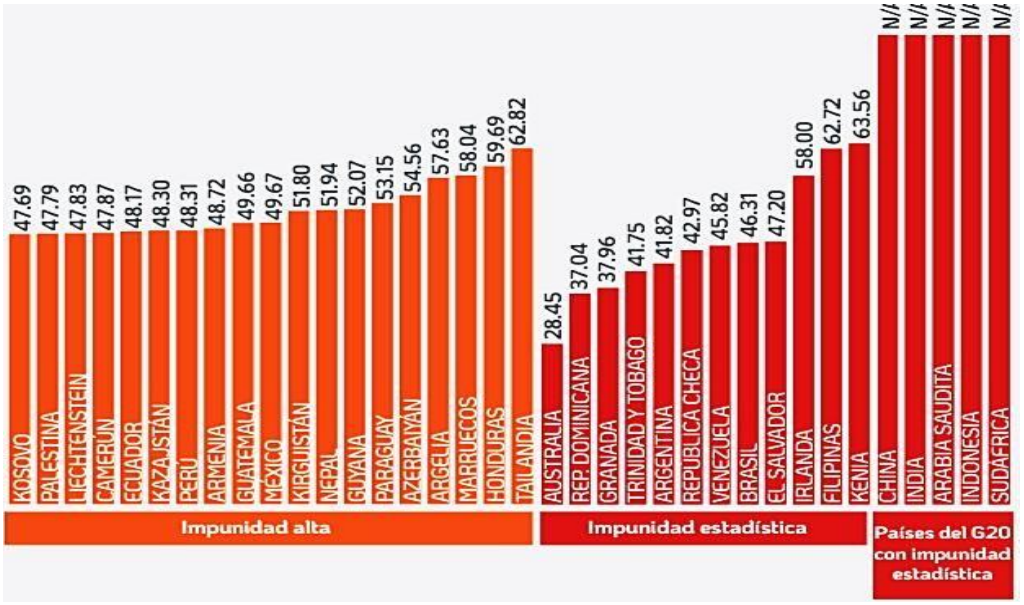
Uno de los problemas cruciales identificados en el texto es la falta de personal fiscal, esta carencia impide el progreso adecuado de las investigaciones y conduce a la acumulación de casos sin resolver. La falta de fiscales especializados en delitos informáticos no solo ralentiza el proceso de investigación, sino que también crea un cuello de botella en el sistema judicial, lo que puede llevar a la demora en el enjuiciamiento y, en última instancia, a la impunidad para los delincuentes.

Además, el texto también, señala que las investigaciones a menudo se estancan en la fase de indagación previa debido a la falta de evidencias sólidas. Esta situación es preocupante porque significa que los casos no pueden avanzar hacia etapas posteriores del debido proceso penal. La falta de evidencia puede deberse a diversos factores, como la naturaleza compleja y cambiante de los delitos informáticos, la sofisticación de los ciberdelincuentes y la falta de recursos técnicos y especializados para recopilar pruebas digitales de manera efectiva.

La consecuencia directa de estos desafíos es el aumento de la impunidad en los delitos informáticos. La falta de enjuiciamientos exitosos y la falta de castigo para los culpables pueden socavar la confianza de la población en el sistema judicial y

desincentivar la denunciade futuros delitos cibernéticos. Esto crea un círculo vicioso en el que la impunidad alimenta laperpetración continua de delitos informáticos.

En un informe presentado por la IGI, Índice Global de Impunidad, expone la alarmante realidad de Ecuador: uno de los países con mayor nivel de impunidad en el mundo.



Fuente: Escalas de Impunidad en el mundo (Juan Le Clercq, 2020, pág. 59)

Esta situación plantea serios desafíos al sistema legal de Ecuador y resalta la necesidad de abordar urgentemente las deficiencias en la administración de justicia y la aplicación efectiva de la ley. El alto nivel de impunidad en Ecuador, representado por el 48.17%, refleja problemas con la capacidad del sistema judicial para resolver casos y castigar a los delincuentes, así como debilidades en la prevención del delito, la investigación criminal,la recopilación de pruebas y la protección de las víctimas.

Estos factores crean un entorno en el que los delincuentes creen que pueden escapar del castigo y participar en actividades ilegales, lo que puede socavar la confianza pública en el sistema de justicia y fomentar la continuación de la delincuencia. Además, la impunidad no sólo tiene un impacto negativo en el nivel de seguridad de los ciudadanos, sino que también desalienta la denuncia de delitos. Esto se debe a que las personas pueden perder la confianza en que las autoridades manejarán adecuadamente sus casos. Esta falta de confianza en el sistema legal puede destruir la armonía social y crear una atmósfera de desconfianza y descontento en la sociedad.

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 ante las formalidades y la virtualidad de los procesos puede tardarse meses (Trejo, 2019).

Este inconveniente plantea serios problemas a la hora de identificar la cuenta o dirección IP desde la que se produjo un ciberataque o suplantación de identidad. La razón de esta complejidad es la formalidad y virtualidad del proceso de investigación, que puede tardarmeses en producir resultados reales. La falta de acuerdos internacionales en los campos de la ciberseguridad y el cibercrimen obstaculiza la cooperación internacional. Estos acuerdos son esenciales para el intercambio rápido y eficiente de información entre países en caso de ciberataques y otras actividades delictivas en línea.

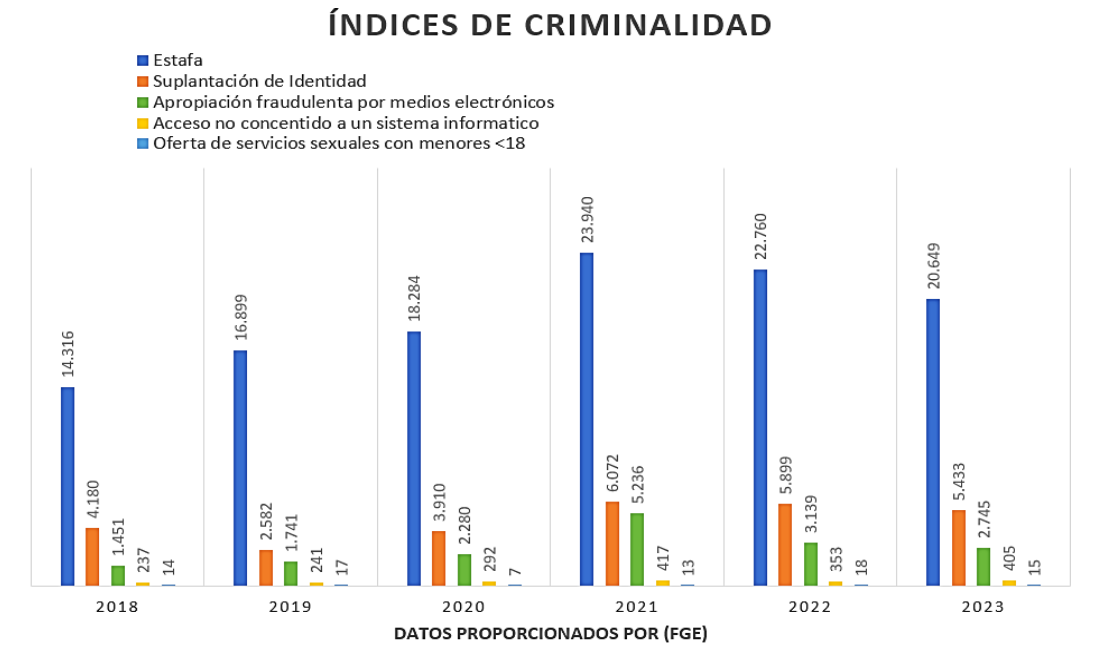
La falta de tratados internacionales también resalta la necesidad de actualizar las leyes y regulaciones locales para abordar el problema actual del delito cibernético. Es necesario reformar las leyes para garantizar una cooperación internacional eficaz y hacer frente a la complejidad del delito cibernético en un mundo cada vez más digital y conectado, ya que la ausencia de estas medidas podría provocar retrasos en las investigaciones y dificultades para llevar a los ciberdelincuentes ante la justicia, lo que subraya la urgente necesidad de abordar estas cuestiones para fortalecer la ciberseguridad y la aplicación de la ley en el país.

4.12.1. Datos proporcionados por fiscalía general del estado

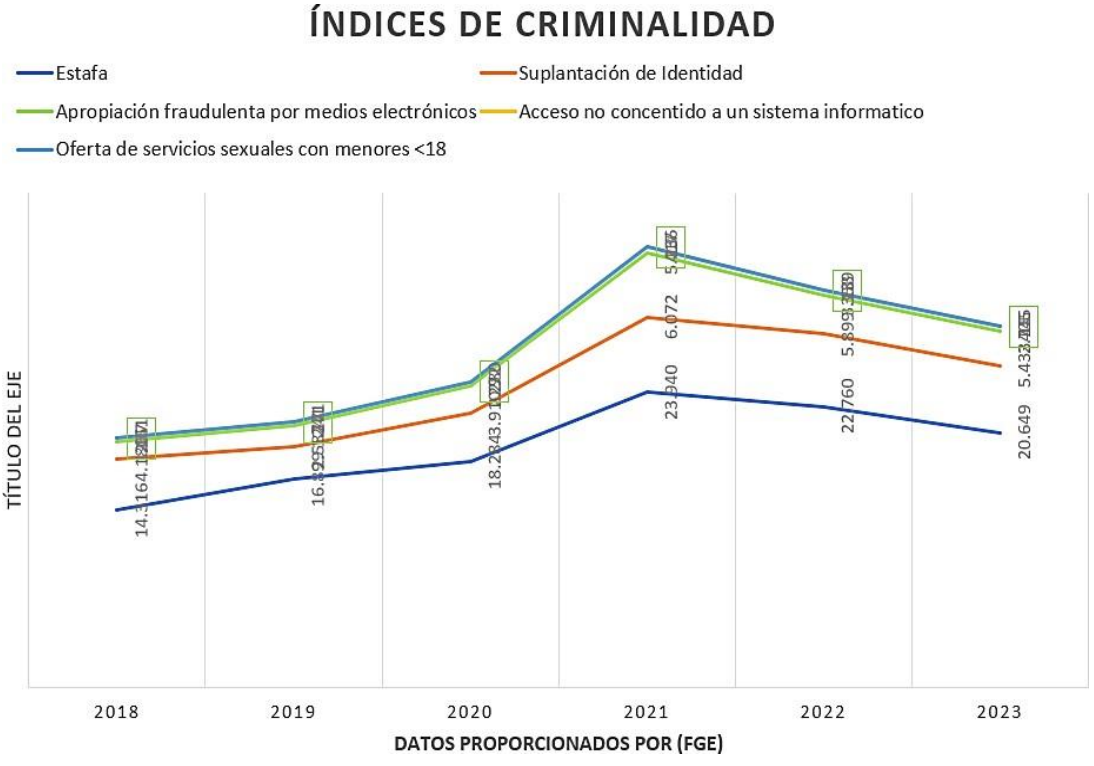
En el desarrollo de la presente investigación, se planteó demostrar los índices de criminalidad en los delitos informáticos en el estado ecuatoriano, para ello en la búsqueda de fuentes fidedignas que permitan el planteamiento de estadísticas o índices reales acerca de la criminalidad en delitos informáticos en ecuador, se tomó como referencia a la Fiscalía General del Estado.

Al amparo del Art.18 de la constitución de la República del Ecuador, que en su numeral 2, establece, “Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley”. Es por ello que, mediante el uso de las Tecnologías de la Información y Comunicación, para ser más específico del correo electrónico, se solicitó datos acerca de las denuncias presentadas por la ciudadanía en todo el territorio ecuatoriano, referente a los delitos de los artículos: 174, 186, 190, 212 y 234, tipificados en el Código Orgánico

Integral Penal (COIP), correspondiente a los años 2018 hasta la actualidad, por lo que, en base a estos datos, realizo la siguienterepresentación gráfica



Fuente: Fiscalía general del Estado
Elaborado por el autor



Fuente; Fiscalía General del EstadoElaborado por el autor

Para lograr el entendimiento de en la presente ilustración, se indica a continuación el método utilizado en cada uno de los delitos abordados. Para el delito de Estafa es representado en la gráfica con el color azul, seguido del delito de Suplantación de Identidad representado con el color naranja, el delito de Apropiación fraudulenta por medios electrónicos representado con el color verde, el delito de Acceso no consentido a un sistema informático representado con el color amarillo y finalmente el delito de oferta de servicios sexuales con menores de dieciocho años representado con el color celeste.

4.12.2 Estafa

En base a los datos proporcionados por fiscalía el delito de estafa es denunciado en base a diferentes numerales del mismo artículo, pero que al final configuran el mismo tipo penal, por lo que, a objeto de estudio, he representado este delito de forma gráfica y detallando el número de denuncias presentadas en los años del 2018 a 2023. En el año 2018 las denuncias presentadas a fiscalía son de 14.316, en el año 2019 son de 16.899, en el año 2020 son de 18.284, en el año 2021 son de 23.940, en el año 2022 son de 22.760 y para el año 2023 hasta la actualidad han sido presentadas 20.649 denuncias.

4.12.3 Suplantación de Identidad

Este delito es representado en la gráfica con el color naranja, en base a ello, represento el número de denuncias presentadas en los años correspondientes, para el año 2018 se han presentado 4.180 denuncias, en el año 2019 son de 2.582 denuncias, en el año 2020 son de 3.910, en el año 2021 son de 6.072, en el año 2022 son de 5.899 y para el año 2023 son de 5.433 hasta la actualidad, gracias a ello, se determina que el año 2021 es en el que se han presentado el mayor número de denuncias presentadas por la ciudadanía.

4.12.4 Apropiación fraudulenta por medios electrónicos

Este delito es representado en la gráfica con el color verde, represento el número de denuncias presentadas en los años correspondientes de la siguiente forma; para el año 2018 sehan presentado 1.451 denuncias, en el año 2019 son de 1.741 denuncias, en el año 2020 son de 2.280, en el año 2021 son de 5.236, en el año 2022 son de 3.139 y para el año 2023 son de 2.745 hasta la actualidad, gracias a ello, se determina que desde el año 2021 alcanza el pico más alto con 5.236 denuncias presentadas en base a este tipo de delito.

4.12.5 Acceso no consentido a un sistema informáticos

Este delito es representado en la gráfica con el color amarillo, represento el número dedenuncias presentadas en los años correspondientes de la siguiente forma; para el año 2018 sehan presentado 237 denuncias, en el año 2019 son de 241 denuncias, en el año 2020 son de 292, en el año 2021 son de 417, en el año 2022 son de 353 y para el año 2023 son de 405 hasta la actualidad, gracias a ello, se determina que desde el año 2021 alcanza el pico más alto en denuncias presentadas en base a este tipo de delito.

4.12.6 Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos

Este delito es representado en la gráfica con el color celeste, el número de denuncias presentadas en los años correspondientes son: para el año 2018 se han presentado 14 denuncias, en el año 2019 son de 17 denuncias, en el año 2020 son de 7, en el año 2021 son de 13, en el año 2022 son de 18 y para el año 2023 son de 15 hasta la actualidad, gracias a ello, se determina que desde el año 2022 alcanza el pico más alto con 18 denuncias presentadas en base a este tipo de delito.

Esto demuestra como los índices de criminalidad en base a los diferentes tipos de delitos informáticos tipificados en la norma penal ecuatoriana, han ido en aumento desde el año 2018 hasta el 2021 siendo este año el que mayor número de denuncias se han presentado, para el año 2022 y 2023 consecuentemente, estas denuncias han ido disminuyendo, esta representación no significa necesariamente, que estos delitos ya no se estén cometiendo, la baja en las denuncias, podría ser por distintas razones, una de ellas podría ser, porque las victimas deciden no denunciar, ya que estas denuncias en muchos de los casos, son archivadas en fase de investigación al no contar con los elementos suficientes, es decir evidencias, para que continue el proceso.

4.13 Derecho Comparado

Para el desarrollo de este inciso, se procedió a analizar la legislación de 4 países, como son: Chile, México, Argentina, Colombia, para realizar un análisis mejor estructurado, se

Derecho Comparado					
Parámetro	**Chile**	**México**	**Argentina**	**Colombia**	**Ecuador**
Norma Legal que regula los delitos informáticos	Ley 19.223 sobre Delitos Informáticos	Ley Federal de Delitos Informáticos	Ley 26.388 - Código Penal de Argentina	Ley 1273 de 2009. Código Penal Colombiano	Código Orgánico Integral Penal
Tipificación en la ley	Art.- 4: (Uso fraudulento de informática y su acceso ilegítimo)	Art.- 386 Bis (Suplantación de identidad electrónica)	(Actividades fraudulentas en línea) Art.-153	Art. 269 lit G: Suplantación de sitios web para capturar datos personales	----------
Adherido al convenio de Budapest	SI (es parte del Convenio de Budapest desde 2003)	SI (es parte del Convenio de Budapest desde 2018)	SI (es parte del Convenio de Budapest desde 2019)	NO es parte del Convenio de Budapest.	NO es parte del Convenio de Budapest.

realiza la representación en el siguiente cuadro comparativo.

Para cubrir rigurosamente el contenido de esta sección, en el contexto de este estudio,llevó a cabo un análisis de las leyes de cuatro países, como son: Chile, México, Argentina y Colombia, desde un análisis sistemático y completo que revela los matices y diferencias claveen las regulaciones legales de estos países. A continuación, se muestra un cuadro comparativo que resume información importante. Esto a fin de que permite identificar fácilmente similitudes y diferencias para lograr obtener una comprensión más profunda del tema en consideración.

El presente cuadro comparativo representa un análisis y estudio de manera concreta acerca de la norma legal de cada legislación en la que se determinar si el delito informático dephishing se encuentra tipificado como tal, de forma literal, en cada una de estas legislaciones o en su defecto identificar en que articulo ya tipificado se amparan para adaptar la conducta delictiva del phishing al tipo penal previsto en dicha ley.

Chile:

Para el caso de Chile la normativa legal que tipifica los delitos informáticos es la Ley 19.223 sobre Delitos Informáticos, en esta se toma como referente al Art. 4 denominado como: "*Uso fraudulento de informática y su acceso ilegítimo*", esto para penalizar el delito informático de Phishing, adecuando con ello la conducta a este tipo penal, el cual establece que: "Art. 4.- Uso fraudulento de informática y su acceso ilegitimo. - La obtención, transferencia o transferencia fraudulenta de datos o de información, o la realización de un acto que afecte o interrumpa un sistema informático, será sancionada con la pena de presidio menor en su grado mínimo a medio y multa de once a veinte unidades tributarias mensuales" (Chile, 2015).

Cabe indica que Chile es uno de los países que SI esta adheridos al Convenio de Budapest desde el año 2003, por lo que se apega a lo descrito en dicho convenio con respeto alas normas y disposiciones ahí establecidas.

México

La ley que tipifica los delitos informáticos en el caso de México, es la "Ley Federal deDelitos Informáticos", en la cual se usa el tipo penal denominado Suplantación de Identidad Electrónica, en la que, basa y adecua el comportamiento de dicho delito, a las conductas del phishing a fin de judicializar dicho delito informático.

Dicho artículo estipula lo siguiente: “Art. 386 Bis. - Suplantación de identidad electrónica. - Comete el delito de suplantación de identidad electrónica quien, sin autorización, se apodere, utilice, altere, copie o duplique una o varias claves de acceso, contraseñas, firma electrónica o cualquier otro dato o mecanismo de identificación electrónica de otra persona. A quien cometa este delito se le impondrá prisión de uno a seis años y multa de trescientos a seiscientos días de salario mínimo” (México, 2012).

En esta legislación, se adecua el delito de phishing a esta conducta como lo es, “Suplantación de identidad electrónica”, en el señala que, comete este delito quien capture, utilice, altere, copie o reproduzca sin permiso una o más claves de acceso, contraseñas, firmas electrónicas u otros datos o mecanismos de identificación electrónica de otra persona. Las actividades prohibidas incluyen el acceso no autorizado a información electrónica protegida, la alteración de información de identificación y el uso indebido de la firma electrónica de otra persona. Estas actividades amenazan la seguridad y privacidad de la información electrónica y requieren sanciones legales.

En términos de consecuencias legales, los infractores según esta norma pueden enfrentarse a entre uno y seis años de prisión. Además, se aplica una multa de 300 a 600 días de salario mínimo. Estas sanciones reflejan la gravedad del delito y están diseñadas para disuadir eficazmente el robo de identidad electrónica. Sin embargo, la naturaleza amplia de la descripción sugiere que incluye todas las formas de manejo no autorizado de datos electrónicos. Cabe señalar también, que México SI es parte del Convenio de Budapest desde el año 2018

Argentina

Por su parte Argentina dispone de la “Ley 26.388” del Código Penal Argentino, en esta el tipo penal tipificado al que se apegan en caso de Phishing es al de “Actividades Fraudulentas en Línea”

Este se determina en el Artículo 153, el cual establece que, “La pena será de prisión de un mes a dos años, cuando el responsable accediere indebidamente a un sistema o dato informático de un tercero, cuando el hecho no constituyere un delito más severamente penado."

Según este artículo, acceder ilegalmente al sistema informático o a los datos de un tercero daría lugar a una pena de prisión de uno a dos años. Esta disposición legal busca proteger la integridad y confidencialidad de la información digital, ya que el acceso no autorizado a sistemas o datos es un delito sujeto a sanciones proporcionadas, incluso si

no alcanza la gravedad de otros delitos. Es importante señalar que estas disposiciones legales tienen como objetivo lograr un equilibrio entre la protección de la propiedad digital y la proporcionalidad de las sanciones, evitando al mismo tiempo castigos excesivos por conductas que, incluso si son inapropiadas, no tienen el nivel de gravedad requerido para delitos graves. Sin embargo, dada la naturaleza dinámica y en evolución de la industria tecnológica y la aplicación continua de la ley para abordar nuevos desafíos de ciberseguridad, es importante considerar la interpretación y aplicación adecuadas de esta disposición en un contexto legal. Además, se recalca que Argentina es uno de los países SI adheridos al convenio de Budapest, siguiendo el ejemplo de México y esto desde el año 2019.

Colombia

En el caso de Colombia el artículo 269G es el que más se apega a la conducta delictiva objeto de estudio de la presente investigación, en este se habla de "Suplantación de sitios Web para capturar datos personales", en el que señala:

"El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave, la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito" (Código Penal Colombia (LEY 1273), 2009, pág. 2)

El articulo señalado anteriormente en cuestión define de forma clara y precisa los actos ilícitos relacionados con la manipulación y elaboración de contenidos digitales. Estas regulaciones cubren una amplia gama de actividades, desde diseñar y desarrollar páginas electrónicas, enlaces o ventanas emergentes hasta distribuir, vender, realizar, programar o transmitir estas actividades con fines ilegales sin la debida autorización. Se castiga con pena de prisión de 48 a 96 meses y multa importante en función del salario mínimo establecido por la legislación colombiana. Cabe señalar que, si una víctima está involucrada en una cadena dedelitos, la pena aumenta entre un tercio y una vez y media.

Además, se destaca que cambiar los sistemas de verificación de nombres de dominio para que los usuarios piensen que tienen acceso a información confiable, como su banco, aumenta la gravedad del comportamiento, este acto es el que más se relaciona y enfoca en el delito informático de phishing. Por su parte Colombia no forma parte, ni es uno de los países adheridos al convenio de Budapest

5. Metodología

En el desarrollo de la presente investigación se empleó distintos tipos de métodos, procedimientos y técnicas, los cuales permitieron que la investigación realizada recabe información necesaria, relevante y de importancia considerable para el desarrollo de la misma, al mismo tiempo, llegar a la comprensión, análisis profundo y sistematizado de la problemática social planteada, a fin de proponer posibles soluciones a la misma.

5.1. Materiales utilizados.

Los materiales empleados durante el desarrollo del presente trabajo, son los que se describen a continuación:

Materiales de Oficina

En cumplimiento de los objetivos planteados al inicio de la investigación, los materiales que se emplearon para el desarrollo del mismo son:

Suministros de oficina: Papel bon A4, resaltadores, borrador, lápiz, esferos gráficos, grapas, clips, notas, separadores adhesivos.

Equipos Electrónicos: Laptop (ordenador personal), computadora de mesa, celular, grabadora de voz, impresora.

Redes y programas Informáticos: Internet, una de las herramientas más importantes y relevantes a lo largo de la investigación, programas de ordenador, como son el Word con el cual desarrolle el documento digital, en donde se plasma mi trabajo de integración curricular, el programa de Excel empleado mayormente para la creación de los gráficos estadísticos representativos e ilustrativos en base a la encuesta y entrevista realizada como parte del trabajo decampo, entre otros programas afines.

Materiales bibliográficos

Para lograr recabar toda la información necesaria, empleada y plasmada en el presente trabajo, se dio la tarea de identificar documentos relacionados directamente con el tema determinado, de manera que se usó:

Libros Jurídicos, Leyes, Manuales, Obras Científicas, Diccionarios Jurídicos, Revistas, entre otros materiales físicos, de los cuales se logró rescatar la información más

relevante, la cual fue citada de manera sistematizada e incluida en el presente trabajo.

Del mismo modo, se empleó el uso de las TIC (Tecnologías de la Información y Comunicación) o más específicamente la Internet, de manera correlacionada las diferentes páginas web y documentos pdf con material tanto nacionales como extranjeros, los cuales aportaron conocimiento con contenido de alto valor, con lo cual pude lograr recopilar información y clasificarla, con el fin de emplear únicamente la información más relevante entre todo el material adquirido.

5.2. Métodos:

Para el desarrollo del presente trabajo de investigación socio-jurídico, se emplearon los siguientes métodos.

Método Inductivo: Para lograr un verdadero entendimiento, fue necesario el empleo de este método, para obtener una comprensión profunda y verdadera del tema de investigación. Este método permitió recopilar sistemáticamente datos relacionados con el ciberdelito específico que se investiga. Al analizar estos datos en detalle, se identificó patrones y tendencias específicos que revelen las motivaciones y métodos utilizados por los ciberdelincuentes en este contexto. El estudio de estos extensos datos fue fundamental para obtener una comprensión clara y precisa del fenómeno en estudio.

Método Deductivo: Lo que caracteriza a este método es que parte de premisas generales para llegar a particulares, esto a su vez sirviendo de complemento al método analítico antes descrito. Por tanto, este método fue empleado en el marco teórico, ya que facilito la comprensión, al momento de analizar la cibercriminalidad, la cual implica un problema tanto para el Estado como para la ciudadanía en general y apuntar a la implementación de medidas o leyes que permitan combatirla de mejor manera.

Método Analítico: Con este método se analizó de forma detallada el fenómeno causante de la problemática social planteada en la presente investigación, para lo cual, se descompuso el todo en sus partes, así como también en los elementos constitutivos. Del mismo modo el presente método fue empleado para el análisis y la interpretación de los resultados de las técnicas aplicadas como lo son la encuesta y la entrevista.

Método Exegético: Este método consiste en la interpretación gramatical o literal de las disposiciones normativas, lo cual, al emplear este método, permitió una interpretación profunda precisa de los términos y disposiciones relevantes de las leyes relacionadas a los ciberdelitos, de manera específica al momento de contextualizar el ciberdelito de phishing y larelación de este con la legislación nacional e internacional, la

cual va correlacionada de manera directa con la cibercriminalidad.

Método Hermenéutico: Este método va enfocado a la interpretación de textos legales y se centra en el significado y la comprensión del texto en su contexto más amplio. Del mismo modo, que empleado gracias a que permite una interpretación profunda y precisa del significado y la intención detrás de las leyes y las disposiciones relevantes, al igual que otros métodos, este fue empleado en el marco teórico

Método Mayéutica: Con este método, pude lograr esclarecer algunos de los cuestionamientos planteados durante la investigación, alcanzando un conocimiento más profundo, de modo que se pudo descubrir y comprender algunos factores subyacentes detrás del delito de phishing y de los distintos tipos de delitos informáticos.

Método Comparativo: Este método lo aplique en el desarrollo del Derecho Comparado, el cual sirvió de gran ayuda ya que me permitió contrastar realidades distintas en bases al estudio de las legislaciones y del mismo modo comparándolas con la legislación ecuatoriana, captando de cada una de ellas información de importancia para el desarrollo de lapresente investigación.

Método Estadístico: Fue empleado para plasmar los datos estadísticos recabados del trabajo de campo realizado, estos datos fueron plasmados en las ilustraciones representativas, usando las técnicas, tanto de la encuesta como de la entrevista, de modo que, logrando de esta manera, recopilar información en base al conocimiento y razonamiento de cada una de las personas encuestadas y entrevistadas, empleado también medios digitales para realizar la tabulación de los datos obtenidos.

Método Sintético: Por último, este método fue empleado para resumir el proceso investigativo, de manera que, se logre exponer los aspectos más relevantes dentro de la investigación realizada lo largo del desarrollo del mismo, fue empleado en el marco teórico yel desarrollo del derecho comparado.

5.3. Técnicas

En el trabajo de campo realizado, se enfocó y direcciono la investigación hacia un ámbito socio-jurídico, poniendo especial énfasis en la problemática objeto de estudio. Para lo cual, se empleó diferentes técnicas como son: la encuesta y la entrevista:

Encuesta: Esta técnica fue aplicada de manera directa, en la ciudad de Loja, a 30 profesionales del Derecho, la cual consistía, en el planteamiento de 5 preguntas puntuales conrespuesta cerrada o concreta, de las cuales, dichos encuestados debían responder Si o No, en base a su criterio, logrando con ello recabar información necesaria, la cual fue

tabulada de manera sistemática a fin de plasmar los resultados obtenidos.

Entrevista: A diferencia de la técnica anterior, esta técnica me permitió entablar un dialogo con el entrevistado, mediante la formulación de preguntas abiertas sobre aspectos fundamentales enfocados a la temática abordada, que permitan al encuestado desenvolverse, en base a su criterio y conocimiento. La entrevista en mención, fue realizada en la Ciudad de Loja, a 5 profesionales del Derecho especialistas, entre los cuales estuvieron inmersos Jueces y Fiscales conocedores de la materia, dicha entrevista, consistió en la formulación de 5 preguntas abiertas, las cuales motivaron al entrevistado al raciocinio e inmersión con la problemática objeto de estudio de la presente investigación.

Observación Documental.

Corresponde para la observación documental el estudio de casos realizado, en base a la problemática abordada.

De los cuales se logró obtener información relevante, así como también, conocimiento acerca del modo en cómo se combate en la actualidad dicha problemática, por medio de los distintos organismos gubernamentales y la función legislativa.

Dichos datos obtenidos resultado de la investigación, son expuestos y plasmados en elpresente documento, usando para ello gráficos, tablas, estadísticas en base a estudios realizados por instituciones estatales, a fin de realizar la verificación de objetivos, reflejar la realidad social actual, falencias en nuestro sistema de justicia, esto en base a la interpretación realizada y del mismo modo, proponer posibles soluciones y recomendaciones a fin de combatir con efectividad dicha problemática social.

6. Resultados

6.1 Resultados de las encuestas

En este apartado se pretende representar los resultados obtenidos durante la ejecución del trabajo de campo, las encuestas fueron realizadas a 30 profesionales del Derecho de la ciudad de Loja.

Primera Pregunta: ¿Conoce en que consiste el delito informático Phishing?

Tabla Estadística 1

Indicadores	Variable	Porcentaje
Si	12	40%
No	18	60%

Tabla 1 Pregunta uno de la encuesta
Fuente: *Encuestas realizadas a profesionales del Derecho*
Autor: *Andy Javier Iñahuazo López*

Gráfica 1

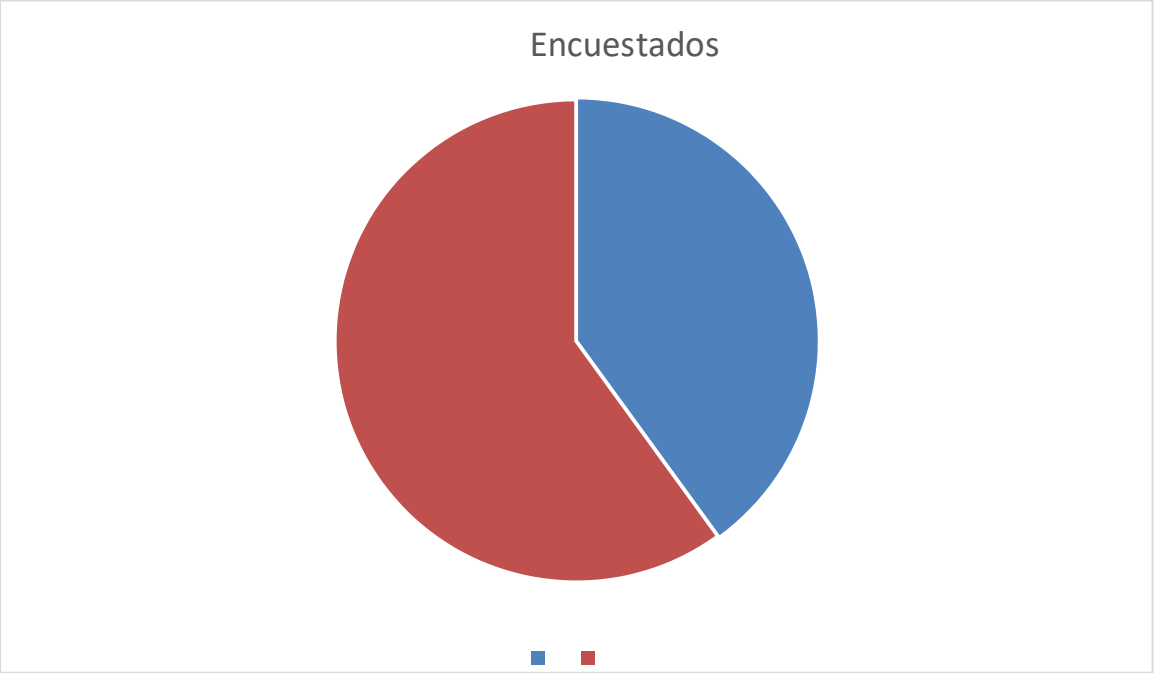


Ilustración 1
Fuente: Encuesta realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Interpretación:

De los datos obtenidos, los cuales son plasmados en la tabla 1 y la ilustración 1, basándonos en dichos resultados a partir de la encuesta realizada, la cual se centra concretamente, sobre el conocimiento que tienen los encuestados, en lo que consiste al delito informático phishing, podemos interpretar que de los 30 encuestados, solamente el 40% de dichos encuestados, saben o tienen una idea encaminada a lo que consiste este delito informático, mientras que por el contrario, el otro 60% no lo sabe.

Análisis:

Con respecto a las respuestas obtenidas, en base a la primera pregunta, se puede verificar que, de los 30 encuestados, solamente el 40% conoce en lo que consiste el Phishing,mientras que el otro 60% no lo sabe.

Este hallazgo sugiere que hay una necesidad de concientización y educación sobre el phishing entre la población encuestada. El phishing es una forma común de ciberataque en la que los delincuentes intentan engañar a las personas para obtener información confidencial, como contraseñas y datos financieros. Dada la prevalencia de amenazas cibernéticas en la actualidad, es crucial que un porcentaje más alto de la población esté informado y preparado para identificar y evitar estos ataques.

Para abordar esta brecha de conocimiento, se podrían implementar estrategias educativas, como seminarios, talleres o materiales informativos, para aumentar la conciencia sobre la ciberseguridad y específicamente sobre el phishing. Además, se podría considerar la integración de conceptos relacionados con la seguridad cibernética en programas educativos formales o en el lugar de trabajo.

Es fundamental destacar la importancia de la educación continua en este ámbito, ya que las amenazas cibernéticas evolucionan constantemente. Un mayor conocimiento sobre el phishing no solo protege a los individuos, sino que también contribuye a la seguridad generalde la comunidad en línea.

Segunda Pregunta: ¿Usted o alguien dentro de su círculo social ha sido víctima de apropiación fraudulenta de su información personal (claves, números de tarjetas de crédito, etc.) mediante engaño a través de correo electrónico, mensajería instantánea, redes sociales o llamadas telefónicas?

Tabla Estadística 2

Indicadores	Variables	Porcentaje
Si	22	73%
No	8	27%

Tabla 2 Pregunta dos de la encuesta
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Gráfica 2

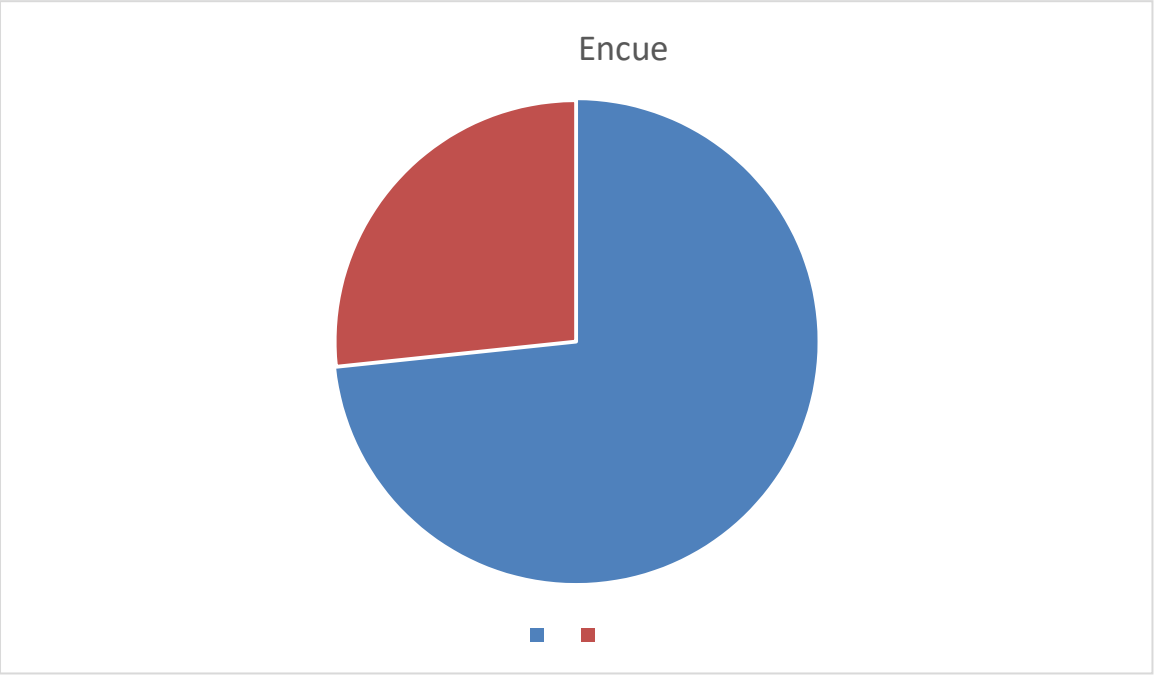


Ilustración 2
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Interpretación:

Basándome en los resultados obtenido, pude verificar que, del total de encuestados, 22 de ellos, que corresponde al 73%, dijeron haber sido víctimas del delito descrito, el cual hace referencia al Phishing, mientras que solo 8 de ellos, que corresponde al 27% dijeron no haber sido víctimas de ninguna de las conductas descritas anteriormente.

Para la mayoría de los encuestados, se familiarizan con la conducta descrita e identifican haber sido víctimas de esta conducta, pero no todos, identifican que la conducta descrita hace referencia al Phishing

Análisis:

Los resultados de la encuesta indican que la mayoría de las personas encuestadas (un 73%) ha sido víctima de la conducta delictiva descrita. Esta opinión puede ser una señal de la preocupación generalizada sobre la seguridad cibernética y la necesidad de una protección más sólida contra los delitos informáticos.

En cuanto a la cifra del 73% de los encuestados que afirmaron haber sido víctimas de esta conducta que hace referencia al Phishing, este dato podría indicar una preocupante prevalencia de este delito en la población encuestada. Para el 27% que

dijeron no haber sido víctimas se debe a como ellos mismo mencionaron, tienen precaución siempre al usar redes sociales, antes de revelar su información personal se percatan de que quien lo solicita cuenta con una cuenta oficial o conocen la complejidad y consecuencia que trae consigo revelar dicha información.

Por lo tanto, los resultados de la encuesta son un llamado a la acción para los responsables de la elaboración y aplicación de la legislación, a fin de considerar medidas parafortalecer la lucha contra los delitos informáticos.

Tercera Pregunta: ¿Considera que la falta de colaboración internacional en el sentido de delitos informáticos afecta la efectividad de la aplicación justicia en Ecuador?

Tabla Estadística 3

Indicadores	Variables	Porcentaje
Si	27	90%
No	3	10%

Tabla 3 Pregunta 3 de la encuesta
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Gráfica 3

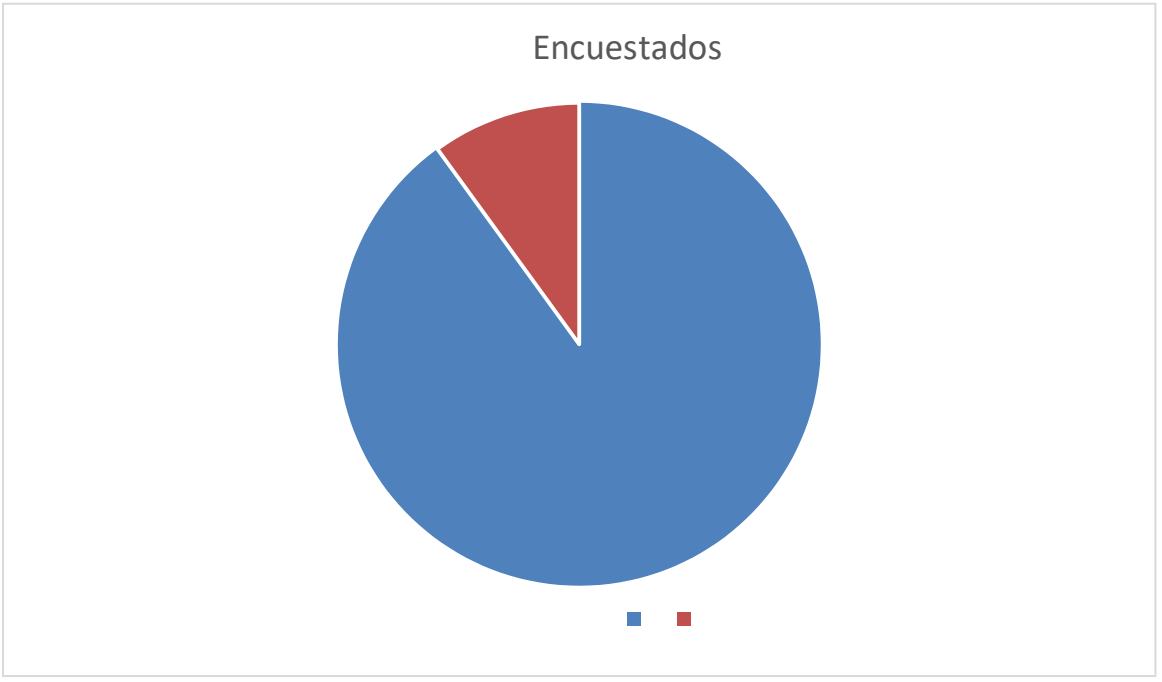


Ilustración 3
Fuente: Encuestas realizadas a profesionales del Derecho

Interpretación:

La interpretación de los resultados de la encuesta indica que la gran mayoría de los encuestados, es decir, el 90%, cree que la falta de cooperación internacional afecta la efectividad de la aplicación de justicia en el sentido de delitos informáticos, esto sugiere que existe una afirmación general que destaca la importancia a que el estado ecuatoriano deba adherirse a algún convenio internacional. Mientras que el 10% del resto de encuestados no consideran que la falta de cooperación internacional afecte la efectividad de la aplicación de justicia.

Análisis:

Los resultados de la encuesta revelan que el 90% de los encuestados sostiene que la falta de cooperación internacional impacta negativamente en la efectividad de la aplicación de justicia en el contexto de delitos informáticos, esto al considerar que los delitos informáticos son delitos transnacionales, por lo que al no contar con esta cooperación es casi imposible lograr una efectiva aplicación de justicia. Este consenso subraya la percepción generalizada de la importancia crucial de que el Estado ecuatoriano se adhiera a algún convenio internacional para mejorar la colaboración entre países en la lucha contra los delitos cibernéticos. Por otro lado, el 10% restante de los encuestados no comparte la opinión de que la falta de cooperación internacional afecte la efectividad de la aplicación de justicia en casos de delitos informáticos. Esta perspectiva minoritaria puede reflejar la confianza en las leyes nacionales para abordar eficazmente estos casos sin depender en gran medida de la colaboración internacional. Este contraste de opiniones destaca la necesidad de considerar medidas que fortalezcan la cooperación internacional, abordando desafíos específicos como la extradición de criminales cibernéticos y el intercambio de pruebas electrónicas.

Cuarta Pregunta: ¿Cree usted necesario que el estado ecuatoriano a través de sus diferentes instituciones debería crear campañas masivas a fin de brindar información acerca de delitos informáticos y como prevenirlos?

Tabla Estadística 4

Indicadores	Variables	Porcentaje

Si	30	100%
No	0	0%

Tabla 4
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Gráfica 4

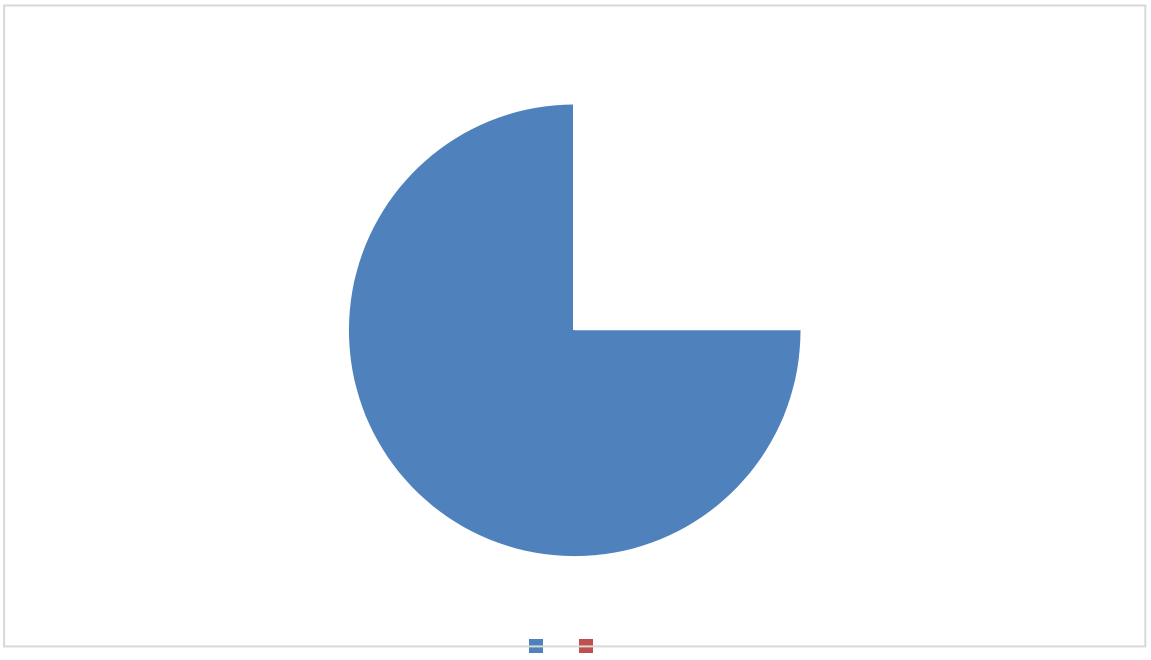


Ilustración 4 pregunta cuatro

Fuente: Encuestas realizadas a profesionales del Derecho

Autor: Andy Javier Iñahuazo López

Interpretación:

Los resultados de la encuesta revelan un consenso del 100% entre los encuestados, quienes coinciden en que el Estado ecuatoriano debería llevar a cabo campañas masivas a través de sus diversas instituciones. El objetivo de estas campañas sería proporcionar información detallada a la ciudadanía sobre los delitos informáticos: cómo se llevan a cabo, sus modalidades y las medidas preventivas recomendadas.

Análisis:

Los resultados obtenidos de la encuesta indican un acuerdo unánime del 100% entre los participantes, lo cual es un dato significativo y relevante. Los encuestados comparten la opinión de que el Estado ecuatoriano debería emprender campañas masivas

mediante sus diversas instituciones. Este consenso destaca la importancia que los profesionales del derecho asignan a la necesidad de abordar y prevenir los delitos informáticos en el contexto ecuatoriano.

La propuesta de llevar a cabo campañas masivas a través de las instituciones estatales revela una preocupación colectiva por mejorar la conciencia ciudadana sobre los delitos informáticos. Este enfoque proactivo es esencial en un entorno legal en constante evolución, donde la tecnología desempeña un papel cada vez más integral en la sociedad. Al reconocer la importancia de proporcionar información detallada, los encuestados demuestran su compromiso con la educación preventiva y la concienciación en materia de ciberseguridad.

La necesidad de informar a la ciudadanía sobre cómo se llevan a cabo los delitos informáticos, sus diferentes modalidades y las medidas preventivas recomendadas, resalta la importancia de abordar este fenómeno desde una perspectiva integral. En este sentido, los profesionales del derecho no solo reconocen la existencia de estos delitos, sino que también subrayan la necesidad de empoderar a la sociedad con conocimientos que les permitan protegerse de manera proactiva.

Quinta Pregunta: ¿Cree usted que una iniciativa importante por parte del Estado es la de tipificar el delito de phishing?

Tabla Estadística 5

Indicadores	Variables	Porcentaje
Si	28	93,03%
No	2	6,07%

Tabla 5: Pregunta cinco
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Gráfica 5

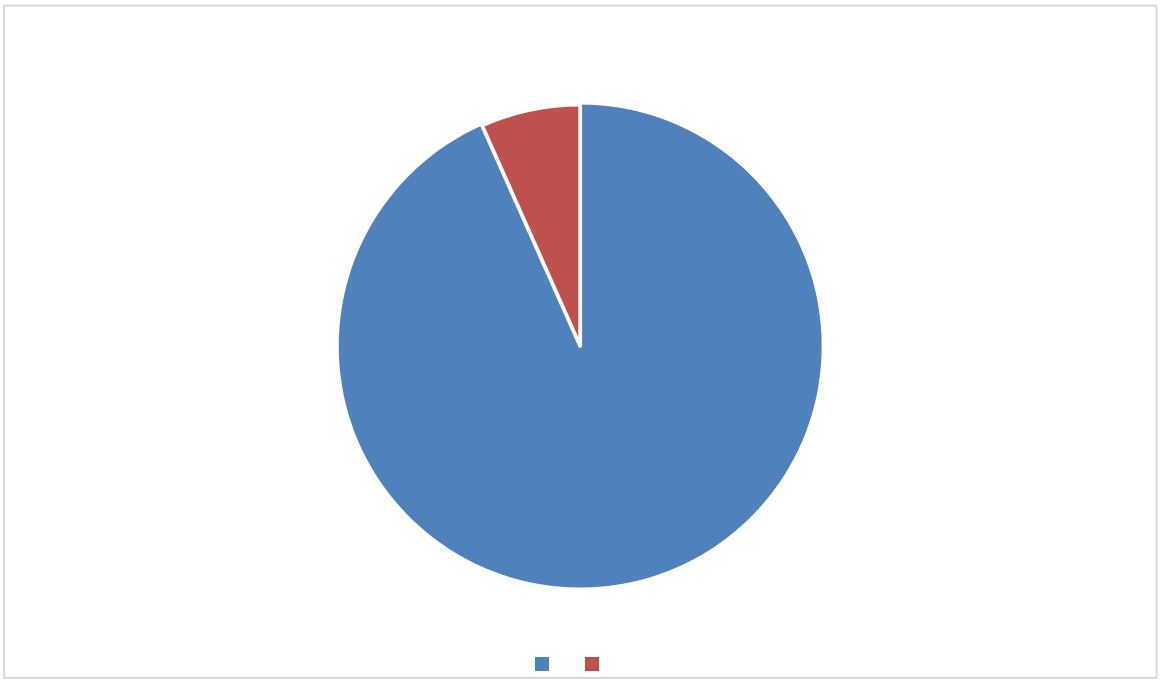


Ilustración 5 Pregunta cinco
Fuente: Encuestas realizadas a profesionales del Derecho
Autor: Andy Javier Iñahuazo López

Interpretación:

Los resultados de la encuesta indican que la mayoría de los encuestados, en específico 28 de ellos, que corresponden al 93%, creen que la tipificación del delito de phishing sería una iniciativa importante por parte del estado ecuatoriano. Esto sugiere que existe una clara demanda de acción legislativa para abordar este delito informático, ya que este, es uno de los métodos más comunes utilizados por los delincuentes cibernéticos dentro de nuestra legislación, con el cual logran obtener información confidencial lo que genera una gran problemática para el estado y la comunidad en general. Las 2 personas restantes que corresponden al 7% de los encuestados expresan una opinión divergente respecto a la tipificación del delito.

Análisis:

A partir de los resultados obtenidos, se evidencia de manera contundente una creciente demanda dentro de la población representada por el 93% de los encuestados, los cuales comparten que, los legisladores deben adoptar medidas rigurosas con el objetivo de hacer frente a la preocupante amenaza de los delitos informáticos, destacándose el phishing como uno de los más prevalentes y perjudiciales. La tipificación del delito de phishing se erige como una necesidad ineludible en este contexto. La distinción de esta modalidad delictiva no solo proporcionaría una mayor precisión en la

identificación y seguimiento de esta conducta, sino que también facilitaría de manera significativa los procesos de investigación y enjuiciamiento. La tipificación del phishing no solo serviría para delinear con mayor claridad las acciones punibles, sino que también enviaría un mensaje claro a los potenciales delincuentes, con el fin de desalentar futuras actividades ilícitas en este ámbito.

6.2 Resultados de las entrevistas:

Para el desarrollo de las entrevistas, se procedió a la formulación de 5 preguntas abiertas, dirigidas a 5 profesionales del Derecho especialistas en Derecho Informático y Derecho Penal de la ciudad de Loja, mediante la cual, a través de dichas preguntas planteadas se incito al entrevistado, al razonamiento profundo, con el fin de que este brinde información necesaria en base a su criterio y conocimiento, enriqueciendo esta investigación con contribuciones significativas.

Esto a su vez, contribuyo a que se logre abordar la problemática planteada y conocer ciertas falencias, para lo cual se procedió en 2 ocasiones a dar uso de una grabadora de voz y los 3 restantes se desarrollaron de manera virtual por medio de la plataforma de zoom, estas fueron transcribidas del mismo modo en el presente documento, las cuales son analizadas e interpretadas a continuación.

Entrevistas

Pregunta: ¿Sabe usted de que trata el Phishing?

Primer Entrevistado: Sí, es un delito de suplantación de identidad.

Segundo Entrevistado: No, eh escuchado, pero no lo tengo claro.

Tercero Entrevistado: Sí, es un delito que vulnera la confidencialidad y la información intima de las personas.

Cuarto Entrevistado: Si, se lo considera como delito informático y se consuma con el uso de medios electrónicos.

Quinto Entrevistado: Si, conozco en que consiste, pero esto se debe prácticamente a que hemos confiado nuestra intimidad nuestra información reservada a un ordenador, el cual en cualquier momento puede ser vulnerado sin nosotros como usuarios poder tener conocimiento. Conforme avance las TIC, se van originando nuevas modalidades o tipos de delitos informáticos, que afectan no solamente derechos patrimoniales, sino también la confidencialidad de la persona.

Comentario del Autor:

Basándonos en los datos proporcionados, podemos concluir que el conocimiento

sobre el phishing no es un concepto claro para los entrevistados, debido a que atribuyen la conducta a diferentes delitos, de los cinco entrevistados, tres de ellos dicen saber que es el Phishing y tienen una idea de lo que trata, mientras que uno de los encuestados no conoce deltema. Es importante destacar que el phishing es una forma común de ataque en línea que puede causar graves consecuencias financieras y personales si no se maneja de manera adecuada, al ser un delito que vulnera múltiples derechos es conceptualizado de diversas formas y quizá a eso se deba el que no haya una definición concreta.

Pregunta: ¿Tienes usted conocimiento, si este delito informático Phishing está tipificado en la ley penal?

Primer Entrevistado: Es un delito muy común que pasa todos los días, la denominación que se le dé en si no es importante, lo que importa es que la conducta se adecue al tipo penal más semejante.

Segundo Entrevistado: A lo que tengo entendido, es que existe un espacio en el COIP para delitos informáticos, de allí se debe salir la figura jurídica para sancionar este delito.

Tercer Entrevistado: En ocasiones suelen referirse a estafa, pero pienso que más bien este delito informático va enfocado a la interceptación ilegal de datos.

Cuarto Entrevistado: Para el caso de los delitos informáticos, estos se juzgan en base al COIP, en el que se tipifican algunos de estos delitos informáticos.

Quinto Entrevistado: En el código penal se contiene estafa en la generalidad, pero que no está configurado como delito derivado de las TIC, podría estar en forma general, en locual se pretenda enmarcar los delitos en una sola manifestación. En el COIP no eh sabido ni si quiera que se han incluido reformas respecto a los tipos de delitos informáticos, estudios, análisis sí, pero no proyecto de reforma. Pero adecuar la legislación aún resulta un problema, porque se necesita llegar hasta el origen mismo de donde se producen los delitos y eso es muy variable.

Comentario del Autor:

En primer lugar, los entrevistados tienen un conocimiento básico sobre el término en cuestión, esto puede indicar una brecha en la formación y educación de los especialistas en cuestiones relacionadas con la ciberseguridad y el derecho informático. El hecho de que los especialistas no estén familiarizados podría indicar múltiples razones, una de ellas que, en el sentido de delitos informáticos, estos son cambiantes y evolucionan a la par con el desarrollo de las tecnológico, además que vulneran múltiples

derechos, por lo que su conceptualización es compleja.

Mientras el primer entrevistado destaca la flexibilidad conceptual al subrayar la importancia de la adecuación de la conducta a un tipo penal similar, sugiriendo así una aproximación menos rígida en la denominación del delito, el segundo entrevistado enfoca la atención en el COIP, insinuando que este código podría ser el instrumento legal para sancionar delitos informáticos, incluido el phishing. Sin embargo, el tercer entrevistado introduce la idea de que, a pesar de la ocasional referencia al phishing como estafa, su esenciase inclina más hacia la interceptación ilegal de datos, resaltando la necesidad de considerar las particularidades de este tipo de delitos. El cuarto entrevistado respalda la idea de que los delitos informáticos se juzgan en base al COIP, indicando una posible aplicabilidad de la legislación existente a casos de phishing. En contraste, el quinto entrevistado señala la generalidad con la que se aborda la estafa en el código penal y la falta de configuración específica como delito derivado de las Tecnologías de la Información y la Comunicación (TIC). Este último comentario destaca la posibilidad de que la legislación no esté completamente actualizada para abordar con precisión los delitos informáticos, incluido el phishing, resaltando la importancia de reformas legales que se ajusten a la dinámica evolutiva de las prácticas delictivas en el ámbito digital. En conjunto, estas perspectivas sugieren una necesidad potencial de revisar y ajustar la legislación para abordar de manera más específica y efectiva los delitos informáticos en el contexto cambiante de la ciberseguridad.

Pregunta: ¿Considera usted que debe incluirse en el Código Orgánico Integral Penal el delito informático de Phishing?

Primer Encuestado: No creo que sea necesario tipificar este delito de forma literal, ya que este tipo de delito vulnera múltiples derechos constitucionales, lo cuales no pueden ser abarcados en un solo tipo penal, de la línea que se considera que todo tiene que estar descrito exactamente en el tipo penal. Me parece que esa exageración, en ocasiones permite espacios para la corrupción y para que mucha gente se haga de la vista gorda

El derecho siempre va a tener un margen de indeterminación, el cual será llenado con el juez, siempre común adecuado criterio, el que determinara cuando realmente esa indeterminación es relevante, causa indefensión a esa persona, cuando afecta una garantía y cuando esa alegación de falta y determinación simplemente es un ejercicio de retórica,

con elfin a veces de irse por la tangente y sacarse a un delincuente de la cárcel, lo cual se torna polémico. El derecho no es una ciencia exacta es una ciencia de razonabilidad.

Segundo Encuestado: Si es necesario tipificarlo, ya que, de no hacerlo, podría existirla violación al principio constitucional de legalidad, siempre y cuando la conducta este descrita como ilícita o ilegal dentro de la normativa penal, antes de haberse cometido el delito, por tanto, si creo conveniente se tipifique esta conducta.

Tercer Encuestado: En mucho de los casos los administradores de justicia, como lo son los fiscales y los jueces al no encontrar una figura específica en la normativa penal, usan el que más se asemeje y en ocasiones estos no dan atención al medio por el cual se comete unilícito, que en este caso es el uso de la tecnología.

Cuarto Encuestado: Si lo creo importante, en base al principio de aplicación objetivade la Ley, que se confiere en el art 226 de CRE es un principio de legalidad, sirve para formar y tutelar el derecho, pero el art 81 nos habla de la protección del derecho, frente a un principio debemos poner un derecho, que en este caso sería el derecho a la seguridad jurídica, con leyes claras, previas, publicas que nos den certeza a los ciudadanos para saber en qué marco nos estamos desenvolviendo, como nos vamos a desarrollar, como nos vamos a comportar en sociedad.

Quinto Encuestado: Si lo creo pertinente, implica ahí la confianza legítima, está íntimamente ligada con el derecho a la seguridad jurídica, como ciudadano necesito, saber que, tengo una disposición legal, que esta previamente determinada, que, si me dice, realizas esta acción, te sometes a esta sanción y si no está prohibida en la ley, según el código civil, está permitida y si no está prohibido en el COIP, podría ejecutarse, porque la ley no me determina que mi conducta, se adecua a un modelo social, a un modelo de convivencia social, en consecuencia, si me pretende sancionar por un delito, por una falta administrativa, si no está previamente determinada y establecida, no acarrea únicamente la falta de legalidad sino también la violación al derecho a la seguridad jurídica. Por tanto, tiene que estar necesariamente tipificado, previamente prevista la conducta o la falta, para poder ser judicializado, o para poder ser sancionado administrativamente.

Comentario del Autor:

Cuatro de los entrevistados parecen estar tomando una posición más restrictiva en relación con el principio de legalidad, hace alusión a que, todo acto que no esté prohibido porla ley se considera permitido. En otras palabras, si una conducta no está expresamente

prohibida por la ley, entonces no puede ser considerada como delito y esto a su vez vulnera el principio de legalidad. Esto es consistente con la noción de que el Estado solo puede ejercer su poder coercitivo si se lo permite la ley, del mismo modo, es posible que estén haciendo referencia al principio de taxatividad o reserva legal, que establece que no se puede castigar una conducta si esta no está expresamente prevista en la ley. Según este principio, solo se puede sancionar una conducta si existe una norma que la prohíba expresamente.

Es importante destacar que, aunque existen diferentes interpretaciones sobre el alcance del principio de legalidad, es un principio fundamental en cualquier sistema jurídico democrático. El principio de legalidad establece que nadie puede ser condenado por una conducta que no esté expresamente prevista en la ley, esto garantiza que el Estado no pueda ejercer su poder coercitivo de manera arbitraria o caprichosa. Es importante tener en cuenta que el principio de legalidad es un elemento clave en cualquier sistema jurídico democrático, y que su violación puede tener consecuencias graves para los derechos, garantías y libertades de los ciudadanos.

Pregunta: ¿Cree necesario reformar la ley penal en materia de delitos informáticos?

Primer Encuestado: No lo considero necesario, los ciberdelitos están tipificados de distintas formas en la ley penal, si una persona comete un delito recibe una sanción.

El problema no es la tipificación del delito, sino más bien es con la prueba, en la valoración de la prueba y del buen uso del criterio.

Segundo Encuestado: Si considero que es necesario, en el caso de los ciberdelitos, estos no solo se cometen dentro del territorio nacional, sino que son delitos transnacionales,lo que complica su persecución es que el estado ecuatoriano aún no se ha suscrito a ningún tratado ni convenio con otras naciones para combatir estos delitos.

Tercer Encuestado: Si, es necesario una reforma a la ley penal, puesto que, al paso acelerado de la evolución tecnológica, los legisladores aún no han tomado la importancia debida a los delitos informáticos.

Cuarto Encuetado: En realidad si lo considero necesario, porque aún hay mucho por esclarecer en las leyes y es muy importante que se le de mayor importancia a los delitos informáticos. Naciones unidad tiene el pronunciamiento respecto a la precaución

que deben tomar los estados respecto a las nuevas tendencias de delitos a través de medios informáticos y como debe adecuar la legislación.

Quinto Encuestado: Debe ser reformado de manera urgente, puesto que, no están catalogados todas la manifestaciones o modos que se dan los delitos informáticos y todavía vivimos quizá enmarcados únicamente en una burbuja territorial, que no somos capaces de ver más allá de lo que sucede en Ecuador.

Necesitamos ir pensando ya no como comunidad delimitada en territorio, sino como comunidad en general, como seres humanos. Para lograr así, que cuando surja una nueva manifestación de delitos, poder buscar soluciones entre legislaciones a fin de combatir dichosdelitos de manera efectiva.

La legislación penal tiene que ser dinámica, tiene que ajustarse a los tiempos, a las realidades para en base a esta globalización, en base a estas conductas, poder nosotros proveer que no se pueda dar en nuestro país, y de darse ya estén catalogados como delitos y con su respectiva pena.

Comentario del Autor:

Los resultados obtenidos revelan que la mayoría de los entrevistados abogan por una reforma efectiva del Código Orgánico Integral Penal (COIP). Esta inclinación hacia la necesidad de modificaciones sugiere que existe una percepción generalizada de que, para resguardar y proteger de manera más eficaz los derechos constitucionales de los ciudadanos, es imperativo que el marco legal actual se adapte a las dinámicas cambiantes de la sociedad, especialmente en lo que respecta a los delitos informáticos. La constatación de que la mayoríade los encuestados respalda la idea de reformar el COIP para abordar los delitos informáticosindica una conciencia creciente sobre la importancia de enfrentar los desafíos emergentes en el ámbito digital. Este consenso subraya la necesidad de mejorar y actualizar la normativa penal, transformándola para que sea capaz de hacer frente a las complejidades y sutilezas de los ciberdelitos de manera más efectiva.

La urgencia de reformar la legislación penal se vincula estrechamente con la necesidad de mantenerse al día con el vertiginoso avance tecnológico y las nuevas formas de delincuencia que surgen en el entorno digital. En este contexto, la reforma del COIP no solo implica la inclusión de nuevos tipos de delitos informáticos, sino también la revisión y actualización constante de las disposiciones existentes para garantizar que sean

lo suficientemente robustas y adaptables a las cambiantes realidades actuales.

Pregunta: Dada la naturaleza transnacional de los delitos informáticos,incluido el phishing, ¿Considera importante la cooperación internacional?

Primer Encuestado: Siempre hay que hacer ajustes sin duda, pero principalmente pienso que debemos cambiar nuestra cultura jurídica, porque a veces los niveles de institucionalidad no son lo mismo en todas las provincias.

Segundo Encuestado: Seria una muy buena iniciativa, claro está que la cooperación internacional es un gran beneficio ya que, al tratarse de delitos informáticos, estos no necesariamente son cometidos dentro del estado ecuatoriano, sino que pueden cometerse desde cualquier país.

Tercer Encuestado: Antes que todo ello, se debería crear organismos o mecanismos de investigación especializada, que logren una verdadera y efectiva persecución para lograr dar con el autor del ilícito.

Cuarto Encuestado: Si, el formar alianzas o convenios con otros estados sería algo importante, ya que al contar con la ayuda de estos se lograría una verdadera persecución e identificación del autor de este tipo de delitos, ya que en muchos casos no siempre este los comete dentro de nuestra jurisdicción territorial.

Quinto Encuestado: Para lograr esto resulta necesario que nuestra legislación procure capacitar a nuestros fiscales, policía judicial y demás organismos que persiguen o investigan el delito, con el fin de que estos tengan la capacidad de lograr descubrir al autor del hecho.

Comentario del Autor:

La mayoría de los entrevistados, incluyendo al segundo, cuarto y quinto, coincide en que estos delitos no están circunscritos a las fronteras nacionales y, por lo tanto, la cooperación internacional es esencial. El segundo entrevistado destaca que, al tratarse de delitos informáticos, estos pueden perpetrarse desde cualquier país, subrayando la naturaleza transnacional de la ciberdelincuencia. El cuarto entrevistado respalda la importancia de formar alianzas con otros estados, subrayando que la colaboración externa es fundamental para lograr una auténtica persecución e identificación de los autores, especialmente cuando estos no actúan dentro de la jurisdicción territorial del país. Por su parte, el quinto entrevistado destaca la necesidad de capacitar a los fiscales y organismos de investigación, señalando la importancia de que la legislación proporcione las herramientas necesarias para enfrentar estos delitos. Aunque el primer y tercer

entrevistado proponen ajustes en la cultura jurídica y la creación de organismos especializados, respectivamente, también reconocen la necesidad de cambios y mejoras en la persecución de estos delitos. En conjunto, la entrevista revela un consenso entre los participantes sobre la importancia crucial de la cooperación internacional y la necesidad de ajustes legales y capacitación para enfrentar eficazmente los desafíos transnacionales de la ciberdelincuencia.

6.3 Estudio de Casos

Noticia #1

Pedro Vicente Maldonado (Pichincha), 08 de octubre de 2020.- Seis personas –casi todos de una misma familia– son investigadas dentro de un proceso penal por presunta apropiación fraudulenta por medios electrónicos.
El fiscal del caso, Hugo Pérez, formuló cargos la tarde de este 8 de octubre de 2020, en la Unidad Judicial de Pedro Vicente Maldonado, al noroccidente de Quito.

Cuatro de los procesados quedaron con prisión preventiva y dos con presentaciones periódicas ante la autoridad y prohibición de salida del país, debido a que pasan los 65 años de edad. La instrucción fiscal durará noventa días.
Los dos adultos mayores, alias "Papá" y "Mamá", así como los otros cuatro, renombrados como "Neutrón", "Topo", "Chino" y "Taz", habrían conformado una organización ciberdelincuencial.

Su presunto modo de operar consistía en utilizar 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.

Esta teoría presentada por el fiscal Hugo Pérez, al Juez de Garantías Penales, en la audiencia de formulación de cargos, se sostuvo en veintiséis elementos de convicción, levantados en el operativo "Phishing", ejecutado la tarde del 7 de octubre de2020, en las provincias de Los Ríos y Santo Domingo de los Tsáchilas; así como los levantados durante la investigación previa, iniciada en agosto de 2020 por la Fiscalía de Pedro Vicente Maldonado, en cooperación con unidades especiales de la Policía Nacional.

Desde el inicio de la pandemia hasta octubre, la organización habría acumulado unos 80.000 dólares en sus cuentas y adquirido tres vehículos, de los cuales dos fueron incautados en el operativo.

Dato jurídico

El delito de apropiación fraudulenta por medios electrónicos está tipificado en el artículo 190 del Código Orgánico Integral Penal (COIP) y determina una pena privativa de la libertad de uno a tres años a la persona que "utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones".

Link de la noticia: ***https://www.fiscalia.gob.ec/fiscalia-abrio-instruccion-fiscal- contra-6- procesados-por-presunto-phishing/***

Infractor/s: Se conoce de 6 personas procesadas (casi todos de la misma familia), de las cuales, cuatro de ellos se les dicta prisión preventiva, mientras que, a los 2 restantes, al ser personas mayores de 65 años, se les dicta presentaciones periódicas ante la autoridad y prohibición de salida del país.

A los cuatro sujetos con prisión preventiva, responden a: Neutrón, Topo, chino y Taz.

Y los dos adultos mayores, responden a: Mamá y Papá

Los cuales habrían conformado una organización ciberdelincuencia.

Víctima: Sujetos pasivos, a los que se les robaba números de tarjetas o códigos confidenciales y personales, con fines ilícitos.

Hecho: El operativo denominado "Phishing", se desarrolló el 07 de octubre del 2022, en las provincias de Los Ríos y Santo Domingo de los Tsáchilas, en la cual FGE, indago que dichos procesados utilizaban números de tarjetas y códigos robados en Estados Unidos y Europa, para comprar cuentas de streaming y mercadería en plataformas virtuales, durante la investigación se pudo corroborar que dichos procesados habrían recaudado alrededor de $80.000 en sus cuentas bancarias y adquirido tres vehículos.

Comentario:

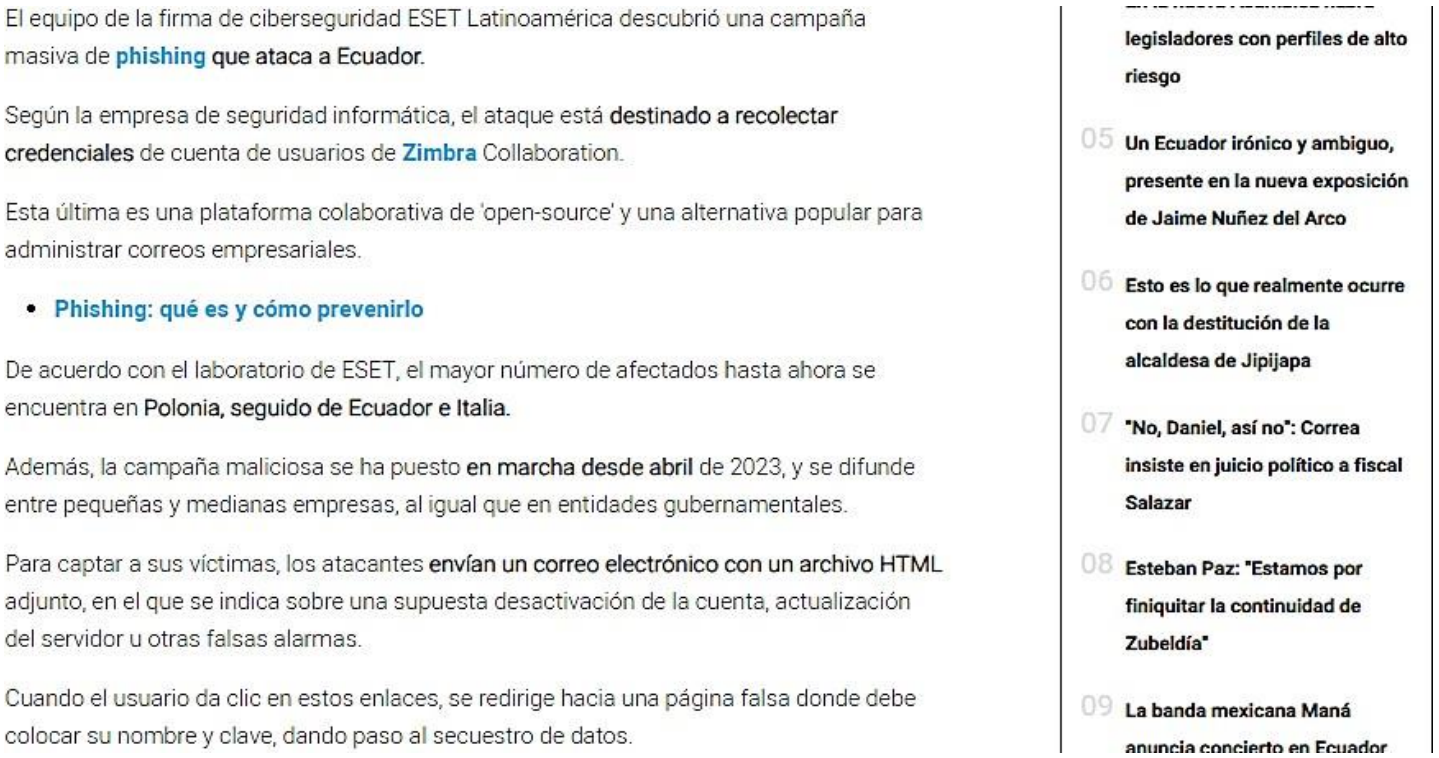
En la presente noticia se puede evidenciar una investigación, realizada por parte de la fiscalía general del Estado, en la cual se investiga el presunto delito de apropiación fraudulenta por medios electrónicos tipificado en el artículo 190 del COIP.

"La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014).

Cabe recalcar que el fiscal del caso correspondiente, realizo la etapa de formulación de cargos basándose en este artículo, por lo que se entiende que Fiscalía General del Estado, considera que este delito tipificado se adecua a la conducta delictiva de Phishing.

La etapa de formulación de cargos es un paso crucial en cualquier caso penal. Es entonces cuando la fiscalía acusa formalmente al sospechoso basándose en las pruebas reunidas durante la investigación. Cabe señalar que en este caso la fiscalía decidió procesar los sospechosos según una disposición específica. Aparentemente este artículo parece contener directrices y elementos que definen el delito de phishing, y los fiscales han determinado que la actividad delictiva en cuestión entra dentro de esa categoría. La decisión de la Fiscalía de presentar cargos por el delito de "Apropiación fráudenla por medios electrónicos", significa que ha evaluado cuidadosamente las pruebas disponibles y ha llegadoa la conclusión que este encuadra las características del phishing.

Noticia #2



El equipo de la firma de ciberseguridad ESET Latinoamérica descubrió una campaña masiva de **phishing** que ataca a Ecuador.

Según la empresa de seguridad informática, el ataque está **destinado a recolectar credenciales** de cuenta de usuarios de **Zimbra** Collaboration.

Esta última es una plataforma colaborativa de 'open-source' y una alternativa popular para administrar correos empresariales.

- **Phishing: qué es y cómo prevenirlo**

De acuerdo con el laboratorio de ESET, el mayor número de afectados hasta ahora se encuentra en **Polonia, seguido de Ecuador e Italia**.

Además, la campaña maliciosa se ha puesto **en marcha desde abril** de 2023, y se difunde entre pequeñas y medianas empresas, al igual que en entidades gubernamentales.

Para captar a sus víctimas, los atacantes **envían un correo electrónico con un archivo HTML** adjunto, en el que se indica sobre una supuesta desactivación de la cuenta, actualización del servidor u otras falsas alarmas.

Cuando el usuario da clic en estos enlaces, se redirige hacia una página falsa donde debe colocar su nombre y clave, dando paso al secuestro de datos.

Link de la noticia: https://www.primicias.ec/noticias/tecnologia/ecuador-ataque-phishing-usuarios/

Infractor/s: Agente/s transnacionales

Víctima: Usuarios miembros de Zimbra Collaboration en Ecuador (Plataforma colaborativa de "open-source" y una alternativa popular para administrar correos empresariales), pequeñas y medias empresas ecuatorianas y entidades gubernamentales.

Hecho: La firma de ciberseguridad ESET Latinoamérica, identifico una campaña basada en ataques de forma masiva dirigida a los miembros de Zimba Collaboration, la cual es una plataforma colaborativa de "Open-source" popular en la administración de correos empresariales. Para lo cual los atacantes a modo de atraer a las víctimas, utilizan métodos engañosos, como enviar correos electrónicos con archivos HTML adjuntos. Estos correos electrónicos advierten sobre la desactivación de cuentas, actualizaciones del servidor u otras falsas alarmas. Cuando los usuarios hacen clic en los enlaces del archivo HTML, son redirigidos a una página web falsa que imita una página web legítima. Esta página solicita al usuario que ingrese su nombre y contraseña. Después de que el usuario proporciona esta información, el atacante roba los datos.

El análisis de ESET muestra que esta campaña de phishing no difiere en

complejidad técnica, pero vale la pena señalar que el código HTML utilizado en los correos electrónicos essignificativo.

Comentario: Este documento destaca la importancia de una legislación penal sólida en Ecuador para sancionar, regular y disuadir las actividades delictivas relacionadas con el delito cibernético. La reciente detección de una campaña de phishing a gran escala dirigida a usuarios de la plataforma de colaboración Zimba de ESET Latinoamérica subraya la necesidad de leyes actualizadas y efectivas para proteger a los ciudadanos y las empresas de las amenazas cibernéticas. En este caso particular, los atacantes utilizan métodos engañosos, como correos electrónicos falsos con archivos adjuntos HTML, para llevar a cabo sus actividades delictivas. Dado que el código HTML utilizado también es legal, si estos mensajes son falsos o poco sutiles, dificulta que las personas detecten la estafa. Hackear información confidencial, como nombres de usuarios y contraseñas, es una violación grave de la privacidad y seguridad de personas y organizaciones.

En este contexto, es esencial contar con leyes penales sólidas y actualizadas para tipificar y castigar eficazmente estos actos delictivos. Estas leyes también deberían incluir disposiciones específicas para combatir el delito cibernético y establecer sanciones proporcionales a la gravedad de los actos cometidos. También es importante que la ley prevea la cooperación entre las autoridades locales y las organizaciones de seguridad cibernética para garantizar una respuesta rápida y coordinada a las amenazas cibernéticas. La conciencia pública sobre el delito cibernético está aumentando constantemente, lo que indica la necesidad de adoptar medidas legislativas decisivas. Las leyes penales eficaces no sólo disuaden a los delincuentes, sino que también brindan a las autoridades las herramientas que necesitan para investigar, rastrear y procesar a los delincuentes. Finalmente, invertir en un derecho penal moderno y adecuado es una medida clave para garantizar la integridad y la confianza en el entorno digital del Ecuador.

7. Discusión

Para llevar a cabo la discusión de los resultados obtenidos durante la realización del trabajo decampo, es importante contrastar y verificar el cumplimiento de los objetivos tanto general, como especifico, los cuales se presentan a continuación.

7.1Verificación de los Objetivos

La presente investigación, consta de un objetivo general y tres objetivos específicos, los cuales se planteó obtener al inicio del trabajo de integración curricular, dichos objetivos son los que se detallan y verifican a continuación.

7.2 Objetivo General.

A partir del planteamiento del problema se determinó el objetivo general el que consiste en:

"Realizar un estudio jurídico y doctrinal en el cual se denote la afectación al bien jurídico protegido por el estado en el delito de Phishing mediante el uso de medios tecnológicos y la importancia de la tipificación como delito informático"

El objetivo general propuesto fue cumplido, lo cual se verifica en el marco teórico, en el cual se analiza en el subtema denominado "Bienes Jurídico Vulnerados en el delito informático de Phishing ", en el cual se ha explicado como ciertos derechos son vulnerados al perpetrase este delito, el cual afecta gravemente el bien jurídico protegido por el estado, en particular el derecho a la seguridad jurídica al no tipificarse en la ley penal esta figura delictiva y que su prevención y sanción son esenciales para garantizar la seguridad y privacidad de la información de los ciudadanos quienes usan las Tecnologías de la Información y Comunicación como algo esencial para su desarrollo social y económico. Así mismo se cumple con la propuesta de reforma al Código Orgánico Integral Penal, demostrando con ello, la importancia y relevancia de estas nuevas figuras delictivas a fin de que se considere la tipificación de esta conducta delictiva como lo es el Phishing.

7.3 Objetivos Específicos.

Se planteó conseguir 3 objetivos específicos con el desarrollo de la presente investigación, los cuales se detallan a continuación:

"Plasmar mediante esta investigación los altos índices de criminalidad existentes en la actualidad en el ciberdelito de Phishing, empleando las TIC como herramienta para lograr el fin delictivo"

Durante el desarrollo de esta investigación se han recopilado diversos datos y estadísticas que evidencian los altos índices de criminalidad que existen actualmente en Ecuador en el ámbito de los ciberdelitos. Se plantea en el objetivo verificar solamente los índices de criminalidad del ciberdelito de Phishing, lo cual no se pudo cumplir con exactitud, ya que esta figura delictiva no se tipifica de forma literal, en su defecto, se

demostró los índices de criminalidad existentes acerca algunos de delitos informáticos en el estado ecuatoriano, con la ayuda de representaciones gráficas, plasmadas en el marco teórico.

Se verifica a su vez, que las TIC son un elemento primordial para lograr consumar o lograr el hecho delictivo, ya que de eso parte los ciberdelitos, del uso de las diferentes herramientas tecnológicas para lograr el cometido y que su uso se ha extendido en gran medida, debido a que, las TIC facilitan la comisión del delito y el anonimato de los ciberdelincuentes.

"Aportar a la comprensión de los ciberdelitos desde un punto de vista crítico, en el cual se pretenderá demostrar la importancia que tiene el derecho informático para laregulación y control de los delitos informáticos".

Se ha logrado constatar el cumplimiento del objetivo de aportar a la comprensión del ciberdelito, ya que, en la investigación realizada, se empleó el uso referente de fuentes fidedignas las cuales lograron investigación e interpretación de varios del cual se ha demostrado la importancia que tiene el derecho informático en Ecuador para la regulación y control de los delitos informáticos, específicamente en el caso del delito de phishing.

Se evaluaron críticamente las limitaciones y deficiencias de las leyes y regulaciones existentes sobre delitos cibernéticos. Esto incluye analizar situaciones en las que la aplicación de la ley es inadecuada o ineficaz debido a lagunas en la legislación o falta de recursos, también se han identificado áreas que requieren mejoras específicas.

Además, se destacó la importancia del derecho informático como disciplina compleja que incluye aspectos jurídicos y técnicos. Se ha demostrado que una comprensión más profunda de las tecnologías de la información y las comunicaciones es esencial para formular leyes y políticas públicas eficaces que puedan abordar la evolución continua de la criminalidad informática y a su vez de los delitos informáticos. Todo lo anterior ha permitidogenerar un conocimiento crítico sobre los ciberdelitos y el derecho informático, lo que contribuirá mejorar la capacidad del Estado y de la sociedad en general para hacer frente a estos fenómenos.

"Demostrar la falta de organismos especializados e insuficiente normativa específica en el sistema jurídico que logre dar solución a esta problemática social, de modo que se pretenda enfocar la importancia y relevancia que se debe dar a los ciberdelitos".

En este sentido, se ha constatado que el Código Orgánico Integral Penal, aborda algunos delitos informáticos y al realizar el estudio de casos se puede verificar que no necesariamente se necesita una norma penal específica para combatir estos delitos, sino más bien adecuarlos e incluirlos a la normativa penal. Lo que resalta la importancia es que las autoridades encargadas de investigar y perseguir los ciberdelitos no cuentan con las herramientas ni la capacitación adecuada para llevar a cabo su labor de manera efectiva. Por tanto, se hace necesario enfocar la importancia y relevancia que se debe dar a los ciberdelitosy promover una mayor atención y recursos para combatirlos de manera efectiva, tomando medidas concretas para dar solución a esta situación y garantizar la protección de la población ante los ciberdelitos.

7.4 Fundamentación jurídica de la propuesta de reforma legal

Para lograr la fundamentación de mi propuesta, creo relevante hacer hincapié, en que los delitos informáticos constituyen una problemática social que va en crecimiento, que no solo se está presentando en la actualidad, sino que va a la par con el desarrollo tecnológico, es por ello que, la creciente incidencia de ciberdelincuencia en Ecuador plantea un desafío significativo para la seguridad nacional y la protección de los ciudadanos en el entorno digital.

El aumento constante en la sofisticación de las tácticas utilizadas por los ciberdelincuentes ha superado la capacidad de las leyes actuales para hacer frente a esta amenaza. En consecuencia, se justifica plenamente la necesidad de revisar y fortalecer el marco legal existente para abordar de manera adecuada los delitos cibernéticos en el país.

Las leyes actuales, diseñadas en una época en la que estas formas de ataques eran menos sofisticadas, no abordan de manera adecuada las tácticas ingeniosas y evolutivas utilizadas por los ciberdelincuentes modernos, por lo cual son indispensables ciertos cambios para abordar mejor este problema.

Por tanto, en la parte de los lineamientos propositivos, incluyo algunas directrices de las cuales ecuador podría implementar, ya sea en la creación de una ley específica o en la adecuación a la ley vigente, por tal, la ley que incluya estas medidas podría ayudar a combatir los delitos informáticos de manera más efectiva y eficiente en el Estado ecuatoriano, tambiénes necesario implementar medidas que abarquen tanto la prevención como la investigación y enjuiciamiento de estos delitos, mejorando la capacidad del sistema judicial.

8. Conclusiones:

Una vez realizada la investigación, puedo llegar a las siguientes conclusiones:

- La investigación ha demostrado que el delito de phishing es una amenaza, caracterizada por engañar a individuos e instituciones mediante el uso de medios electrónicosa fin de obtener información confidencial, representando en sí, una seria vulneración de la seguridad cibernética y de los usuarios en línea. Es necesario abordar esta cuestión desde una perspectiva más allá de la legal, apegado a la tecnología y nuevos mecanismos de protección para garantizar seguridad en el espacio digital.

- En nuestra legislación el delito del Phishing, dado a su complejidad no se encuentra tipificado específicamente, sin embargo, sus características se encuentran dispersas en varios tipos penales del COIP, resultando en cierto punto innecesario el desarrollar un tipo penal específico dentro de la normativa, ya que mediante un proceso de concurso ideal y real de normas se puede dar resolución al problema mediante figuras que comparten los mismos elementos del tipo penal.

- La eficacia de la legislación vigente depende de diversos factores, entre estos el tema de recursos económicos, humanos y desarrollo de políticas públicas enfocados en ciberseguridad y protección de los usuarios son insuficientes para atender las necesidades emergentes.

- Se puede apreciar que en el Ecuador el Phishing ha crecido exponencialmente, mediante varios mecanismos como son los de llamadas telefónicas, correos maliciosos, entre otros, de los cuales, Fiscalía ha recibido denuncias por supuesto phishing bajo el tipo penal apropiación fraudulenta por medios electrónicos, aproximadamente desde 2018 al 2023 se ha receptado 16592 denuncias.
- En el Ecuador no existen instituciones y organismos especializados en el tratamiento de este tipo de situaciones legales, a ello tenemos autoridades que en cierta medida desconocen de la figura penal del Phishing por lo que les resulta difícil acoplar las características de este a tipos penales vigentes que están dentro de nuestra legislación.

9. Recomendaciones

Las recomendaciones que he considerado son:

- Desarrollar dentro del Plan Nacional de Desarrollo de los gobiernos de turno, políticas públicas enfocadas en fortalecer la protección de la información de todas las entidades y usuarios.

- Crear colaboración mediante organismos internacionales y países, a fin de que se pueda establecer una red de comunicación para actualizar y compartir información de mecanismos efectivos para controlar el Phishing y una serie de ciberdelitos.

- Crear una institución específica anexa a una unidad de inteligencia para el trato de este tipo de delitos, mediante la asignación de recursos permanentes y que cumpla una serie de procesos de control y calidad a fin de garantizar que se cumpla con sus debidas funciones.

- Velar que en el desarrollo de las políticas públicas se cumpla el ciclo de la política pública a fin de que esta no sea distorsionada y pueda surtir los efectos esperados sea a corto, mediano o largo plazo que se plantee esta.

- Capacitación de personal a fin de fortalecer conocimiento sobre la forma de accionar de este tipo de delitos y como se puede aplicar la legislación vigente de acuerdo a la modalidad en que este se manifieste.

- Desarrollar cobertura y capacidad con las instituciones a fin de poder llegar a todas las personas que son víctimas en este tipo de delitos sin dejarles en estado de indefensión además de establecer charlas de concientización e información sobre el uso de losmedios electrónicos a la población en general para mitigar los índices del cometimiento de este tipo de delitos.

9.1 Proyecto de Reforma al Código Orgánico Integral Penal

LA REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL

CONSIDERANDO:

Que, el Art. 1, de la Constitución de la República del Ecuador establece que el Ecuador es un Estado constitucional de derechos y justicia social, por lo que de ser necesario se podrá reformar la normativa legal vigente, que responda al cumplimiento de un Estado garantista.

Que, el Art. 66 de la Constitución señala que: "19. El derecho a la protección de datosde carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"

Que la Constitución de la República del Ecuador, de conformidad con el Art. 75, reconoce a las personas el derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediacióny celeridad, y que en ningún caso quedaran en indefensión.

Que, el Art. 76 de la Constitución establece que: "Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley".

Que, en base al Art. 82 de la Norma Constitucional, se señala el derecho a la seguridad jurídica lo cual se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Que, en el ejercicio de sus atribuciones, la Asamblea Nacional, de acuerdo al Art. 84 de la Constitución de la República del Ecuador, tiene la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitucióny respectivamente en los tratados internacionales.

Que, el inciso 1, del Art. 5, del Código Orgánico Integral Penal sobre el principio de legalidad manifiesta: "No hay infracción penal, pena, ni proceso penal sin ley anterior al hecho".

Que, el Código Orgánico Integral Penal, en el Art 13 establece normas de interpretación: 1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando al sentido literal de la norma. 3. Queda prohibida la

utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

En ejercicio de sus atribuciones previstas en el numeral 6 del artículo 120 de la Constitución de la República del Ecuador expide la siguiente:

LEY REFORMATORIA AL CODIGO ORGANICO INTEGRAL PENAL

Art. 1. Agréguese al artículo 190 del Código Orgánico Integral Penal, los numerales siguiente:

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá, si la infracción se comete cuando:

La persona que sin autorización se apodere, utilice, altere, copie o duplique una o varias claves de acceso, contraseñas, firma electrónica o cualquier otro dato o mecanismo de identificación electrónica de otra persona.

La persona que, a través del engaño, cree o use sitios web falsos que imitan a entidades legitimas o envié correos electrónicos, mensajes de datos, llamadas telefónica, solicitando información confidencial, sensible o personal para obtener contraseñas, números de tarjetas de crédito y datos bancarios o personales.

La persona que, con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

DISPOSICIÓN FINAL. – La presente Ley entrara en vigencia a partir de la fecha desu publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los 15 del mes de noviembre del año dos mil veintitrés.

10. Bibliografía

AcurioDel Pino, S. (2016). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf Americas Puebla.

ARCOTEL. (Febrero de 2015). *Espectro Rdioelectrico*. Obtenido de Agencia de Regulación y control de las telecomunicaciones.

Banco Interamericano de Desarrollo. (28 de 11 de 2018). Obtenido de BID: https://blogs.iadb.org/seguridad-ciudadana/es/tecnologia-contra-el-crimen-entusiasmo-con- criterio/

Cabanellas, G. (1993). *Diccionario Juridico Elemental.* HELIASTA S.R.L.

Chile, C. d. (22 de 12 de 2015). Obtenido de Biblioteca del Congreso Nacional de Chile.

Código Orgánico Integral Penal . (2014).

Coldono. (2022). Obtenido de https://dominemoslatecnologia.org/es/formas- violencias/phishing *Conrado*.

Constitución de la Republica del Ecuador. (2008). Quito.

CONVENIO DE BUDAPESt. Universidad de la Rioja.

Díaz, A. (2010). *EL DELITO INFORMÁTICO, SU PROBLEMÁTICA Y LA COOPERACIÓN INTERNACIONAL COMO PARADIGMA DE SU SOLUCIÓN: EL*

Enciso, J. (2021). Obtenido de MICRONET: https://blog.grupomicronet.com/cuales-son-los-origenes-del-phishing

Hugo Bayardo Santacruz, M. M. (2019). Los delitos informáticos y su tipificación en la. *Revista Ibérica de Sistemas e Tecnologias de Información*.

INFORMÁTICOS. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://libros.ecotec.edu.ec/index.php/editoria l/catalog/download/32/29/243-

2?inline=1#:~:text=La%20criminalidad%20inform%C3%A1tica%20tiene%20un,han%20sido%20utilizados%20como%20medio.

Jesús Loredo. (2013). En D. i. combatirlo. Celerinet.

Juan Le Clercq, G. S. (2020). *Indice Global de Impunidad.* Universidad de las

Ley Orgánica de Telecomunicaciones . (2015).

Malwarebytes. (2022). Obtenido de https://es.malwarebytes.com/phishing/

México, S. d. (2012). Obtenido de Gaceta del Senado: https://www.senado.gob.mx/65/gaceta_del_senado/documento/35208

Pérez, A. E. (1998). Internet y el Derecho. Sevilla.

Real Academia de la lengua Española. (2023). Obtenido de https://dle.rae.es/internet?m=form

Revista Seguridad 360. (23 de 12 de 2021). Obtenido de https://revistaseguridad360.com/destacados/tipos-de-delitos-informaticos/

Roberto Baelo, Isabel Cantón. (2009). *Las tecnologías de la información y la comunicación.* Revista Iberoamericana de Educación. Obtenido de https://rieoei.org/historico/deloslectores/3034Baelo.pdf

Rodriguez, V. (2007). *Derecho Informático.* Buenos Aires (Argentina): Aplicación Tributaria S.A.

Saltos Salgado, M. F. (2021). Análisis conceptual del delito informático en Ecuador.

Trejo, C. A. (2019). *LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS*

Zaffaroni, R. (2006). *Manual de Derecho Penal.* Buenos Aires: Ediar.

11. Anexos

Cuestionario Encuestas y Entrevistas.

UNIVERSIDAD NACIONAL DE LOJA
FACULTAD JURÍDICA SOCIAL ADMINISTRATIVA
CARRERA DE DERECHO

ESTUDIO JURÍDICO Y DOCTRINARIO SOBRE EL CIBER DELITO DENOMINADO PHISHING Y LA FALTA DE NORMATIVA LEGAL QUE REGULE LOS DELITOS INFORMATICOS

Por: Andy Javier Iñahuazo López

Estimado(a) Abogado(a): En razón de que al momento me encuentro realizando el desarrollo de mi Trabajo de Integración Curricular, me permito solicitarle a usted de la manera más cordial, dar contestación a la siguiente encuesta, la cual me permitirá recabar información necesaria para mi trabajo y posterior culminación del mismo.

Introducción: Los avances tecnológicos han sido de gran importancia y relevancia para las diferentes formas de vida e interacción de las personas, desde la educación hasta las distintas formas de comercio y comunicación, con ello no solo se a generado beneficios, sino también, que ha surgido una nueva forma de criminalidad la cual al dia de hoy es conocida como cibercriminalidad.

Dando origen así a una serie de delitos informáticos, los cuales han aprovechado el desarrollo tecnológico para usarlo como medio o fin para cometer ilicitos, creando así una nueva problemática social muy compleja y a la vez dificil de combatir, es por tanto la importancia del estudio de este tipo de delitos y del mismo modo su tipificación en las normas jurídicas.

"Si usted piensa que la tecnología puede resolver sus problemas de seguridad, entonces usted no entiende los problemas de seguridad y tampoco entiende la tecnología" (SCHNEIER, 2015)

ENCUESTA

1. ¿Conoce en que consiste el delito informático Phishing?

SI ☐

NO ☐

2. ¿Usted o alguien dentro de su círculo social ha sido víctima de apropiación fraudulenta de su información personal (claves, números de tarjetas de crédito, etc.) mediante engaño a través de correo electrónico, mensajería instantánea, redes sociales o llamadas telefónicas?

SI ☐

NO ☐

3. ¿Considera que la falta de colaboración internacional en el sentido de delitos informáticos afecta la efectividad de la aplicación justicia en Ecuador?

SI ☐

NO ☐

4. ¿Cree usted necesario que el estado ecuatoriano a través de sus diferentes instituciones debería crear campañas masivas a fin de brindar información acerca de delitos informáticos y como prevenirlos?

SI ☐

NO ☐

5. ¿Cree usted que una iniciativa importante por parte del Estado es la de tipificar el delito de phishing?

SI ☐

NO ☐

Cuestionario de Entrevista.

ENTREVISTA

1. ¿Sabe usted de que trata el Phishing?

_____

_____

_____

2. ¿Tienes usted conocimiento, si este delito informático Phishing está tipificado en la ley penal?

_____

_____

_____

3. ¿Considera usted que debe incluirse en el Código Orgánico Integral Penal el delito informático de Phishing?

_____

_____

_____

4. ¿Cree necesario reformar la ley penal en materia de delitos informáticos?

_____

_____

_____

5. Dada la naturaleza transnacional de los delitos informáticos, incluido el phishing, ¿Considera importante la cooperación internacional?

_____

_____

_____

Facultad Jurídica, Social y Administrativa

Carrera de Derecho

CERTIFICADO

Bryan Andrés Moreno Navarrete
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN: MENCIÓN IDIOMA INGLÉS

CERTIFICA:

Haber realizado la traducción del resumen del Proyecto de Titulación denominado: **"Estudio jurídico y doctrinario sobre el ciber delito denominado Phishing y la falta de normativa legal que regule los delitos informáticos"** de autoría del **Sr. Andy Javier Iñahuazo López** de nacionalidad ecuatoriana con cédula de ciudadanía 1150594586. La traducción ha sido entregada al autor para ser fielmente reflejada en la sección denominada "Abstract" de su Trabajo de Titulación.

Es todo en cuanto puedo certificar en honor a la verdad, pudiendo al interesado hacer uso del presente en lo que estime conveniente.

Loja, 2 de Enero del 2024

Firmado electrónicamente por:
BRYAN ANDRES MORENO NAVARRETE

Lic. Bryan Andrés Moreno Navarrete
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN: MENCIÓN IDIOMA INGLÉS
Registro SENESCYT: 1008-2021-2267745 **CI:**
2350659427