UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

"El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación Ecuatoriana: *Phishing*"

Trabajo de Titulación para optar al título de Abogada de los Tribunales y Juzgados de la República del Ecuador

Autores:

Jessica Isabel García Andrade

Gissela Estefanía Pilco Guamán

Tutor:

Dr. Julio Adrián Alvarado Vélez

Riobamba, Ecuador. 2024

DECLARATORIA DE AUTORÍA

Yo, **JESSICA ISABEL GARCÍA ANDRADE**, con cedula de ciudadanía **230048964-4** y **GISSELA ESTEFANÍA PILCO GUAMÁN**, con cédula de ciudadanía **060644789-4,** autor (as) del trabajo de investigación titulado: **DERECHO A LA PROPIEDAD PRIVADA Y NUEVAS MODALIDADES DE DELITOS CIBERNÉTICOS EN LA LEGISLACIÓN ECUATORIANA: PHISHING**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, a los 31 del mes de mayo del 2024.

Jessica Isabel García Andrade
C.I .230048964-4

Gissela Estefanía Pilco Guamán
C.I. 060644789-4

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, **JULIO ADRIÁN ALVARADO VÉLEZ** catedrático adscrito a la Facultad de Ciencias Políticas y Administrativas por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado **"DERECHO A LA PROPIEDAD PRIVADA Y NUEVAS MODALIDADES DE DELITOS CIBERNÉTICOS EN LA LEGISLACIÓN ECUATORIANA: PHISHING"** bajo la autoría de Jessica Isabel García Andrade y Gissela Estefanía Pilco Guamán; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 10 días del mes de abril de 2024.

Dr. Julio Adrián Alvarado Vélez
C.I: 171728267-5

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"EL DERECHO A LA PROPIEDAD PRIVADA Y NUEVAS MODALIDADES DE DELITOS CIBERNÉTICOS EN LA LEGISLACIÓN ECUATORIANA: *PHISHING*"**, presentado por las señoritas **Jessica Isabel García Andrade** con cedula de identidad **230048964-4** y **Gissela Estefanía Pilco Guamán** con cedula de identidad **060644789-4**, bajo la tutoría del Dr. Julio Adrián Alvarado Vélez certificamos que recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba, 28 de junio del 2024

Dr. Freire Sánchez Nelson Francisco

PRESIDENTE DEL TRIBUNAL DE GRADO

Dra. Campuzano Llaguno Rosita Elena

MIEMBRO DEL TRIBUNAL DE GRADO

Dr. Carvajal Flor Bécquer

MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, Jessica Isabel Andrade García con CC: 2300489644 y Gissela Estefanía Pilco Guamán con CC: 0606447894, estudiantes de la Carrera de Derecho, Facultad de **Ciencias Políticas y Administrativas**; han trabajado bajo mi tutoría el trabajo de investigación titulado **"El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación Ecuatoriana: *Phishing*"**, cumple con el **2%**, de acuerdo con el reporte del sistema antiplagio Turnitin porcentaje aceptado de acuerdo con la reglamentación institucional, por consiguiente, autorizo continuar con el proceso.

Riobamba, 21 de mayo del 2024

Dr. Julio Adrián Alvarado Vélez
TUTOR

DEDICATORIA

Dedico el presente trabajo investigativo en primer lugar a Dios y a la Virgencita María, por brindarme salud y permitirme alcanzar este momento tan importante en mi vida. A mis padres María y Rodrigo, a mis hermanos Maykel, Diana por su amor, entrega y sacrificio, por ser los pilares de mi vida, sus sabios consejos que han guiado mi camino académico. A mi enamorado, por su apoyo incondicional y motivación constante. De igual forma, quiero dedicar este logro a mí misma, a mi determinación y perseverancia a pesar de los obstáculos, nunca dejé de creer en mi capacidad para lograr grandes cosas. Esta tesis representa la culminación de años de trabajo y dedicación. A mi perrhija, Lexi, mi fiel compañera en las largas noches de desvelo, por siempre recibirme con alegría después de una larga jornada académica, por aliviar los momentos de estrés con sus travesuras y ladridos llenos de alegría.

Con gratitud,

Jessica Isabel García Andrade

Agradezco a Dios, a la Virgencita de Baños de Agua Santa, al hermanito José Gregorio Hernández y Santo Tomasito que han sido mi roca y mi luz en cada momento. Que su gracia y sabiduría continúen iluminando mi camino mientras avanzo en esta jornada de descubrimiento y aprendizaje. A mi mamá Rosa Guamán, a mi papá Manuel Pilco, a mi hermano Carlos que han sido el motor incondicional en cada momento de mi vida, de igual forma al hermanito Fabian Montenegro y a cada uno de mis tíos y tías que me apoyaron para llegar donde estoy. A mi segunda familia que son mis amigos de Riobamba, pero en especial a Jessica, quien ha sido mi compañera desde el inicio de la carrera y con quien la culminaré. Agradezco a todas las personas que han sido parte de mi vida y me han ayudado a superar los obstáculos con sus consejos y apoyo. En cuanto a mí, quiero dejar constancia de que perseguir los sueños y metas no es fácil, pero con perseverancia y determinación, todo es posible.

Gissela Estefanía Pilco Guamán

AGRADECIMIENTO

Queremos expresar nuestro sincero agradecimiento a la Universidad Nacional de Chimborazo y a todos aquellos que contribuyeron al éxito de esta tesis. Sin su apoyo, orientación y estímulo, no habríamos alcanzado este logro. En primer lugar, extendemos nuestra gratitud al Dr. Julio Adrián Alvarado Vélez, nuestro tutor de tesis, cuya experiencia, paciencia y dedicación fueron fundamentales para dar forma a este trabajo. Su sabiduría académica y valiosos consejos nos inspiraron a superar desafíos y seguir adelante.

También agradecemos a nuestra familia y amigos por su amor incondicional, palabras de ánimo y comprensión durante momentos difíciles.

Reconocemos el invaluable aporte de nuestros profesores a lo largo de nuestra formación académica, quienes nos proporcionaron una educación de calidad y compartieron sus conocimientos, enriqueciendo nuestra investigación, en especial al Dr. Diego Andrade Ulloa, Dr. Hugo Hidalgo y al Dr. Germán Mancheno.

Además, extendemos nuestro agradecimiento a todas las personas que colaboraron en la recopilación de datos, cuya participación fue esencial para obtener información relevante. Por último, a cada uno de ustedes, les agradecemos por dejar una huella indeleble en nuestra vida académica y personal, y por el valioso papel que desempeñaron en este proceso.

¡Gracias a todos!

Jessica García y Gissela Pilco

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación se enfoca en el estudio del derecho a la propiedad privada y el *phishing* como una nueva modalidad de delito cibernético en la legislación ecuatoriana, mediante un análisis de concepciones doctrinarias, disposiciones legales del Ecuador y una comparación con la legislación estadounidense. Se aborda que la normativa ecuatoriana carece de las herramientas necesarias para tipificar estos nuevos delitos que con el mesurado avance de la tecnología se apropian cada vez más del ciberespacio, además, de dificultar la persecución de estas conductas delictivas puesto que no se encuentra contemplado como una figura penal independiente sino más bien, lo adaptan al Artículo 190 del Código Orgánico Integral Penal en la mayoría de los casos. Por ende, el objetivo principal consiste en comprender la problemática del phishing desde una perspectiva global a fin de sugerir una propuesta de reforma que incluya este delito, con el fin de brindar una seguridad jurídica. En la investigación se emplearon diversos métodos, entre los cuales se incluyen el dogmático, deductivo, de comparación jurídica, histórico lógico y exegético. El estudio adopta un enfoque cualitativo con un diseño no experimental. Se utilizaron técnicas como la entrevista y el fichaje, respaldados por instrumentos específicos como la guía de entrevista para recopilar información de los fiscales del cantón de Riobamba, y un fichaje para el análisis del Derecho Comparado. De acuerdo con los resultados obtenidos se concluye que es necesario de una reforma legal para que regule de manera adecuada este delito informático, se destaca la falta de convenios internacionales para combatir el cibercrimen en contraste con la legislación estadounidense, además, de la necesidad de integrar especialistas en ciberdelitos, como peritos y fiscales con amplios conocimientos en el área, para la eficaz guía y obtención de evidencias, abarcando no sólo casos de phishing sino también otros delitos informáticos.

Palabras clave: Derecho a la propiedad privada, *phishing*, delito cibernético, derecho comparado, reforma.

ABSTRACT

This degree work focuses on the study of the right to private property and phishing as a new type of cybercrime in Ecuadorian legislation, through an analysis of doctrinal conceptions, legal provisions of Ecuador and a comparison with U.S. legislation. It is discussed that the Ecuadorian legislation lacks the necessary tools to typify these new crimes that with the measured advance of technology are increasingly taking over cyberspace, in addition to hindering the prosecution of these criminal conducts since it is not contemplated as an independent criminal figure but rather, it is adapted to Article 190 of the Organic Integral Penal Code in most cases. Therefore, the main objective is to understand the problem of phishing from a global perspective in order to suggest a reform proposal that includes this crime, in order to provide legal certainty. Various methods were used in the research, including dogmatic, deductive, legal comparison, historical-logical and exegetical methods. The study adopts a qualitative approach with a non-experimental design. Techniques such as the interview and the file were used, supported by specific instruments such as the interview guide to collect information from the prosecutors of the canton of Riobamba, and a file for the analysis of comparative law. According to the results obtained, it is concluded that a legal reform is necessary to adequately regulate this computer crime, the lack of international conventions to combat cybercrime in contrast to U.S. legislation is highlighted, in addition, the need to integrate specialists in cybercrime, as experts and prosecutors with extensive knowledge in the area, for the effective guidance and collection of evidence, covering not only cases of phishing but also other computer crimes.

Key words: Private property law, phishing, cybercrime, comparative law, reform.

Firmado electrónicamente por:
JHON JAIRO INCA GUERRERO

Reviewed by:
M.Ed. Jhon Inca Guerrero.
ENGLISH PROFESSOR
C.C. 0604136572

CAPÍTULO I

1. INTRODUCCIÓN

El *phishing* es una amenaza global que puede afectar a cualquier persona u organizaciones en el mundo. Sin embargo, algunos países son más vulnerables a los ataques de este ciberdelito debido a ciertos factores como la tecnología, el ordenamiento jurídico y la educación en seguridad informática (Minori, 2023). En los últimos años los ataques de este delito han aumentado significativamente debido al crecimiento en el uso de internet y redes sociales, pero, así como la tecnología evoluciona, los ciberdelincuentes también lo hacen aprovechando las nuevas modalidades y técnicas para el enriquecimiento ilícito, incluyendo estafas y fraudes en línea, lo que ha originado la afectación a los bienes jurídicos protegidos por el Estado, en especial el derecho a la propiedad privada.

La pandemia de COVID-19 y el consecuente confinamiento provocaron que este modus operandi se hiciera aún más notable. Con las restricciones de movilidad, los delincuentes buscaron nuevas formas de obtener recursos económicos ilícitos. Según estadísticas de Interpol en 2020, el *phishing* destacó como la principal ciberamenaza, seguido por el *malware* y *ransomware*. América Latina se vio especialmente afectada por este aumento del cibercrimen durante la pandemia, Brasil encabezó la lista de países más impactados, seguido por Perú, Colombia, Ecuador, Chile y Argentina. El aislamiento y la mayor dependencia de actividades en línea generaron condiciones propicias para que estos ataques proliferaran en la región. |

Por lo que estos delitos cometidos a través de internet representan una amenaza importante para la sociedad, siendo los ciudadanos y empresarios blancos de numerosos ataques mediante correos electrónicos engañosos, mensajes de texto y plataformas de redes sociales. Ahora bien, la persecución de estos cibercrímenes posee una complejidad especialmente en lo que respecta a la obtención de pruebas y la dificultad de identificar y procesar legalmente a los culpables por lo que esta situación representa un desafío relevante para las autoridades judiciales, complicando la aplicación efectiva de sanciones y el cumplimiento de la ley. Por ende, este problema no solo atrae la atención de la esfera legal, sino que también se convierte en un punto de interés académico y científico, a través de este análisis se podrá obtener claridad sobre los elementos que deben incluirse en una legislación

para que la misma tenga un respaldo de sanción que evite que estos ciberdelitos queden en la impunidad.

1.1. PLANTEAMIENTO DEL PROBLEMA

El phishing es una forma delictiva en el ámbito cibernético que busca engañar al usuario con el objetivo de obtener información confidencial y sensible. En la mayoría de los casos, los datos que el atacante pretende conocer, incluyen detalles de la tarjeta de crédito, nombre de usuarios, contraseñas y datos bancarios, entre otros. Estos ataques suelen llevarse a cabo a través de correos electrónicos fraudulentos, mensajes de texto y llamadas telefónicas maliciosas (Hernández et al., 2022).

Desde la década de los noventa, American Online (AOL) fue la primera empresa en experimentar ataques cibernéticos. Esto se debió a que era la principal proveedora de servicios de Internet en el país. En este contexto, los hackers optaron por hacerse pasar por empleados de AOL, utilizando mensajes engañosos en la mensajería instantánea. Su objetivo era persuadir a las víctimas para que proporcionaran sus contraseñas y datos de tarjetas de crédito. En respuesta a esta amenaza, la compañía emitió comunicados de advertencia a los usuarios, destacando las estafas que se estaban desarrollando específicamente en la sala de chat denominada "New Member Lounge" (Rekouche, 2011).

En el caso de España, las decisiones judiciales que eximieron de responsabilidad a ciertos delitos vinculados con el mal uso de tarjetas de crédito en línea provocaron la necesidad de revisar y reformar el Código Penal. Este ajuste legal tenía como objetivo sancionar delitos informáticos, como el phishing, especialmente cuando estos afectan el patrimonio de las personas. De manera paralela, en los Estados Unidos de América, se ha promulgado una ley que establece sanciones, incluyendo multas y penas de prisión, para aquellos que llevan a cabo suplantación de identidad en entornos digitales. Estos cambios reflejan los esfuerzos a nivel internacional por hacer frente a las amenazas en línea y garantizar la integridad de los sistemas financieros y de identificación (Rico, 2013).

En cuanto a América Latina, de acuerdo al último Panorama de Amenazas de Kaspersky manifiesta un incremento en los ataques de phishing, siendo Brasil el país con 134 millones de amenazas por estos ciberdelitos, seguidos por México (43 millones), Perú (31,5 millones), Colombia (30,9 millones), Ecuador (12,2 millones), Chile (10,5 millones) y Argentina (9,4 millones). En base a ello, el experto Fabio Assolini menciona que estos

fraudes informáticos aumentan significativamente con la postpandemia y de herramientas que manejan Inteligencia Artificial (Kaspersky, 2023). Por ello, estos datos estadísticos, demuestran una elevada vulnerabilidad en el entorno digital, además, de que, si no se toman las debidas de protección tanto en ciberseguridad como en el marco legal, estos delitos cobrarán más fuerza a medida que avance la tecnología.

A nivel de nacional, los datos estadísticos provenientes de la Unidad de Ciberdelitos de la Policía dan a conocer que entre el año 2020 y el 6 de julio de 2022, se han contabilizado un total de 3,183 incidentes vinculados con delitos informáticos. Durante el año 2020, se dio un total de 682 casos; ya para el año 2021, las cifras aumentaron rápidamente a 1,851 y en los primeros meses del año 2022, se han puesto en ejecución 650 investigaciones a nivel nacional (El Comercio, 2022).

Por otro lado, la mayoría de los perjudicados por ciberdelincuentes son adultos mayores, puesto que muchos de ellos no manejan demasiado la tecnología y tampoco sospechan de correos falsos, además, de jóvenes o millennials que caen en este tipo de estafas (Notimundo, 2022). Siendo timados en la mayoría de casos por el uso de medios electrónicos, además, de que la pandemia impulsó los consumos virtuales, la instalación de aplicaciones para el uso de dinero tanto en celulares como en computadoras.

En base de ese contexto, se dio el caso de la señora Dora de 75 años, publicado en el diario Universo, el cual consistía, que la señora recibió varias llamadas que le decían que su sobrina que estaba en el aeropuerto de Guayaquil necesitaba cancelar un impuesto por una mercadería proveniente de Estados Unidos, sin duda alguna, la señora transfirió la cantidad de 12.000 dólares de dos cuentas bancarias mencionadas en la llamada. Cuando los familiares supieron del hecho, llamaron a los bancos para que congelen una de las transferencias, posterior a ello, Dora puso la denuncia en la Fiscalía, más tarde, el titular de la cuenta que se transfirió el dinero, se comunicó con el ejecutivo del banco en Quito y le supo manifestar que, si la señora quitaba la denuncia, le devolvía los 9.000 dólares (El Universo, 2021).

Por consiguiente, a lo manifestado existen preguntas que ameritan ser investigadas y respondidas en la presente investigación: ¿Cuál es la problemática del phishing desde una perspectiva global centrándose en el derecho comparado entre Estados Unidos y Ecuador?,

¿Por qué el phishing es considerado como una nueva modalidad de ciberdelito?, ¿Las normas vigentes en la legislación ecuatoriana son suficientes para penalizar de manera efectiva el phishing?, ¿Cuál sería una propuesta de reforma legislativa para incorporar el phishing como un delito cibernético en el COIP?

Por ende, está investigación del phishing reviste de importancia, dado su impacto global y su evolución a lo largo de las décadas. El análisis comparativo entre Estados Unidos y Ecuador permitirá identificar diferencias y similitudes legales que contribuirán a la comprensión de esta problemática en contextos diversos. Además, la revisión de casos específicos y estadísticas locales brindará una perspectiva detallada de la situación en Ecuador, destacando la necesidad de reformas legales. De tal forma, éste estudio es viable, debido a que cuenta con fuentes de información disponibles y la colaboración de entidades judiciales.

1.1.1. Formulación del Problema

¿La legislación ecuatoriana actual es adecuada para sancionar los nuevos delitos cibernéticos, centrándose especialmente en el phishing y su impacto en el derecho a la propiedad privada?

1.2. JUSTIFICACIÓN

El aporte de este proyecto tiene como fundamento, exponer la importancia del phishing en el contexto del derecho a la propiedad privada que se evidencia por la creciente amenaza de delitos cibernéticos debido a la rápida transición hacia lo digital, por lo tanto, la legislación ecuatoriana debe adaptarse y reforzar las protecciones legales para garantizar la integridad de los derechos fundamentales en este nuevo entorno. La evolución de la propiedad privada en la era digital, centrada en datos personales, financieros y comerciales, hace imperativo abordar este delito informático como un desafío que compromete directamente esta forma de propiedad, exponiendo a individuos y entidades públicas o privadas.

Por ello, el interés de este estudio, radica en fortalecer y actualizar los cuerpos normativos en base a las nuevas modalidades de delitos cibernéticos, debido a los vacíos legales que representa este cibercrimen, existe una falta de normativa en la obtención y manejo de pruebas digitales, así como en la especialización y capacitación constante en

autoridades judiciales que son los encargados de la persecución de estos delitos a nivel nacional e internacional. En este sentido, el derecho comparado emerge como el aliado más idóneo para abordar diversas perspectivas legales y culturales al examinar cómo diferentes jurisdicciones enfrentan este problema. Para ello, se ha tomado como referencia la legislación tanto estadounidense como ecuatoriana.

La trascendencia de esta investigación reside en que los casos de presunto phishing en la legislación ecuatoriana son actualmente sancionados con normas generales, dado que no existe una tipificación específica que aborde este ciberdelito. Este vacío legal subraya la necesidad de proponer una reforma que contemple penas proporcionales a la gravedad de los delitos en línea cometidos. Finalmente, se aspira que, en algún momento dado, esta propuesta sea considerada como proyecto de ley por la Asamblea Nacional.

En cuanto a los beneficiarios de este proyecto son todas las personas que utilizan internet o participan en redes sociales, así como a autoridades y profesionales del derecho. Su impacto se centra en proporcionar a estos usuarios y expertos una sólida base de conocimientos sobre el tema tratado, con la intención de que se convierta en un valioso aporte tanto en el ámbito académico como legal.

1.3. OBJETIVOS

1.3.1. Objetivo General

Comprender la problemática del *phishing* desde una perspectiva global centrándose en el derecho comparado entre Estados Unidos y Ecuador para proponer una reforma que incluya este delito en el Código Orgánico Integral Penal.

1.3.2. Objetivos Específicos

- Analizar jurídica y doctrinariamente el contexto del phishing como una nueva modalidad de ciberdelito.
- Identificar si las normas existentes dentro de la legislación ecuatoriana son adecuadas para sancionar el phishing a través de un derecho comparado con Estados Unidos.
- Establecer una propuesta de reforma que incluya el phishing como delito cibernético en el Código Orgánico Integral Penal (COIP).

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ESTADO DEL ARTE

La investigación sobre el phishing y su impacto en el derecho a la propiedad privada ha suscitado un creciente interés tanto a nivel nacional como internacional. A pesar de la existencia de diversos estudios sobre este ciberdelito, su constante evolución subraya la necesidad de un análisis más exhaustivo en el ámbito legal y académico por lo que seguidamente se exponen las conclusiones más relevantes que constituyen fundamentos primordiales para la presente investigación.

La INTERPOL ha manifestado que durante la afectación mundial de la pandemia COVID-19 varios de los delincuentes tomaron como oportunidad esta epidemia para lograr un éxito en sus ataques de phishing, es por ello que esta institución realiza varios estudios acerca del tema, sin embargo, los más significativos para la presente investigación se denominan "COVID-19-Protéjase" y "Ciberdelincuencia: efectos de la COVID-19" que muestran como resultado de sus estudios un alarmante aumento de los ciberataques. En cambio, It Digital Security (2020) lleva a cabo un informe que profundiza en la cuestión al emplear a profesionales de ciberseguridad como muestra para su investigación. Los resultados revelan que alrededor del 30% de estos expertos señala que los ataques de phishing mediante el correo electrónico han tenido éxito durante este período (INTERPOL, 2020).

Por ello, varios estudios señalan la necesidad de tipificar al phishing como una figura penal independiente Masaquiza (2021) y Bisquert (2006). A través de esas investigaciones demuestran que con los avances tecnológicos y la falta de normas específicas que traten este tipo de delito informático genera vacíos legales. La metodología utilizada es un análisis crítico-jurídico y doctrinal, lo cual permitió concluir por una parte la vulnerabilidad que representa la ciberseguridad en países de América Latina, específicamente Ecuador, por otra parte, que se requiere de una reforma legal para que regule concretamente este ciberdelito.

Por otra parte, se puede encontrar la aportación de Aparicio (2021) en sus indagaciones habla de los delitos informáticos en Ecuador, en el cual hace un estudio comparativo en donde menciona que el aumento de los delitos informáticos se debe en gran

parte a los progresos que está causando la tecnología, la falta de conocimiento de los usuarios al utilizar los mismos, y sobre todo, la responsabilidad de implementar medidas necesarias en cuanto a las leyes ecuatorianas, de ese modo, cesar estos ataques tecnológicos.

De igual manera Juca y Medina (2023) realizaron una publicación titulada: "*los Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas*", en este estudio se busca analizar los ciberdelitos y su impacto social, empleando una metodología en base al análisis documental y la exegética, entre los resultados que se destacan, un aumento importante de los delitos en línea en el país, tales como el robo de información personal, ataques a empresas y entidades públicas, fraude en línea, entre otros. Aparte, de que se debe reforzar la seguridad digital, pactar convenios internacionales y que se garantice la viabilidad de los casos en cuanto a estos delitos.

Así pues, Divito (2021) hace referencia en su investigación no solo como surge este tipo de delito sino más bien la afectación que causa a los bienes jurídicos protegidos en el contexto de defraudaciones tecnológicas como el *skimming y phishing*, dando como resultados obtenidos el perjuicio económico que padecen los individuos debido al uso ilegal de sus datos financieros. Estas actividades implican una vulneración directa a la propiedad privada de las personas, por ende, se requiere actualizar la legislación penal para abarcar eficazmente estos delitos y precautelar la integridad de los derechos de las personas y empresas a obtener, poseer y disponer de ellos.

En vista del avance de las modalidades del *phishing* grandes corporaciones tecnológicas, así como diferentes autores han realizado algunas recomendaciones que una persona debe tener en cuenta para no ser blanco fácil, es así, como tenemos a Microsoft (Microsoft, 2021) con su informe y Abroshan, Devos, Poels y Laermans (Abroshan et al., 2021) que realizaron una investigación titulada: "*Phishing happens beyond technology: The effects of human behaviours and demographics on each step of a phishing process*". Concluyendo, que las personas deben tener cuidado con los correos electrónicos o mensajes no solicitados, en los que se solicita información personal, enlaces o archivos adjuntos sospechosos, URL mal escritas y solicitudes de información confidencial. Por lo que, deben verificar la autenticidad de los sitios web y actualizar periódicamente su software de seguridad.

2.2. ASPECTOS TEÓRICOS

2.2.1. UNIDAD 1: EL DERECHO A LA PROPIEDAD PRIVADA

2.2.1.1. Definiciones de los bienes jurídicos

Los bienes jurídicos pueden abarcar elementos tangibles o intangibles, como objetos, relaciones, intereses o derechos, que deben ser considerados socialmente valiosos y, en consecuencia, merecedores de protección jurídica. Esto puede ser llevado a cabo por diversas ramas del derecho e incluso por el ámbito penal (Diccionario panhispánico del español jurídico, 2023).

Otra definición indica que, son aquellos que se distinguen entre el objeto material y el objeto jurídico del delito, puesto que el objeto material u objeto de la acción, en el caso de un robo, es la cosa mueble o inmueble que ha sido arrebatado, en el cual, el bien jurídico es la propiedad. Por ello, estos bienes jurídicos no son suscitados por el derecho, más bien se los reconoce, y a través del reconocimiento es que son bienes de interés vital para la sociedad (Kierszenbaum, 2009).

Por ende, el bien jurídico es aquel interés vital para el desarrollo de los individuos, por ejemplo, en el delito de apropiación fraudulenta por medios electrónicos, la persona viene hacer el objeto material y el bien jurídico afectado es la propiedad, por ello, quien ocasione daños materiales e inmateriales está perjudicando este derecho que está garantizado por el Estado al ser un bien jurídico tutelado. Cabe recalcar, que el derecho subjetivo no es similar al bien jurídico, puesto que el uno hace referencia a la facultad que tiene toda persona de exigir sus derechos, mientras que el otro contiene una realidad valiosa y que debe ser protegido. De igual forma, el autor Salgado (2012) manifiesta que toda norma engloba un bien jurídico, por ello, quien incumple dicha disposición afecta el interés legítimo que ella contiene.

Por otro lado, el bien jurídico representa el objeto o interés que se busca proteger mediante una norma jurídica. Cuando una persona transgrede o desobedece una ley, se produce una lesión o afectación al bien jurídico que dicha norma resguarda. En otras palabras, cada ley o regulación está diseñada para salvaguardar un determinado bien jurídico, y quien infringe esa ley está dañando o vulnerando ese bien que la norma busca tutelar en beneficio del Estado y la sociedad (Salgado, 2012).

En concordancia, un caso hipotético, es en el que Ana, con habilidades informáticas avanzadas, manipula el funcionamiento de las redes electrónicas y del sistema bancario en línea para transferir dinero de la cuenta de Pedro a su propia cuenta sin su consentimiento. Al realizar esta acción, Ana está cometiendo apropiación fraudulenta por medios electrónicos, según lo establecido en el Artículo 190 del COIP. Este acto lesiona el bien jurídico protegido por la norma, que es la integridad de los sistemas electrónicos y la protección contra la apropiación no consentida de bienes. Por ende, una confusión que se puede dar con frecuencia es que se crea que el derecho penal es el creador de los bienes jurídicos, cuando realmente lo que hace es imponer una pena a ciertos tipos penales que dañan ciertos bienes.

2.2.1.2. Tipología de los bienes jurídicos

Bienes muebles e inmuebles

Es de gran importancia partir de la definición y clasificación de los bienes, por ende, los bienes se refieren a cosas corporales e incorporales, al referirse a cosas corporales, son aquellas que pueden ser observadas a través de los sentidos, por ejemplo, una casa, un auto; en cambio, los incorporales se refieren específicamente en derechos, como lo créditos, usufructo o servidumbres. Una vez manifestado lo anterior, las cosas corporales se clasifican en muebles e inmuebles. Los muebles son aquellos que se pueden cambiar de un lugar a otro, sea que se puedan trasladar por sus propios medios o a su vez una fuerza extrema provoque que modifique su posición; al contrario, de los inmuebles, son aquellos que no puedan moverse de un lugar a otro, por ejemplo, las tierras, edificios, árboles entre otros (Código Civil, 2005, Art.583).

Bienes patrimoniales y económicos

Los bienes patrimoniales se refieren a los activos, tanto tangibles como intangibles y estos a su vez pueden ser muebles e inmuebles, activos principales como accesorios. De tal manera, el patrimonio comprende todos los derechos, obligaciones, facultades que tiene una persona en su totalidad, por ello, estos bienes cumplen con un papel importante, debido a que una persona puede utilizarlos de diversas formar, por ejemplo, como una garantía general para los acreedores; como una subrogación real con título universal, es decir, como

el reemplazo de un bien por otro; y también, como facilitador para la transmitir de manera universal y general derechos y obligaciones (Gisca, 2022).

Por otra parte, los bienes económicos se caracterizan por tener un acceso limitado y un valor que requiere consideración para su manejo. Su adquisición está vinculada a técnicas productivas, y desempeñan diversas funciones en términos de administración, distribución y venta en lugares específicos. Estos bienes también cumplen la función esencial de satisfacer necesidades, lo que los convierte en elementos de vital importancia en el mercado. Es importante destacar que estos bienes pueden manifestarse tanto en forma tangible como intangible, siendo transferibles y sujetos a variaciones. Ejemplos de estos bienes incluyen vehículos, ordenadores, viviendas, divisas, criptomonedas y otros dispositivos de uso cotidiano (Lozsan, 2022).

Bienes jurídicos individuales y colectivos

Si bien es cierto, los bienes jurídicos son de diversos tipos, cada uno de ellos con su respectiva concepción, por ello, se distinguen, en bienes jurídicos individuales y los también denominados como supraindividuales, colectivos o universales. A continuación, se tratará de estos dos tipos de bienes, los cuales son de gran relevancia para la comprensión y distinción de los mismos.

"Los bienes jurídicos individuales son de titularidad o sirven a una persona determinada o a un grupo de personas determinadas" (Mayer, 2017, p. 2). Esto quiere decir, que son bienes que tiene carácter personal, como es el bien jurídico de la vida, la propiedad, integridad física, libertad, entre otros, de tal manera, que si existe una afectación a estos bienes va a repercutir en el libre desenvolvimiento de una persona o un grupo de personas en específico.

"Los bienes jurídicos colectivos son de titularidad o sirven a la generalidad de las personas que integran el cuerpo social" (Mayer, 2017, p. 2). Esto se fundamenta, en que estos bienes no son excluyentes para ninguna persona, ni para un grupo de personas en específico sino al contrario para todos, puesto que se refiere a intereses preexistentes, que se encuentran íntegramente para el uso armónico y disfrute de todos. Por ello, si existe una afectación al bien jurídico individual también incidirá en el pleno desarrollo colectivo.

Propiedad privada

Para entender la propiedad privada es necesario conocer algunas definiciones es por ello que si analizamos los antecedentes debemos remontarnos al derecho romano como lo establece Pierre Joseph en su libro "¿Qué es la propiedad?". Así pues, la propiedad se entendía como el derecho de usar y disponer de las cosas, siempre y cuando estuviera respaldado por la razón del derecho. Por lo tanto, probablemente el autor nos quiere indicar que la propiedad es una forma de garantizar que una persona no sea despojada de manera arbitraria de sus bienes jurídicos (Proudhon, 2005).

Asimismo, en la Declaración de los Derechos del Hombre, publicada al frente de la Constitución de 1793, la propiedad es "el derecho que tiene todo hombre de disfrutar y disponer a su voluntad de sus bienes, de sus rentas, del fruto de su trabajo y de su industria" (Proudhon, 2005). Ahora bien, dentro de la legislación ecuatoriana este derecho también se encuentra reconocido dentro de la Constitución de la República del Ecuador en el artículo 66 numeral 26 y en el artículo 321 en el que claramente se establece que "El Estado reconoce y garantiza el derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental" (Constitución de la República del Ecuador [C.R.E.], 2008).

Por consiguiente, la propiedad privada es el derecho que todas las personas, tanto individuos como empresas, tienen para usar, disfrutar y disponer de sus bienes de manera libre, con las limitaciones establecidas claramente por la Constitución y las leyes. En el contexto del constitucionalismo ecuatoriano, este derecho se considera una expresión de libertad. Además, este principio también está reconocido en el Sistema Interamericano de Protección de Derechos. En la Convención Americana de Derechos Humanos, el artículo 21 afirma el derecho a la propiedad privada, indicando que todas las personas tienen el derecho de usar y disfrutar de sus bienes. Sin embargo, este uso puede estar sujeto a las necesidades de la sociedad (Masapanta, 2022).

La privación de la propiedad solo puede ocurrir mediante una compensación justa y bajo circunstancias específicas establecidas por la ley, como razones de utilidad pública. Además, la ley debe prohibir la usura y cualquier forma de explotación del ser humano por parte de otros. En otras palabras, la propiedad privada que una persona llegue a tener no

podrá ser arrebatada de manera injustificada, es decir, que solamente en el caso que exista un interés social se lo podría justificar tomando en consideración que el Estado deberá pagar un valor real por dicho bien, por ende, un caso emblemático que no puede pasar por alto es el de la Corte Interamericana de Derechos en el caso Salvador Chiriboga versus Ecuador. En conclusión, la propiedad privada es un derecho que permite a cada persona gozar, usar y manejar a su antojo los bienes que va adquiriendo a lo largo de su vida sin que otra persona tenga la facultad o el derecho de mencionar que es lo que debería hacer con sus bienes jurídicos.

La privación de la propiedad solo puede tener lugar mediante una compensación justa y bajo circunstancias específicas establecidas por la ley, como en casos de utilidad pública. Es crucial que la legislación prohíba la usura y cualquier forma de explotación humana por parte de otros. En otras palabras, la propiedad privada de un individuo no puede ser arrebatada de manera injustificada. Solo en situaciones donde exista un interés social legítimo, el Estado podría justificar tal intervención, siempre y cuando compense al propietario con un valor real por el bien en cuestión. Un ejemplo paradigmático de este principio se observa en la sentencia de la Corte Interamericana de Derechos en el caso Salvador Chiriboga versus Ecuador. En resumen, la propiedad privada es un derecho que permite a cada persona disfrutar, utilizar y gestionar a su discreción los bienes adquiridos a lo largo de su vida, sin que otros tengan la facultad o el derecho de dictar cómo deben ser manejados.

2.2.1.3. Análisis del derecho a la propiedad privada

La Constitución de la República del Ecuador garantiza los derechos fundamentales de las personas, entre ellos el derecho a la propiedad y el buen vivir. En este sentido, se respaldan las actividades económicas de los individuos, siempre y cuando estas se realicen dentro de los límites legales establecidos y no infrinjan ninguna normativa vigente. Es decir, una persona trabaja con el propósito de adquirir bienes legítimos como una casa, un vehículo, un terreno u otros activos, evitando cualquier actividad ilegal en el proceso.

Es importante destacar que el derecho a la propiedad está no solo consagrado en nuestra Constitución, sino también en el Código Civil ecuatoriano. Este derecho se encuentra regulado específicamente en el segundo libro del código, titulado "De los bienes y de su dominio, posesión, uso, goce y limitaciones". Asimismo, es relevante mencionar que otras

legislaciones, como la canadiense, también contemplan disposiciones similares en sus códigos civiles. En el caso de Canadá, encontramos estas regulaciones dentro del Libro Cuarto denominado "Propiedad". Este reconocimiento legal del derecho a la propiedad resalta su importancia universal y su presencia en diversos sistemas jurídicos en todo el mundo.

Por otro lado, Héctor Santaella Quintero aborda la cuestión de la propiedad privada en su obra "La Propiedad Privada Constitucional: Una teoría". En este contexto, hace referencia a una perspicaz afirmación de Leisner que ilustra de manera elocuente la paradoja inherente a la propiedad: la propiedad se presenta como un derecho particular, ya que la mayoría lo posee y todos anhelan obtenerlo; sin embargo, paradójicamente, su presencia genera controversias en todos los ámbitos (Santaella, 2019).

Por tal razón “la propiedad privada no puede dejar de ser vista como un ámbito positivo de actuación conferida al particular para actuar y determinar libremente su existencia en el ámbito jurídico-patrimonial” (Santaella, 2019, p. 13). Para ilustrar la importancia de lo anteriormente dicho consideremos el ejemplo de un granjero que trabaja en su granja criando animales para consumo propio y para la venta. De esta manera, el granjero puede obtener ingresos. Sin embargo, si un vecino, aprovechándose de su fuerza, decidiera quitarle sus animales y su propiedad, estaríamos cayendo en una situación de ley del más fuerte. Obviamente, si esto ocurriera, las personas perderían el incentivo para progresar, perdiendo la motivación para trabajar y aspirar a un mejor futuro, dado que sus bienes materiales les fueron arrebatados. Por consiguiente, cada individuo busca obtener una recompensa justa y representativa por su trabajo, generalmente en forma de dinero.

Es en este contexto donde se comprende la importancia del derecho a la propiedad privada y la necesidad de un sistema que garantice su protección también se puede palpar que existen diversos tipos de propiedades como lo son los bienes muebles e inmuebles, sin embargo, la afectación que más frecuente se da es el ámbito económico, por ello, es necesario que dentro de los ordenamientos jurídicos se reconozcan las nuevas formas de propiedad para que exista un puente con otras disciplinas, como la economía.

Esta nueva perspectiva permite que el derecho evolucione conforme avanza el tiempo, garantizando el reconocimiento de los derechos patrimoniales tanto en el ámbito real

como en el virtual. En este sentido, el derecho a la propiedad abarca tanto los bienes tangibles como los intangibles que se ven afectados en el tráfico jurídico-económico. El cambio notable en la atención de los agentes económicos hacia la generación, procesamiento y distribución de información y conocimiento, propio de la sociedad postindustrial, es una evidencia clara de esta evolución. Las numerosas oportunidades que emergen y el creciente impacto de sectores como Internet y las nuevas tecnologías en la economía son indicativos de esta transformación (Santaella, 2019).

2.2.2. UNIDAD 2: LOS CIBERDELITOS

2.2.2.1. La tecnología de la información y la comunicación y el ciberespacio

La sociedad siempre va a estar en un constante cambio por ende cada día se van creando nuevas herramientas dentro de la tecnología de la información y de la comunicación, no obstante, es indispensable señalar que, así como existen estos avances también se crea una amplia gama de posibilidades en las cuales son los usuarios de estos programas o redes sociales quienes deben saber utilizarlos. Además de ello, las Tecnologías de la Información y Comunicación (TICs) tuvieron su origen en la década de los noventa, marcada por la creación de la primera computadora llamada Mark I. Aunque en sus inicios se asociaron principalmente con el ámbito computacional, las TICs engloban un conjunto de procesos para el manejo de datos informáticos a través de computadoras conectadas a internet o mediante cables de datos. Su evolución ha estado ligada al desarrollo de las computadoras, la creación de internet y los avances tecnológicos (Masaquiza, 2021).

Dentro de las Tecnologías de la Información y Comunicación (TICs) se puede establecer una clasificación en cuanto a los medios tangibles como una laptop, una Tablet, un celular, una televisión y una radio, es decir son los objetos que se pueden tocar mientras que al momento de hablar de los medios intangibles hacemos referencia a las redes sociales que son sistemas de comunicación que se conectan entre sí, a través de usuarios, *software* y *hardware,* es así entonces como han creado nuevas fuentes de innovación para diversos campos.

Con el auge de las tecnologías digitales, se genera una fácil accesibilidad a todo el público pues esto crea espacios donde personas puedan realizar distintos tipos de actividades dentro y fuera de la ley. Aquellas personas que generan malestar son denominados

ciberdelincuentes, quienes cometen delitos a través del internet, por lo que, en esta nueva era es necesario que se regulen y se penalicen estas conductas que afectan los bienes jurídicos o patrimoniales de los individuos. Dentro de los delitos cibernéticos más comunes se encuentra el *phishing* que es un problema a nivel global que deben enfrentar todos los Estados.

Con el progreso de las Tecnologías de la Información y Comunicación (TIC), diversas potencias, como China, han avanzado en el desarrollo de una disciplina novedosa cuyo propósito es investigar los fenómenos que tienen lugar a través de internet. Es así como ha surgido la disciplina conocida como "*CiberGeografía*", definida por Toudert y Buzai (Toudert & Buzai, 2004), como la especialidad encargada de realizar un análisis que se enfoca en la dimensión espacial de las redes de comunicación informáticas. Esta abarca no solo INTERNET y la *World Wide Web*, sino también otros espacios electrónicos que virtualmente se encuentran entre las pantallas de los ordenadores, siendo comúnmente denominado como Ciberespacio.

La noción del ciberespacio como concepto se originó en la novela de ciencia ficción "Neuromancer" de William Gibson en 1984. En dicha obra, Gibson lo describe como una alucinación consensuada experimentada a diario por innumerables operadores legítimos en todo el mundo, incluyendo niños a los que se les instruye en conceptos matemáticos avanzados. Es presentado como una representación gráfica de información extraída de las bases de datos de todos los ordenadores del sistema humano, manifestando una complejidad inimaginable. Se describe mediante líneas de luz clasificadas en el no-espacio de la mente, formando conglomerados y constelaciones de información, similar a las luces de una ciudad que se aleja (Toudert & Buzai, 2004).

Un concepto más reciente fue propuesto por Jornal Komunikasi (2023), quien define el ciberespacio como el entorno virtual generado por las redes informáticas, facilitando la interacción, comunicación y compartición electrónica de información entre individuos. Este ámbito digital va más allá de las restricciones físicas y posibilita el intercambio de ideas y opiniones. En base a estos conceptos podríamos imaginar a millones de usuarios, desde niños aprendices de matemáticas hasta expertos en diversas disciplinas, participando en una experiencia colectiva.

Este colectivo genera un paisaje digital, donde las líneas de luz representan conexiones de datos entre computadoras, formando constelaciones de información que fluyen y evolucionan en el no espacio de la mente. Por ejemplo, un estudiante en China podría colaborar virtualmente con un investigador en Brasil, ambos contribuyendo a un proyecto global que utiliza datos abstractos de diversas fuentes. Este intercambio de información y pensamiento crea una realidad digital compleja y en constante cambio, similar a las luces de una ciudad lejana que se desvanecen y reaparecen a medida que los participantes aportan sus conocimientos y experiencias al vasto ciberespacio compartido, que se caracteriza por su alcance al traspasar las fronteras de cada país, la asimetría puesto que es global, sencillo y económico, el anonimato que es esencial al momento de ocultar las verdaderas intenciones de una persona , el tiempo y la versatilidad que hace referencia a la capacidad de adaptarse y reutilizar infraestructuras técnicas o herramientas (Instituto Español de Estudios Estratégicos, 2021).

Por lo tanto, la esfera ciberespacial constituye un entorno global compartido que se destaca por su funcionalidad abierta y su constante cambio. Sin embargo, la falta de soberanía, la jurisdicción débil, la facilidad de acceso y la complicada atribución de las actividades que tienen lugar en este espacio definen un escenario lleno de posibilidades para el futuro, aunque también plantea desafíos significativos en términos de seguridad, especialmente en lo que respecta a la proliferación de ciberdelitos.

2.2.2.2. Conceptualización de los ciberdelitos

Un nuevo despertar para la sociedad se ha convertido la era digital en la cual la tecnología ha transformado la forma en que la sociedad vive, trabaja y se comunica. Sin embargo, junto con los beneficios que ofrece este nuevo avance también hemos sido testigos de un aumento significativo de ciberdelitos, por lo que las autoridades y la ciudadanía en general debe prepararse para combatir estos desafíos sustanciales para obtener una seguridad colectiva e individual. Surge, por tanto, la necesidad imperativa de comprender y familiarizarse con las definiciones y conceptos asociados a estos nuevos delitos perpetrados a través de internet, como un paso crucial en la lucha contra esta creciente amenaza.

Así pues, los ciberdelitos constituyen acciones ilícitas perpetradas mediante el uso de computadoras o Internet como instrumentos. Engloban la utilización de tecnología para

llevar a cabo actividades delictivas tales como piratería informática, robo de identidad, estafa, fraude y difusión de malware o virus. Los ciberdelincuentes operan en el ciberespacio, aprovechando las vulnerabilidades presentes en sistemas y redes informáticas con el fin de sustraer información confidencial o interrumpir operaciones digitales, en otras palabras, lo que buscan este tipo de personas es obtener acceso no autorizado a los a los datos informáticos que posee un individuo para conseguir un beneficio que generalmente es pecuniario (Amusan et al., 2023).

Estos actos delictivos representan amenazas significativas tanto para individuos como para organizaciones, e incluso para la seguridad nacional. La detección y prevención de ciberdelitos se convierte en un aspecto crucial para salvaguardar la seguridad y estabilidad económica, especialmente en sectores como la banca, donde las transacciones financieras se realizan en línea. Por otra parte, en el artículo titulado "Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas", se indica que “los ciberdelitos constituyen acciones ilícitas realizadas en el entorno digital con el propósito de obtener beneficios económicos, políticos o personales para los delincuentes” Well (2007, citado en Juca y Medina, 2023, p. 4).

Sin embargo, hay que considerar que el impacto del ciberdelito no se limita únicamente a consecuencias económicas; también acarrea ramificaciones psicológicas y emocionales. Este fenómeno puede ocasionar daños significativos en la integridad de la víctima, especialmente cuando imágenes o videos íntimos se difunden en las redes sociales. Las repercusiones emocionales, como la vergüenza, el miedo y la ansiedad, pueden llevar a la víctima a tomar decisiones lamentables, incluso llegando al extremo de considerar el suicidio.

Un ejemplo de ello es cuando un usuario recibe un correo electrónico aparentemente legítimo de su banco, solicitándole que actualice urgentemente sus datos de cuenta debido a una supuesta brecha de seguridad. El correo electrónico incluye enlaces que llevan a una página web falsa, muy similar a la del banco real. El usuario, preocupado por la seguridad de sus fondos para comprar una casita decide ingresar sus datos personales y bancarios.

A medida que pasa el tiempo, el usuario se da cuenta de que cayó en una estafa de *phishing* y que ha compartido información confidencial con los delincuentes. Experimenta una mezcla de emociones, incluyendo vergüenza, miedo y ansiedad, al darse cuenta del

riesgo de robo de identidad y pérdida de dinero para su casa. Además, el constante temor a las posibles consecuencias negativas en sus cuentas y su seguridad financiera contribuye a un impacto psicológico prolongado. Este ejemplo ilustra cómo el *phishing* no solo tiene repercusiones financieras, sino que también puede generar consecuencias emocionales significativas para la víctima.

Por ende, las tácticas convencionales para detectar ciberdelitos son importantes por lo que a menudo enfrentan desafíos al identificar ataques coordinados y distribuidos, y también pueden generar un alto número de alertas falsas. Para abordar estos desafíos, los investigadores han desarrollado sistemas mejorados que emplean técnicas como la regla de fluctuación modificada (MRDR) y redes neuronales para analizar datos de transacciones e identificar actividades sospechosas puesto que las técnicas más utilizadas para conseguir está información son el *phishing*, el *malware, ransomware*, entre otras.

2.2.2.3. Tipos de ciberdelitos

Los delitos informáticos o ciberdelitos son las acciones delictivas que son llevadas a cabo por uno o varios ciberdelincuentes, cuyo objetivo tienen puesto en los dispositivos electrónicos con libre acceso a celulares, ordenadores, *tablets* y sobre todo redes sociales. A través de estos medios, se aprovechan para tener obtener información, atentar contra la privacidad de datos tanto personales como comerciales (UNIR, 2024).

Por otro lado, es importante señalar que existe una gran variedad de ciberdelitos y estos a su vez no son permanentes sino que a medida como avance la tecnología se desarrollan, el único limitante es la imaginación del sujeto quien realiza el ataque cibernético, su competencia técnica y las vulnerabilidades que presenta los sistemas informáticos (Acurio, 2016). A continuación, se detalla los principales ciberdelitos:

Uno de ellos, son los fraudes informáticos, los mismos que abarcan diversas técnicas, desde la manipulación de datos de entrada hasta el phishing, diseñado para robar la identidad del usuario. Estas prácticas van desde alterar transacciones empresariales de manera sutil hasta falsificar documentos comerciales mediante tecnología avanzada. La complejidad y diversidad de estos delitos reflejan los desafíos que enfrenta la seguridad informática.

Otro de los ciberdelitos, es el sabotaje informático se presenta cuando se manipulan funciones o datos de una computadora sin autorización, lo que interfiere con su

funcionamiento normal. Por otro lado, el espionaje informático y el robo de software, como la fuga de datos, implican la divulgación no autorizada de información confidencial de empresas. En el caso del hurto del tiempo del computador, se trata del uso indebido del tiempo de uso de computadoras, como el acceso no autorizado a servicios de Internet. Además, el acceso no autorizado a servicios informáticos se refiere a la introducción de interrupciones en la lógica de programas para realizar acciones no autorizadas, como la manipulación de resultados intermedios o la creación de salidas de control falsas.

Por otra parte, es importante hacer alusión a los ciberdelitos más comunes en la legislación ecuatoriana, que impactan tanto a empresas como a individuos, incluyen el robo de identidad. Este delito implica el empleo de diversas técnicas por parte de los delincuentes para obtener información confidencial, como contraseñas bancarias, a través de métodos como el *phishing* y el *malware*. Estas prácticas buscan facilitar fraudes mientras los perpetradores mantienen oculta su verdadera identidad.

Otra modalidad en aumento en Ecuador es la sextorsión, que consiste en el chantaje mediante la obtención de imágenes o videos íntimos de la víctima. Asimismo, el ciberacoso, orientado especialmente a niños y adolescentes, implica hostigamiento y amenazas con el objetivo de intimidar. Además, se destacan los ataques informáticos dirigidos a empresas, tanto públicas como privadas. Un ejemplo vívido de esto es el ataque cibernético registrado en la Contraloría General del Estado, que afectó a más de 16,000 cuentas de correo electrónico (Juca & Medina, 2023).

El informe de ESET, empresa líder en la detección proactiva de amenazas, presentado en enero de 2023, destaca las amenazas que impactan la ciberseguridad tanto de empresas como de individuos. Entre estos desafíos, se destacan enemigos implacables como el *ransomware* y el *phishing*, consideradas como las técnicas más utilizadas. Por otro lado, el medio digital "Primicias" informa que el Ecuador es un país que lidera en toda América el mayor número de ataques de *phishing* registrado (Primicias, 2023). Esta información es respaldada por el diario "El Universo", que señala que Ecuador ocupa el tercer lugar en cuanto a la recepción de ataques cibernéticos.

Además, durante el periodo que abarcó desde agosto de 2022 hasta agosto de 2023, se documentaron más de dos millones de ataques cibernéticos en Latinoamérica, según datos

recopilados por la empresa de seguridad cibernética Kaspersky. Estas cifras reflejan un riesgo en aumento para los dispositivos móviles (El Universo, 2023). Ahora bien, dentro de los tipos de prácticas más comunes de los ciberdelitos como se indicó se encuentra el *ransomware* que es un tipo de software malicioso que encripta los archivos del usuario y solicita un pago para restaurarlos mientras que el phishing generalmente se caracteriza por engañar a los usuarios con el fin de obtener información confidencial, como contraseñas o datos bancarios a través de correos electrónicos o páginas webs falsas. Finalmente, las acciones de ataque *DDoS* tienen como objetivo sobrecargar un servidor mediante la generación de numerosas solicitudes, resultando en su colapso y la consiguiente interrupción del servicio.

2.2.2.4. La normativa ecuatoriana y estadounidense sobre delitos cibernéticos

Los delitos informáticos representan uno de los desafíos globales más representativos que enfrentan los Estados en la actualidad. Con el continuo avance de la tecnología, surgen nuevas técnicas y modalidades de ciberdelitos perpetrados a través de internet, los cuales pueden causar daños a los bienes jurídicos de los ciudadanos. Por lo tanto, es crucial que las normativas legales evolucionen para abordar estos problemas y castigar las acciones ilegales de manera proporcional.

En este sentido, Estados Unidos se recalca como un referente en materia de ciberseguridad. Para la presente investigación, analizaremos la normativa estadunidense, en particular la del Estado de California, con el fin de comprender de mejor manera cómo responde ante la creciente demanda de ataques cibernéticos, como el *phishing*, surgidos a raíz de la reciente pandemia de COVID-19 (It Digital Security, 2020). Es por ello que el primer convenio que se debe analizar es el de Budapest.

Entonces el acuerdo fue firmado el 23 de noviembre de 2001 por los Estados miembros del Consejo de Europa y comenzó a estar en vigor a partir del 1 de julio de 2004. Es importante destacar que este tratado no ofrece una definición explícita del término "ciberdelincuencia"; en su lugar, establece los tipos de crímenes cibernéticos que cada país debe o debería tipificar en su legislación. Los delitos informáticos mencionados en el Título II de este marco normativo son particularmente relevantes e impactantes. El Convenio de Budapest tiene como objetivo principal mejorar la efectividad de las investigaciones y procedimientos penales relacionados con delitos que involucran sistemas y datos

informáticos. Esto se logra mediante la búsqueda de pruebas electrónicas de los delitos y promoviendo una cooperación internacional más sólida, rápida y efectiva en asuntos penales (Estuardo, 2021).

A continuación, se acentúan algunas disposiciones relevantes del Convenio de Budapest que son relevantes para los delitos informáticos. El artículo 7 y 8 son ejemplos que se refieren a la falsificación informática, así como al fraude informático que llegan a perjudicar los bienes patrimoniales a través de la introducción, alteración, eliminación o interrupción de datos informáticos con el objetivo de obtener un beneficio económico, ya sea para el perpetrador o para terceros (Consejo de Europa, 2001).

Cabe señalar que los artículos anteriores tomados hacen más referencia a delitos cometidos como el *phishing*. No obstante, existen otros artículos dentro del Convenio que abordan diferentes aspectos de los delitos informáticos. Estos incluyen el acceso ilegal a sistemas informáticos, la interceptación ilícita de datos mediante medios técnicos, ataques a la integridad de los datos y sistemas, así como el abuso de dispositivos. Estas disposiciones complementarias ofrecen un marco integral para abordar diversas formas de delitos cibernéticos y proteger la seguridad de los sistemas y datos informáticos (Consejo de Europa, 2001).

Los países que estuvieron involucrados en las negociaciones del Convenio (los miembros del Consejo de Europa, junto con Canadá, Japón, Sudáfrica y los EE. UU.) tienen la opción de firmar y ratificar el tratado. Según lo establecido en el artículo 37, cualquier otro Estado puede unirse al tratado a través de un proceso de "adhesión", siempre y cuando esté dispuesto a cumplir con las disposiciones del mismo.

En abril de 2023, el Convenio contaba con la participación de 68 Estados como Partes, incluyendo países europeos y otros como Argentina, Australia, Estados Unidos, Filipinas, de igual manera, otros 18 países como Ecuador, Guatemala y Corea habían sido invitados a unirse. Estos 88 Estados participan como miembros (Partes) u observadores (firmantes o invitados) en el Comité del Convenio sobre la Ciberdelincuencia (T-CY) (Council of Europe, 2023).

De igual forma Estados Unidos es parte de la OTAN que está trabajando en la prevención, detección y respuesta a los riesgos asociados al ciberespacio, los Equipos de

Respuesta a Incidentes de Seguridad de la Información (CERTs) operan a nivel técnico, siendo vital mejorar la cooperación y el intercambio de información entre ellos a nivel global, un desafío significativo para la ciberseguridad tanto en organizaciones públicas como privadas. En este contexto, la OTAN, a través de su Equipo de Capacidad de Respuesta de Incidentes Informáticos (NCIRC) y el Equipo de Respuesta ante Incidentes de la Unión Europea (CERT-EU), firmaron un Acuerdo Técnico el 10 de febrero de 2016 para fomentar el intercambio de información y buenas prácticas técnicas. Esta acción se enmarca en las prioridades establecidas por la Política de Defensa Cibernética de la Unión Europea, que busca fortalecer la cooperación con la OTAN en este ámbito (Departamento de Seguridad Nacional, s.f.).

Por otra parte, la Organización de las Naciones Unidas (ONU) también ha incursionado en el estudio de los ciberdelitos a través de su oficina de lucha contra el terrorismo. Esta oficina ha adoptado diversas resoluciones y declaraciones dirigidas a abordar los desafíos de la ciberseguridad y los ciberdelitos. Estos documentos representan una guía y establecen marcos de cooperación internacional para hacer frente a estas amenazas (Organización de las Naciones Unidas [ONU], s.f.).

En el ámbito de las políticas públicas internas adoptadas por Estados Unidos, destacan las medidas impulsadas por la administración del presidente Joe Biden para fortalecer la ciberseguridad y salvaguardar al país de posibles amenazas cibernéticas. Desde que asumió su cargo en enero de 2021, Biden ha demostrado un compromiso firme con la mejora de las infraestructuras tecnológicas del país para hacer frente a los ciberataques que puedan afectar a ciudadanos, empresas y la administración pública. Entre las acciones más notables se encuentra la emisión de una orden ejecutiva en mayo de 2021 para aumentar la inversión en ciberseguridad y modernizar la tecnología disponible. Además, Biden ha mantenido reuniones con líderes de importantes empresas tecnológicas para instarles a elevar los estándares de ciberseguridad.

Como resultado, varias empresas, incluidas *Apple, Google, IBM* y *Microsoft*, se han comprometido a invertir considerablemente en programas de seguridad y formación en ciberseguridad. Asimismo, en octubre, más de 150 empresas de servicios públicos se comprometieron a desarrollar tecnologías de ciberseguridad y a invertir en formación. A nivel internacional, la administración de Biden ha firmado acuerdos cruciales, como el

Acuerdo de París, para fortalecer la cooperación en materia de ciberseguridad a nivel mundial. Además, se están implementando una serie de medidas para mejorar la seguridad de las agencias gubernamentales más sensibles, incluyendo la adopción de sistemas de autenticación de múltiples factores y encriptación aprobada por la Agencia Nacional de Seguridad. Por último, cabe destacar la creciente demanda de profesionales en ciberseguridad y la disponibilidad de programas de formación en línea, como el Máster en Ciberseguridad ofrecido por UNIR, para satisfacer esta necesidad en el mercado laboral (Pascual, 2022).

La Ley de Fraude y Abuso Informático, conocida como CFAA (por sus siglas en inglés), es una ley fundamental que regula la ciberseguridad en los Estados Unidos. Su ámbito de aplicación incluye la protección de computadoras con interés federal, como las gubernamentales, bancarias y aquellas utilizadas en el comercio interestatal y exterior. La CFAA se ha modificado en varias ocasiones desde su creación, reflejando los cambios en la delincuencia cibernética. Originalmente, prohibía acciones como el acceso no autorizado a sistemas informáticos gubernamentales o bancarios, el daño a dichos sistemas, y el fraude informático relacionado. Las enmiendas posteriores ampliaron su alcance para incluir la protección de sistemas financieros, permitieron demandas civiles y abordaron nuevos delitos cibernéticos, como el robo de información personal. Las violaciones de la CFAA pueden resultar en sanciones que van desde penas de prisión hasta multas monetarias significativas, dependiendo de la gravedad del delito. A pesar de sus críticas y desafíos legales, la CFAA sigue siendo un instrumento importante para castigar los delitos cibernéticos y proteger los intereses estadounidenses en línea (Ley de Fraude y Abuso Informático, 1986).

Ahora bien, para ser un poco más específicos con el objeto de estudio de esta investigación se analizó las leyes relacionadas a la sanción del delito cibernético *phishing*, centrándonos en la legislación del Estado de California conocida como Ley *Anti-Phishing*, la cual aborda dos aspectos principales:

El primero es la Ley de robo de identidad de California (Código Penal 530.5 PC) que contempla la posibilidad de procesar a una persona por un delito menor o grave, dependiendo de la naturaleza de su conducta, es decir, si utilizó la información robada para cometer un acto ilegal. En términos de sanción, esta ley prevé una multa o un período de prisión de uno a tres años (Shouse California Law Group, s.f.).

El segundo aspecto es el Fraude con tarjeta de crédito (Código Penal 484e) que implica el uso de correos electrónicos para obtener números de tarjetas de crédito de terceros. Este delito puede resultar en penas de prisión de uno a tres años por un robo mayor, mientras que, si se trata de un hurto menor, la sanción puede ser de hasta seis meses de cárcel y una multa de hasta $1000 (Shouse California Law Group, s.f.).

Por otro lado, Ecuador también participa activamente en la cooperación internacional en materia de ciberseguridad, destacándose su colaboración con otras naciones. En este sentido, el Programa de Ciberseguridad del CICTE sobresale como el principal proveedor regional de asistencia a los Estados miembros de la Organización de los Estados Americanos (OEA) para fortalecer sus capacidades en ciberseguridad, tanto en el ámbito técnico como en el de políticas públicas. Sus acciones y programas están dirigidos a garantizar un ciberespacio abierto, seguro y resiliente en toda la región del hemisferio occidental. También cabe recalcar que uno de los objetivos principales de este programa es optimizar la transferencia de información, promover una colaboración y coordinación sólidas, eficaces y oportunas entre las entidades involucradas en la seguridad cibernética a nivel nacional, regional y global (Organización de los Estados Americanos, 2003).

De igual manera, Ecuador debería pensar en adherirse al convenio de Budapest puesto que tiene la invitación para hacerlo, sin embargo, aún no lo hace. Por otro lado, este acuerdo establece un marco integral y coherente en contra del cibercrimen y la evidencia electrónica (Council of Europe, 2023) por lo que sí es importante para el país unirse para obtener los beneficios como la cooperación internacional con otros Estados con los que podría intercambiar información o agilizar las investigaciones.

En cuanto a los tratados internacionales que se ha ratificado o se ha adherido, destacan el Convenio de Berna sobre los derechos de autor, la Convención para la Protección y Producción de Fonogramas de 1971, el Convenio Internacional de Telecomunicaciones y el Convenio de París. Estos tratados fueron aceptados antes del año 2000, lo que indica la importancia de unirse a nuevos tratados que aborden las cambiantes necesidades de la sociedad (Ortiz, 2019).

En Ecuador, las sanciones por delitos informáticos varían en función de su gravedad y la categorización legal que les corresponda. Dado que el delito del *phishing* no está

específicamente tipificado en el Código Orgánico Integral Penal (COIP), los fiscales y abogados suelen recurrir a encuadrar este delito dentro de los que existen dentro de este cuerpo normativo tomando como referencia el Artículo 186 numeral 2 que hace referencia al fraude mediante el uso de dispositivos electrónicos que "alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares" (Código Orgánico Integral Penal [COIP], 2014).

Además, el artículo 190 aborda la apropiación fraudulenta mediante medios electrónicos, estableciendo una pena de uno a tres años de privación de libertad. De igual manera, el artículo 229 trata sobre la revelación ilegal de bases de datos, con una pena similar de uno a tres años de prisión. En cuanto a la interceptación ilegal de datos, contemplada en el Artículo 230, la pena aumenta a tres a cinco años de prisión. Por otra parte, el artículo 231 aborda la transferencia electrónica de activo patrimonial, con una pena también de tres a cinco años. El Artículo 232 se enfoca en los ataques a la integridad de sistemas informáticos, imponiendo una pena de igual duración, de tres a cinco años. De manera similar, el Artículo 234 se refiere al acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, con la misma pena de tres a cinco años de privación de libertad. Asimismo, el Artículo 234, numeral 1, detalla la falsificación informática, también sancionada con tres a cinco años de cárcel (Código Orgánico Integral Penal [COIP], 2014).

A pesar de existir estos artículos que hacen referencia a los ciberdelitos que están surgiendo en la actualidad se puede palpar que muchos de estos delitos informáticos como el *phishing* no tiene una regulación específica por lo que dependería mucho de la percepción del fiscal para que el delito sea encuadrado en cualquier artículo anteriormente mencionado y se lo pueda perseguir para que el juez imponga una pena.

Por otra parte, la Ley Orgánica de Protección de Datos Personales (LOPD) también es un gran apoyo para contrarrestar los efectos causados a la sociedad por los delitos cometidos a través de internet puesto que esta normativa tiene como objeto y finalidad la protección de los datos personales que se encuentren en cualquier soporte automatizado o no. Por otro lado, también tenemos la Ley de Comercio Electrónico, Firmas y Mensajes de Datos que protege la prestación de servicios en línea a través de redes de información, lo que abarca el comercio electrónico, garantizando la protección de los usuarios de estos sistemas

puesto que en la actualidad muchas de las personas aprovechan el internet para llevar a cabo sus emprendimientos online que generalmente consiste en vender algún producto.

2.2.3. UNIDAD 3: *PHISHING*

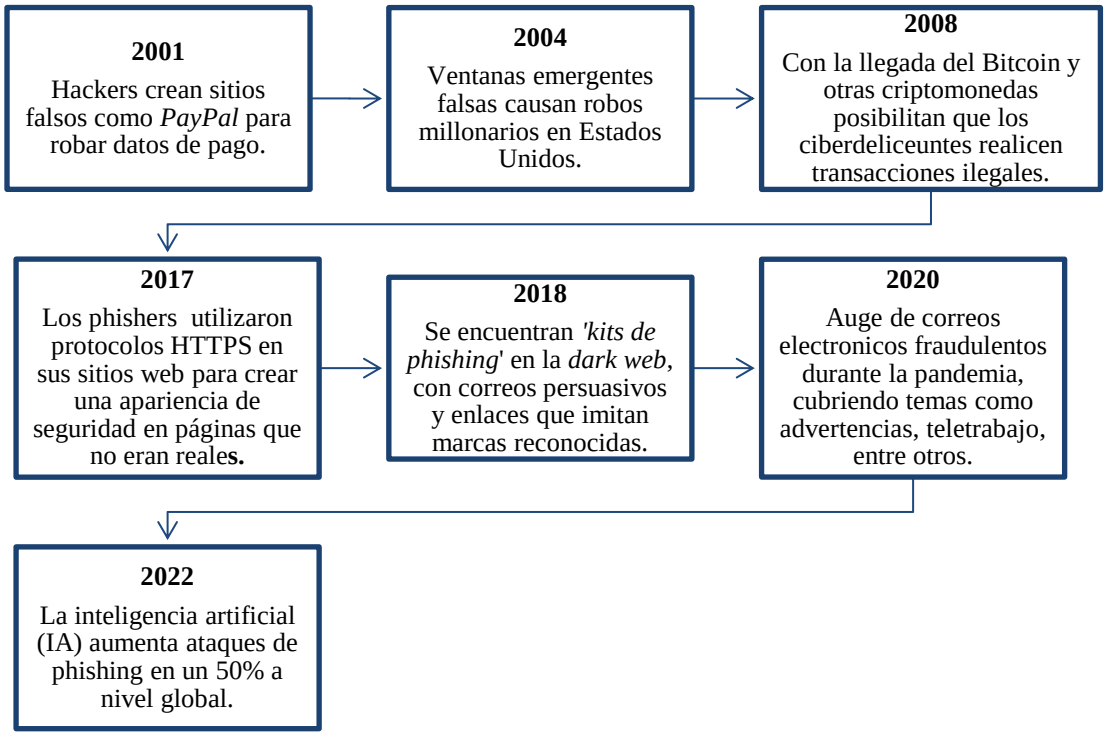
2.2.3.1. Análisis histórico de la evolución del *phishing* como conducta delictiva

El *phishing* ha sido una técnica que se ha transformado con el tiempo hasta llegar a ser una amenaza relevante y continua, empezó a tomar forma a mediados de los años noventa con la aparición de software de piratería el robo masivo de contraseñas e información de tarjetas de crédito en la plataforma *America Online (AOL).* Posterior a ello, la creación de *AOHell,* siendo uno de los primeros programas en este ámbito, el cual dio un hito importante al vincular el término *"phishing"* y generar un mecanismo automatizado para este tipo de fraude desde enero de 1995. Este software sentó las bases para el desarrollo de futuras herramientas automatizadas de forma fraudulenta. Cabe recalcar, que el origen de estas prácticas se empezó en una pequeña comunidad de autodenominados *hackers* en *AOL*, en el cual los individuos como "Da Chronic, un joven de 16 años, y su compañero Dave Lusby, investigaron métodos para engañar a los usuarios haciéndose pasar por empleados del servicio para tener acceso a sus cuentas personales y financieras (Rekouche, 2011).

En base a este contexto, lo que comenzó como una actividad marginal dentro de una comunidad en línea evolucionó hacia una amenaza global, pasando de ser un simple truco de adolescentes rebeldes a una de las mayores preocupaciones de seguridad cibernética, afectando no solo a individuos, organizaciones y gobiernos. De tal manera, que la transición del *phishing* de *AOL* a otros soportes digitales se ha notado la participación de delincuentes profesionales en internet.

Por otra parte, desde el 2020, la incidencia de ataques cibernéticos experimentó un marcado incremento debido a la pandemia del COVID-19. Con las restricciones de movilidad, las personas recurrieron masivamente al uso de internet para sus actividades diarias, lo que, al depender de los servicios en línea, propició que estas conductas delictivas aumenten a gran escala. (Montagner & Merkle, 2022). A continuación, se detalla la evolución que ha tenido el *phishing* a lo largo de la historia.

Figura 1. ***Evolución del Phishing.***



Nota: Evolución del *phishing* adoptado de (González, 2024).

2.2.3.2. ¿En qué consiste el phishing?

El *phishing* es un tipo de ataque cibernético, en el cual los atacantes se dirigen a los usuarios mediante engaños, de esta manera ingresan a su información personal a través de correos electrónicos que a simple vista parecen legítimos y confiables. Por ello, estos ataques tienden a confundir al usuario, puesto que en algunos casos los sitios web presentan una similitud tanto con el interfaz como el URL (Shouq Alnemari & Alshammari, 2023).

De igual forma, la Asociación de Internautas (2007) considera al presunto *phishing* como una suplantación de identidad que se maneja por distinto medios de comunicación tales como son: correo electrónico, los sitios web, llamadas que en la mayoría de los casos provienen de otros países, asimismo, mensajes de texto, con la finalidad de acceder a sus bienes económicos.

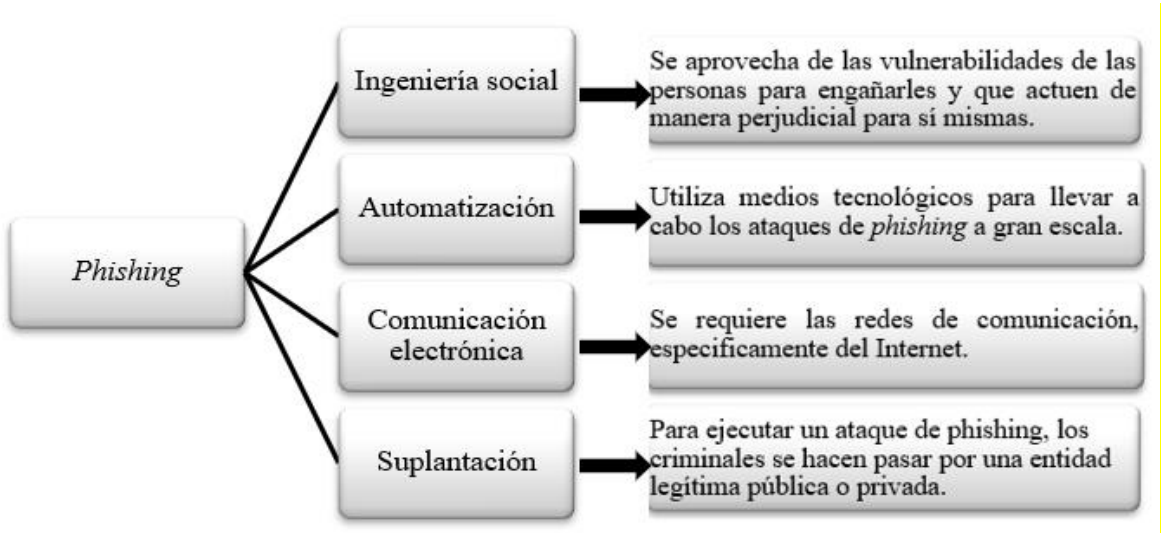
Otra definición, que contiene la idea básica que subyace tras el *phishing*, lo define como un tipo de ataque de ingeniería social puesto que las personas caen en las redes del phishing puesto que obtienen fácilmente los datos del usuario, claves, información

financiera, además, de que el ataque no solo se enfoca en la información confidencial sino en la instalación de malware tanto en dispositivos como en el manejo de los usuarios para ejecutar actividades que favorezca al ciberdelincuente (Lutfor et al., 2023).

Por consiguiente, al hablar de ingeniería social, se refiere que el atacante conocido como *phishers*, tienden a basarse en la psicología humana, para aprovecharse de la información que les puedan arrebatar, dejando vulnerable y sensible al usuario, puesto que ellos manejan correos electrónicos, mensajes, actividades de seguridad al sistema con la finalidad de que la persona acceda y una vez que esté dentro de las redes, tomen el contenido que más les favorezca (Vilela et al., 2022).

Partiendo de estas definiciones y considerando las diversas fuentes involucradas de una u otra forma en el ámbito de los delitos informáticos, es importante señalar lo que diferencia al *phishing* de otros tipos de fraude, en el cual se denotará los cuatros elementos fundamentales.

Figura 2. ***Diferencias del phishing***



Nota: Diferencias del *phishing* adoptado de Instituto Nacional de Tecnologías de la Comunicación [INCO] (2007).

2.2.3.3. Tipología del *phishing*

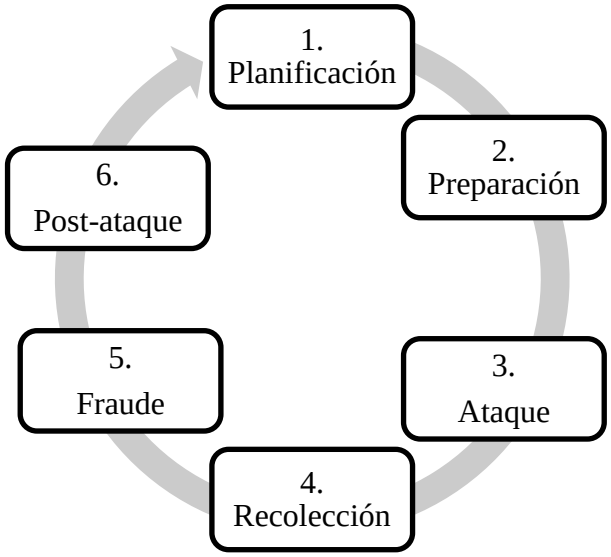
Los tipos de *phishing* han ido aumentando de acuerdo al grado de sofisticación y profundidad, si bien es cierto, no existe una única clasificación de estos delitos, por ello, el Instituto Nacional de Tecnologías de la Comunicación (2007) menciona que uno de los mas conocidos es el *phishing* engañoso conocido como el *Deceptive Phishing*, el cual inició con el objetivo de obtener cuentas de AOL utilizando la mensajería instantánea, empero en la actualidad se da por medio del envío de correos fraudulentos. Además, dentro de este *phishing* se incluye dos modus operandi de estafa: *Vishing y el Smishing.*

Además, el *phishing* que implica el uso de software dañino, o *"Malware-Based Phishing"*, aprovecha programas perjudiciales para comprometer las computadoras de las víctimas, recurriendo frecuentemente a tácticas de ingeniería social. Por otro lado, el phishing basado en manipulaciones del Sistema de Nombres de Dominio, o "*Pharming*", representa un reto importante frente a otros métodos por su capacidad de engañar a las víctimas con una apariencia de legitimidad, minimizando la necesidad de su cooperación activa.

La introducción de contenido fraudulento en páginas web legítimas, conocido como "*Content-Injection Phishing*", constituye otra estrategia, facilitando el redireccionamiento de usuarios hacia sitios maliciosos o la instalación de *software* perjudicial sin su conocimiento. El ataque de intermediario, o *"Man-in-the-Middle Phishing" (MitM),* describe la situación en la que el atacante se interpone discretamente en la comunicación entre un usuario y un servidor *web,* permitiéndole alterar o robar la información transmitida sin ser percibido. Finalmente, el *"Search Engine Phishing"* implica la creación de sitios web o enlaces fraudulentos que se promocionan a través de los motores de búsqueda, con el objetivo de capturar datos personales o financieros de usuarios incautos.

2.2.3.4. Fases del *phishing*

Figura 3. ***Fases del phishing.***



Nota: Fases del *phishing* adoptado de Instituto Nacional de Tecnologías de la Comunicación [INCO] (2007).

La figura 3 ha permitido identificar las seis fases clave para llevar a cabo un ataque de phishing. Al analizar la primera fase, el *phisher* realiza una investigación exhaustiva sobre el usuario, ya sea un individuo o una organización. De esta manera, recopilan información personal y detalles relevantes necesarios para ejecutar el ataque de manera efectiva. Referente a la segunda fase, una vez recopilado la información, el atacante procede a realizar correos electrónicos, mensajes de voz y de texto, llamadas telefónicas, interfaces y URL que guarden similitud y sobre todo se vean legítimos, de esa forma, se crea los mensajes de *phishing* dando como resultado que la víctima se vea vulnerable y accesible. Como tercera fase, los mensajes anteriormente mencionados son enviados por diferentes canales, masificando enlaces falsos, y que la gran parte de la población que es dependiente del internet, sea víctima de este ataque cibernético. En relación a la cuarta fase, es cuestión de esperar que el código instalado consiga los datos de forma fraudulenta. En la quinta fase, los delincuentes proceden a la estafa ya sea de forma directa o vendiendo esa información a otros estafadores. Finalmente, la sexta fase, el delincuente elimina todo rastro que haya quedado.

2.2.3.5. Naturaleza jurídica del *phishing*

El phishing se considera un tipo de delito cibernético en el ámbito del fraude en Internet, y se ha determinado su marco legal y regulatorio, por ello, la regulación internacional y la lucha contra la ciberdelincuencia, incluido el phishing, se lleva a cabo a través de medidas legales, técnicas y procesales, y la cooperación internacional. De tal manera, que la naturaleza jurídica va a depender de las diferentes regulaciones que le da cada estado, por ejemplo, en los Estados Unidos, este tipo de ataque generalmente se procesa bajo las leyes existentes relacionadas con el fraude, el robo de identidad y los delitos informáticos. Por ello, la cooperación y colaboraciones internacionales también son importantes en la lucha contra el phishing, ya que organizaciones como el Grupo de Trabajo Anti-Phishing (APWG) trabajan para crear conciencia y coordinar esfuerzos.

Asimismo, la Ley CAN-SPAM de 2003 en los Estados Unidos aborda específicamente las prácticas engañosas de correo electrónico, incluido el *phishing*. En la Unión Europea, el Reglamento General de Protección de Datos (GDPR) proporciona un marco legal para proteger los datos personales e imponer sanciones por violaciones de datos, que pueden incluir ataques. Otros países pueden tener su propia legislación y regulaciones para abordar el *phishing*, como la Ley de uso indebido de computadoras y ciberseguridad en Singapur (Mohd et al., 2007).

Sin embargo, en el Ecuador este tipo ciberdelitos no se encuentra tipificado en la norma, es decir, en el Código Orgánico Integral Penal (COIP), más bien, se refieren de forma general, específicamente en el artículo 190 de la norma anteriormente mencionada, que habla sobre la apropiación fraudulenta por medios electrónicos, si bien, indica que la persona que manipule tanto bienes, programas, sistemas informáticos sin el consentimiento de la persona será sancionado con una pena privativa de libertad de 1 a tres años. De tal manera, que no tipifica los diferentes tipos de estafas en línea, y a su vez las sanciones que deben tener aquellas personas que se basan de ese medio para apropiarse de bienes ajenos.

2.2.3.6. Casos de *Phishing*

Estados Unidos

El 26 de enero de 2004, la Comisión Federal de Comercio (FTC) de Estados Unidos, inició su primer proceso legal por un presunto *phisher*. El caso de un joven de California acusado de crear una página web falso que imitaba al de la compañía América Online para robar información de tarjetas de crédito. Continuando el ejemplo estadounidense, tanto Europa como Brasil comenzaron acciones contra individuos sospechosos de *phishing*. Mas tarde, en marzo de 2005, una persona proveniente de estonio fue detenido por utilizar una puerta trasera en su sitio web fraudulento que contenía un *keylogger*, es decir, un software malicioso para espiar lo que redactaban los usuarios. Asimismo, las autoridades arrestaron a Valdir Paulo de Almeida, cabecilla de una gran red de phishing responsable del robo de 18 a 37 millones de dólares en aproximadamente en dos años. En junio de 2005, el Reino Unido arrestó a dos personas en coordinación con la *Operation Firewall* del Servicio Secreto de EE.UU, que señalaba a sitios conocidos por practicar el phishing (Salazar, 2007).

A partir de los casos que han surgido a causa del presunto phishing, el senador estadounidense Patrick Leahy propuso la Ley Anti-Phishing 2005 el 1 de marzo del mismo año, estableciendo sanciones severas, una de ellas, son las multas de hasta $250.000 y penas de prisión de hasta cinco años, para los creadores de sitios web fraudulentos y los que remitan correos electrónicos engañosos. Cabe recalcar, que Microsoft se sumó a la lucha contra el *phishing*, dando a conocer 117 demandas federales presentadas ante la Corte del Distrito de Washington el 31 de marzo de 2005. Estas demandas, en contra de *phishers* no identificadas, tenían como objetivo destruir redes de phishing importantes. También, Microsoft trabajo en conjunto con el Gobierno Australiano en marzo de 2005 para promover la legislación y educación que ayuden a combatir los delitos cibernéticos, en especial, el *phishing* (Salazar, 2007).

Ecuador

Siendo el caso, el 8 de octubre del 2020 en la Unidad Pedro Vicente Maldonado al noroccidente de Quito, el fiscal Hugo Pérez abrió una instrucción fiscal por presunto "phishing", como infractores se obtuvo a seis personas procesadas (casi todos de la misma familia) a los cuales se los conoce como alías mamá, papá, neutrón, chino, topo y taz, los

mismos que utilizaban números de tarjetas y códigos robados en Estados Unidos y Europa para poder adquirir cuentas de *streaming* y mercadería en línea. A través de estas actividades, generaron beneficios económicos de $80.000 y lograron adquirir tres vehículos para su organización dedicada a la ciberdelincuencia. Cabe señalar que el fiscal que llevó el caso lo adecuó en base al artículo 190 del COIP puesto que es el artículo que más se asemejaba a este delito informático (Fiscalía General del Estado, 2020).

Perú

Otros de los casos de *phishing*, se dio en la ciudad de Chiclayo perteneciente a la Costa Norte del Perú, el mismo que consta en la Resolución Final N°1961-2022/CC1. El 23 de septiembre de 2021, a las 10:30 horas, la Sra. Ramos fue engañada mediante un correo de "SERPOST" que le pedía abonar S/5.90 para modificar la dirección de entrega de un envío. Al seguir el enlace proporcionado, ingresó sus datos personales y un código de validación recibido vía SMS, cayendo así en una trampa de phishing. Una hora después, a las 11:30, su banco la contactó para informarle sobre el bloqueo temporal de su tarjeta debido a la detección de cuatro transacciones anómalas, realizadas en la mañana, por montos que sumaban miles de dólares. La Sra. Ramos, al no reconocer dichas operaciones, contactó inmediatamente al banco para negar su autorización y bloquear su tarjeta. No obstante, el banco solo revocó las dos últimas operaciones, manteniendo las primeras dos como legítimas. Después de intentar sin éxito resolver el asunto por las vías administrativas, la Sra. Ramos denunció al banco ante Indecopi el 14 de diciembre de 2021, alegando una violación a su derecho de seguridad en el consumo, especificado en los artículos 18° y 19° de la Ley N°29571, Código de Protección y Defensa del Consumidor. Refutó que el banco no implementó adecuadas medidas de seguridad, permitiendo así que se efectuaran operaciones fraudulentas con su tarjeta de crédito (Torres, 2023).

El caso se analizó bajo la evidencia de capturas de pantalla que mostraban la introducción manual de la información confidencial de la tarjeta y los detalles de las transacciones sospechosas. A pesar de que el banco identificó estas operaciones como distintas a las habituales del cliente y tenía medios para alertar de tales anomalías, la decisión final sobre la denuncia dependía de si se consideraba que el banco había fallado en adoptar las necesarias medidas de seguridad. Se debatía si declarar la denuncia como infundada, lo que significaría aceptar que el banco actuó correctamente, o como fundada, reconociendo

que el banco no cumplió adecuadamente con sus obligaciones de seguridad hacia el consumidor, lo que al final se declaró como infundada la denuncia. En este caso se denotó la importancia de la seguridad en línea, la responsabilidad de las instituciones financieras en la protección de los datos y transacciones de los clientes, y la aplicación adecuada de las normativas de protección al consumidor para garantizar la integridad y seguridad de las operaciones financieras.

2.2.3.7. Bien jurídico afectado en el *phishing*

El phishing al ser un tipo de estafa informática se ve afectado por algunos bienes jurídicos, uno de ellos, es el bien jurídico a la propiedad privada, si bien es cierto, es un derecho que tiene todo ser humano de usar, disfrutar y manejar sus bienes tanto materiales como inmateriales de acuerdo a sus necesidades. No obstante, las personas que acceden a los medios telemáticos e internet, se ven expuestos a diferentes ataques cibernéticos, en el cual, los atacantes se aprovechan de la información que exponen los usuarios ya sea en la página de una empresa, en sitios web, correos electrónicos, entre otros. De esa forma, obtienen el contenido para proceder a cometer el delito en línea, sin el consentimiento de la misma.

Por ello, al configurarse este delito ya se está afectando a los bienes jurídicos tanto individuales como colectivos, al decir, individuales se refiere al derecho de propiedad privada, es decir, el daño que ha sufrido ese usuario sobre sus bienes económicos ocasionando de manera inmediata a otro bien jurídico de tipo de naturaleza colectiva, en el cual se ve perjudicado el ordenado funcionamiento de los sistemas informáticos, dicha afectación no solo hay una lesión de un bien de naturaleza individual sino también colectivo.

Por otro lado, en todo delito informático interviene tanto el sujeto activo como el sujeto pasivo, en ese sentido, la persona que lesione el bien jurídico se considera el sujeto activo y el titular del bien jurídico viene hacer el sujeto pasivo, por ello es importante diferenciar estas dos concepciones puesto que la mayoría de estos delitos no son descubiertos ni denunciados a las autoridades correspondientes. Por ende, para el autor Acurio (2016) manifiesta que las personas que inciden en delitos informáticos tiene competencias avanzadas en cuanto al desarrollo de tecnologías de la información. Reiteradamente, estas personas mantienen puestos laborales que les permite acceder a información delicada. Sin

embargo, aunque estas personas no se encuentren dichos lugares de trabajo, adquieren gran facilidad para el manejo de sistemas informatizados.

De tal manera, que para los sujetos activos se les facilita cometer este tipo de delito cibernético debido a las aptitudes que presentan estos atacantes al manejar los sistemas informáticos, con el objetivo de obtener la información confidencial al sujeto pasivo mediante engaños. Al hablar de sujeto pasivo del delito informático, alude a las víctimas que por el desconocimiento del modus operandi de los sujetos activos, ingresando a correos electrónicos que a simple vista parecen legales, pero no lo son. En la mayoría de los casos, las victimas que han sido estafadas por medio de correos electrónicos, mensajes, enlaces, entre otros, no realizan la respectiva denuncia, por consiguiente, los casos aumentan y estos delitos quedan en la impunidad (Acurio, 2016, p. 19).

CAPÍTULO III

3. METODOLOGÍA

3.1. Técnicas e instrumentos de investigación

Se empleó la entrevista como técnica de investigación, la cual se llevó a cabo mediante el uso de instrumento denominado guía de entrevista, con la finalidad de recoger conocimientos en base a la experiencia de los Fiscales Especializados de Patrimonio del cantón Riobamba, además de ello, la información obtenida fue procesada a través del programa Atlas.ti. para establecer un estudio de tendencias y un análisis de categoría por código que permitió tener una idea clara acerca del ciberdelito phishing y su procedimiento. También, se implementó el fichaje como técnica, utilizando el correspondiente instrumento para realizar el Derecho Comparado entre la legislación ecuatoriana y estadounidense.

3.2. Unidad de análisis

La investigación sobre: "El derecho a la propiedad privada y las nuevas modalidades de delitos cibernéticos en la legislación Ecuatoriana: *Phishing*", se desarrolló en la provincia de Chimborazo, cantón Riobamba, en el cual se analizó la problemática del *phishing* desde una perspectiva global centrándose en el derecho comparado entre Estados Unidos y Ecuador.

3.3. Métodos

Para el estudio de la problemática se utilizaron los siguientes métodos de investigación:

Método Dogmático: Rojas (2019) menciona que el método dogmático en el estudio del derecho se basa en analizar el ordenamiento jurídico para entender y de esa manera transmitir ese conocimiento, aplicar, perfeccionar y mejorarlo. En concordancia con la idea previa, con este método en la presente investigación se logró analizar normas, doctrinas, jurisprudencias, facilitando de esa manera la correcta comprensión de este nuevo delito cibernético denominado *phishing*.

Método deductivo: Ponce (s.f.) indica que el método deductivo se centra en la aplicación de principios o conocimientos generales para obtener conclusiones especificas dentro de un campo de estudio. Por ende, se empleó el método deductivo, comenzando con

conceptos generales que engloben normas y doctrinas proporcionadas por las ciencias pertinentes. Este enfoque permitió alcanzar conclusiones que contribuyan al progreso de la investigación.

Método de comparación jurídica: Herrera (2021) destaca la comparación jurídica como una herramienta que facilita la adquisición de conocimientos al considerar diferentes sistemas legales, lo cual permite una mejor compresión del propio marco legal mediante la comparación con otros. En base a lo manifestado, este método permitió analizar las similitudes y disparidades inherentes al objeto de la investigación en los distintos sistemas jurídicos, por medio de un análisis comparativo entre el ordenamiento jurídico ecuatoriano y la normativa estadounidense.

Método histórico-lógico: Torres (2020) este método se enfoca en analizar la evolución concreta de los fenómenos y eventos a lo largo de la historia, mientras que el método lógico se enfatiza en investigar los principios generales que rigen el funcionamiento y el desarrollo de dichos fenómenos. En base a ese concepto, en la investigación se estudió la transcendencia histórica de los delitos informáticos, específicamente del *phishing* y los problemas jurídicos que eso ha contraído al ordenamiento jurídico ecuatoriano.

Método exegético: De acuerdo a Martínez (2023) este método funciona como un componente de la interpretación del Derecho, comprendiendo a esta disciplina como una ciencia que, por su naturaleza, incorpora un aspecto interpretativo relacionado con la explicación y la implementación de las normas. En virtud de lo expuesto, en la investigación se analizó el artículo 190 del Código Orgánico General de Procesos ecuatoriano debido a que en la mayoría de los casos se asocia el presunto *phishing* a ese artículo puesto que no está regulado, existiendo un problema jurídico de interpretación normativa.

3.4. Enfoque de investigación

La investigación por sus características, objetivos, objeto y su desarrollo en las Ciencias Sociales es de enfoque cualitativo.

3.5. Tipo de investigación

Para el desarrollo del presente proyecto de investigación y alcanzar sus fines, se aplicaron los siguientes tipos de investigación:

Investigación documental: Con respecto a este tipo de investigación Rodríguez y

Gonzáles (2019) esta investigación aborda la información obtenida o examinada de documentos y otros materiales impresos que son adecuados para ser evaluados, procesados y entendidos. De esa manera, se realizó por medio de material legal y bibliográfico existente para el estudio.

Investigación jurídica descriptiva: Para Aldaz (2023) esta investigación implica descomponer el tema en tantas partes como sea posible. Esto se refiere que el tema debe ser, salvo que se persiga otro fin, muy bien delimitado. Por ello, con la aplicación de este tipo de investigación se pudo delimitar las cualidades y características de la problemática, las cuales se obtuvieron mediante un análisis y recopilación de información, de tal modo, fue transcendental para alcanzar los objetivos del estudio.

3.6. Diseño de investigación

La investigación se inicia con un análisis jurídico y doctrinario exhaustivo del phishing como modalidad delictiva en el ámbito cibernético. Esta etapa implica revisar la legislación vigente, la jurisprudencia relevante y los tratados internacionales pertinentes relacionados con el delito de phishing tanto en Estados Unidos como en Ecuador. Se examinan definiciones legales, tipos penales, sanciones y otros aspectos relevantes para comprender el marco legal existente y su efectividad en la prevención y persecución de este tipo de delitos.

Posteriormente, se procede a realizar entrevistas a profesionales del derecho, específicamente a miembros de la fiscalía expertos en el campo legal relacionado con la ciberseguridad y los delitos informáticos. Estas entrevistas proporcionan una visión práctica y empírica sobre cómo se aborda el phishing en el sistema legal ecuatoriano, identificando posibles desafíos, brechas o áreas de mejora en la aplicación de la ley.

Luego, se lleva a cabo un estudio de derecho comparado entre Estados Unidos y Ecuador. Esta fase implica analizar las similitudes y diferencias entre los enfoques legales de ambos países en cuanto al tratamiento del phishing, examinando no solo la legislación, sino también la jurisprudencia, las políticas gubernamentales y las prácticas judiciales en la persecución de estos delitos. Se busca identificar modelos exitosos, mejores prácticas y lecciones aprendidas que puedan ser aplicables al contexto legal ecuatoriano.

Con base en los hallazgos del análisis jurídico, las entrevistas y el estudio de derecho comparado, se procede a formular una propuesta de reforma al artículo 190 del Código Orgánico Integral Penal (COIP) de Ecuador. Esta propuesta tiene como objetivo abordar las deficiencias identificadas en la legislación actual y fortalecer el marco legal para combatir el phishing de manera más efectiva. Se consideran aspectos como la definición del delito, las sanciones, los mecanismos de investigación y la cooperación internacional, entre otros.

3.7. Población y muestra

3.7.1. Población

La población para el presente trabajo investigativo fueron los fiscales provinciales Especializados de Patrimonio Ciudadano, del cantón Riobamba, provincia de Chimborazo, de los cuales se realizó un muestreo no probabilístico por conveniencia.

3.7.2. Muestra

Es de tipo intencional no probabilística, bajo los siguientes criterios de inclusión:

- Fiscales Especializados de Patrimonio del cantón Riobamba que aceptaron el consentimiento informado.

3.8. Técnicas para el tratamiento de información

En cuanto al tratamiento de la información, se llevó a cabo mediante el uso de un programa llamado Atlas.ti. Este proceso implicó inicialmente la transcripción de las entrevistas grabadas, con el fin de transformar el contenido oral en texto escrito. Una vez completada esta etapa, se procedió a analizar los resultados obtenidos a través de este instrumento. Para facilitar la comprensión y el análisis de los datos, se llevó a cabo una codificación por pregunta, lo que permitió organizar la información de manera estructurada y detallada. Esta técnica de codificación por pregunta ayudó a identificar patrones, tendencias y temas relevantes presentes en las respuestas de los entrevistados, contribuyendo así a una comprensión más profunda y significativa de los resultados obtenidos. Por lo tanto, el proceso de tratamiento de información se llevó a cabo de la siguiente manera:

En primer lugar, se llevó a cabo la transcripción de las entrevistas grabadas, por lo que esta transcripción implicó escuchar detenidamente cada grabación y escribir el contenido de manera textual. Es importante asegurar la precisión y fidelidad en la transcripción para

garantizar que la información recolectada se refleje de manera exacta en el texto escrito. Como segundo punto se organizó los datos transcritos de manera sistemática lo que involucró la estructuración de las transcripciones de acuerdo con la secuencia de preguntas realizadas durante la entrevista y los distintos temas abordados.

En tercer lugar, se dio el análisis de los resultados, esto implicó revisar detalladamente cada transcripción para identificar patrones, tendencias y temas recurrentes en las respuestas de los entrevistados. Después, se llevó a cabo una codificación por pregunta asignando etiquetas o códigos a cada respuesta según la pregunta a la que corresponde. Por ejemplo, si una pregunta trata sobre los desafíos del phishing, todas las respuestas relacionadas con este tema serían codificadas bajo una misma etiqueta.

Como quinto lugar, se organizó la información codificada en una base de datos o en un software de análisis cualitativo. Esto permitió tener acceso rápido y estructurado a los datos, facilitando su interpretación y análisis posterior. Finalmente, se procedió a interpretar los resultados obtenidos a partir del análisis de los datos codificados permitiendo identificar conclusiones, tendencias y hallazgos significativos que surgieron a partir de las respuestas de los entrevistados.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Resultados

4.1.1. Análisis jurídico y doctrinario del *phishing* como modalidad de delito cibernético.

El *phishing* es un tipo de ataque cibernético que implica engañar a los usuarios para obtener información confidencial como contraseñas, datos bancarios, etc. a través de correos electrónicos, sitios web falsos y otras tácticas de ingeniería social. Aunque este delito no está tipificado de manera específica en la legislación ecuatoriana, se lo puede encuadrar bajo disposiciones más generales sobre fraudes y delitos informáticos en el Código Orgánico Integral Penal (COIP).

Doctrinariamente, el *phishing* se considera un delito dentro del ámbito del fraude en internet. Su naturaleza jurídica varía según las regulaciones de cada país, pero generalmente se procesa bajo leyes relacionadas con fraude, robo de identidad y delitos informáticos. A nivel internacional, el Convenio de Budapest del Consejo de Europa sienta un marco normativo vinculante, aunque Ecuador no es parte de este. Por otro lado, el bien jurídico principal que se ve afectado en el *phishing* es el derecho a la propiedad privada, ya que los atacantes obtienen acceso no autorizado a bienes económicos de las víctimas. Asimismo, afecta bienes jurídicos colectivos como la integridad y el funcionamiento ordenado de los sistemas informáticos.

Las penas implementadas en Ecuador varían de 1 a 5 años de prisión dependiendo de cómo se encuadre el delito del phishing para que sea sancionado, mientras que en Estados Unidos puede ser sancionado con penas incluso más severas bajo leyes específicas contra el *phishing* como el *Computer Fraud and Abuse Act*. Si bien Ecuador cuenta con la Ley de Protección de Datos Personales, se requiere un mayor desarrollo normativo enfocado específicamente en delitos como el *phishing*. De tal manera, se podrían tomar como referencia marcos legales más desarrollados como los de Estados Unidos. Además, se necesitan mayores esfuerzos de cooperación internacional, jurisdicción extraterritorial, prevención y educación pública en torno al phishing para un abordaje integral de este delito emergente.

4.1.1.1. Análisis de entrevistas

Entrevistado 1. Dr. Diego Lenin Andrade Ulloa

Entrevistado 2. Dra. María Esther Caguano Velastegui

El *phishing* se define técnicamente como un delito patrimonial que implica un engaño o acción fraudulenta a través de sistemas informáticos, con el objetivo de obtener información confidencial como claves de acceso, tarjetas de crédito, etc. para apropiarse indebidamente de dinero. Las características distintivas son el apoderamiento del patrimonio de la víctima por medios fraudulentos en un entorno electrónico, como la manipulación de cajeros automáticos o la implantación de virus para captar claves de acceso.

Para la recopilación de pruebas digitales en casos de phishing, es fundamental realizar un reconocimiento del lugar, una pericia informática para determinar los accesos y esquemas de cronología, así como asegurar los mecanismos probatorios dada la fragilidad y posible manipulación de los indicios. Un desafío es rastrear la autoría cuando se utilizan direcciones IP o servidores en el extranjero, lo que dificulta la investigación por límites de jurisdicción.

La cooperación internacional se ve dificultada por la lentitud y falta de colaboración de algunas autoridades internacionales, siendo INTERPOL una vía más fluida. A nivel legal, se aplican principalmente los tipos penales de apropiación fraudulenta por medios electrónicos, suplantación de identidad y estafa, contemplados en el Código Orgánico Integral Penal para sancionar el *phishing* debido a que no existe una normativa específica que sancione este ciberdelito.

Las principales falencias identificadas son la insuficiente capacitación y recursos técnicos de los operadores de justicia, así como la falta de concientización y programas de prevención a nivel público y empresarial. Se propone considerar una tipificación específica del phishing que contemple sus particularidades, junto con el fortalecimiento de la cooperación internacional y el desarrollo de pruebas digitales más robustas.

Categoría de análisis

Normativa

Se destaca el Artículo 190 del Código Orgánico Integral Penal (COIP), que abarca la apropiación fraudulenta por medios electrónicos. Se mencionan diversas formas de abordar este delito, como la estafa, el acceso no autorizado a sistemas informáticos y la suplantación de identidad. Se resalta la importancia de la Ley de Protección de Datos como un marco fundamental para abordar casos de phishing y otras formas de delitos cibernéticos. Además, se señala la necesidad de establecer regulaciones y precisiones técnicas para abordar adecuadamente estos casos, considerando la transferencia no consentida de bienes, valores o derechos como perjuicio patrimonial. El análisis legal aborda la concurrencia de varios tipos penales en casos de phishing, destacando la amplitud del Artículo 190 del COIP y su aplicabilidad a situaciones específicas de acceso no autorizado y apropiación indebida. Se destaca la penalización del acceso no permitido a sistemas informáticos y la manipulación de redes electrónicas.

En cuanto a la legislación general, se mencionan otras normativas como la Constitución y la Ley de Protección de Datos que respaldan la persecución de estos delitos. Sin embargo, se reconoce que la legislación ecuatoriana aún está en desarrollo y presenta limitaciones en términos de aplicación y cooperación internacional en casos de phishing y hackeos. En resumen, la entrevista destaca la necesidad de fortalecer la legislación y las medidas técnicas para abordar de manera efectiva los delitos cibernéticos, con especial atención al phishing, en el contexto legal ecuatoriano.

Vacíos Legales

Se ilustra un caso donde la apropiación de información se trató como estafa debido a la falta de una categoría específica para abordar situaciones de acceso no autorizado a datos con intenciones fraudulentas. Se destaca la dificultad para encajar el phishing dentro del marco legal existente, ya que el tipo penal de apropiación fraudulenta por medios electrónicos, contemplado en el artículo 190, resulta amplio y no tiene una circunstancia específica para el phishing. La entrevista resalta que el acceso no permitido ya debería considerarse como tipo penal, subrayando la necesidad de definiciones más específicas en la legislación para abordar este tipo de delitos cibernéticos.

Se presenta una crítica sobre la amplitud de los tipos penales existentes, destacando la complejidad para la acusación y defensa. Además, se compara el acceso no consentido con el delito de apropiación fraudulenta por medios electrónicos, señalando la similitud y la posible confusión entre ambos. Se menciona un ejemplo de manipulación del sistema informático para desviar fondos, evidenciando que los tipos penales pueden ser concurrentes en el ámbito de los delitos informáticos, generando complejidades en su aplicación y en la delimitación de responsabilidades. En resumen, la entrevista resalta la necesidad de revisar y mejorar la legislación ecuatoriana para abordar de manera más efectiva los delitos cibernéticos, especialmente el phishing, y destaca los desafíos asociados a la falta de claridad y especificidad en las normativas existentes.

Análisis de casos

En el análisis de casos presentados, se destacó la variedad de métodos utilizados, como la manipulación de sistemas para implantar virus y la apropiación de registros mediante engaños, más allá del phishing convencional. Un caso particular involucró la estafa a una persona con acceso a transacciones internacionales, donde los delincuentes, ubicados en China, lograron realizar un desembolso significativo al manipular la información de la víctima. Se mencionaron casos de apropiaciones ilícitas a través de cajeros automáticos y lectores de tarjetas de crédito, subrayando la diversidad de enfoques empleados por los infractores. Se enfatizó la importancia de la protección de datos, incluyendo la identificación biométrica, como un aspecto crítico en la prevención de delitos cibernéticos.

Por otro lado, se resaltó la responsabilidad individual en la seguridad, comparando la exposición en línea con situaciones físicas vulnerables. Se argumentó que la conciencia y la autoprotección son fundamentales, ya que la seguridad no es exclusiva del Estado. Se sugirió que la ciudadanía debe comprender la necesidad de resguardar sus datos y adoptar medidas de seguridad, como antivirus y precauciones con aplicaciones desconocidas.

En términos legales, se abordó el delito de apropiación fraudulenta por medios electrónicos, específicamente el artículo 190, que contempla perjuicios al patrimonio a través de transferencias no consentidas de bienes, valores o derechos. Se destacó la necesidad de comprender las características técnicas y legales para abordar eficazmente estos delitos, y se ilustró la complejidad mediante la comparación con otros tipos penales concurrentes.

Finalmente, se mencionó la posible disparidad en la capacidad de investigar delitos cibernéticos entre diferentes regiones, señalando que, en lugares con más recursos informáticos, como Quito, podría haber una mayor eficacia en las investigaciones.

Reforma de ley

Se propone analizar si el tipo penal actual es el más adecuado y, en caso contrario, buscar medios para fortalecer la sanción de este delito y brindar una mayor protección a la sociedad. Se plantea la inquietud sobre si el acceso no autorizado debería considerarse como un tipo penal por sí mismo, ya que el phishing implica no solo el acceso sin autorización, sino también la apropiación indebida de bienes patrimoniales. Se sugiere la posibilidad de introducir circunstancias agravantes o considerar la gravedad de la afectación al patrimonio en la determinación de las penas, especialmente cuando se trata de delitos como el phishing.

Además, se aboga por la inclusión del phishing como un tipo penal independiente en la legislación, en lugar de depender de figuras penales generales. La propuesta es verificar las particularidades y la incidencia específica del phishing en cada área, brindando así una tipificación clara y estableciendo penas adecuadas para este delito. En resumen, la entrevista aboga por una reforma legal que considere la singularidad del phishing como delito cibernético, proponiendo medidas específicas y penas ajustadas para abordar eficazmente esta problemática en la legislación ecuatoriana.

Conocimiento

Se exploró las nuevas modalidades de delitos cibernéticos, centrándose en el phishing y su impacto en el derecho a la propiedad privada en la legislación ecuatoriana. Se destacó que el phishing constituye un delito patrimonial que se lleva a cabo mediante engaños y acciones fraudulentas, afectando tanto a personas naturales como jurídicas. Se explicó que este tipo de fraude electrónico se realiza a través de sistemas informáticos, implicando la violación de contraseñas, tarjetas de crédito y otra información confidencial mediante el acceso a claves.

Se subrayó que el phishing se manifiesta a menudo a través de correos electrónicos disfrazados, buscando obtener acceso a sistemas informáticos y cuentas para apoderarse de información valiosa. Se resaltó el propósito fundamental de los perpetradores detrás de estas acciones, que consiste en obtener claves de teléfonos para acceder a cuentas y malversar

fondos. El objetivo principal del phishing es la apropiación de bienes ajenos, incluyendo prácticas como chantajes, destacando la relevancia del aspecto patrimonial en estos delitos cibernéticos. En resumen, la entrevista proporcionó una visión clara de cómo el phishing se materializa como un delito patrimonial que busca apoderarse de información valiosa y afectar directamente al patrimonio de las personas, tanto a nivel individual como organizacional.

Desafíos legales

Se destacó la complejidad para determinar la ubicación exacta en casos de ataques cibernéticos, especialmente cuando los perpetradores utilizan direcciones IP enmascaradas o servidores ubicados fuera del país. La limitación en el rastreo de estas direcciones IP debido a cuestiones de tiempo y al derecho internacional fue señalada como un desafío importante. En cuanto a los parámetros de prueba, se resaltó la necesidad de contar con especialistas en delitos informáticos y fiscales con conocimientos avanzados en esta área. La importancia de asegurar mecanismos probatorios con estándares más elevados, dado que ciertos indicios pueden desaparecer o ser manipulados, fue enfatizada.

La entrevista destacó la demora como un desafío crítico en la Fiscalía, especialmente en la coordinación de asuntos internacionales en Quito, afectando los tiempos de respuesta. La falta de recursos especializados, como peritos informáticos, fue mencionada como un obstáculo en la realización de pericias técnicas informáticas esenciales para determinar la apropiación fraudulenta de sistemas informáticos.

En términos de cooperación internacional, se evidenció la dificultad para obtener asistencia penal en casos de países como China, donde la falta de convenios y la aparente falta de interés crean obstáculos significativos. Se resaltó que la falta de convenios y la escasa buena voluntad en la cooperación internacional presentan un desafío adicional para la Fiscalía. En resumen, la entrevista revela que los desafíos legales relacionados con el tiempo, recursos especializados, cooperación internacional y desarrollo normativo representan barreras significativas para la efectiva persecución de delitos cibernéticos en Ecuador.

Recopilación de pruebas

Se enfatiza la necesidad de realizar diligencias básicas, como el reconocimiento del lugar del delito, para determinar la competencia del juez y fiscal. Se resalta la relevancia de la pericia informática en casos de phishing, ya que este delito implica la sustracción de claves en lugar de una modificación o acceso no autorizado al sistema. Se subraya la falta de un estándar definido y se aboga por contar con especialistas en delitos informáticos, peritos informáticos y fiscales con conocimientos sólidos en esta área. Además, se menciona la dificultad relacionada con la limitación de peritos informáticos, lo cual puede afectar la investigación, especialmente en zonas geográficas extensas.

Se destaca la importancia de preservar la evidencia desde el inicio, incluyendo la información de IP, correos maliciosos y capturas de pantalla. Se subraya la necesidad de informar a los técnicos de sistemas para recuperar la información esencial. Se enfatiza la importancia de las pericias informáticas de alto nivel para determinar la procedencia de los correos y la identificación del posible manipulador, incluso si se encuentra en otro país. En resumen, la entrevista resalta la complejidad de recopilar pruebas en casos de phishing y destaca la necesidad de contar con profesionales especializados y tecnologías avanzadas para abordar de manera efectiva estos delitos cibernéticos en la legislación ecuatoriana.

Cooperación Internacional

Se destacó que la Fiscalía maneja la cooperación internacional a través de una coordinación de asuntos internacionales en Quito, pero se evidenció que los tiempos de respuesta son excesivamente largos, lo cual se presenta como un desafío significativo en la persecución eficaz de delitos cibernéticos. Se subrayó la disparidad en las respuestas de los gobiernos en función de la cooperación internacional, indicando que algunos colaboran de manera más efectiva que otros. La entrevista resaltó la importancia de la cooperación con INTERPOL, permitiendo una conexión más fluida tanto en América como en Europa.

El proceso de asistencia penal internacional fue abordado como esencial para realizar solicitudes que, aunque podrían tratarse internamente, requieren un nivel de cooperación internacional. Se mencionó un caso específico en China, donde la falta de interés por parte del gobierno chino, debido a la percepción de que la cantidad involucrada (80,000 dólares) era insuficiente, ilustra los desafíos en la cooperación internacional.

A pesar de contar con convenios con algunos países, como Colombia, para viabilizar la cooperación, se destacó la lentitud en la obtención de información, especialmente en casos que implican la extradición de personas. Además, se señaló la falta de desarrollo en las leyes ecuatorianas con respecto a la aplicación del phishing y la escasa cooperación internacional en relación con estos ataques cibernéticos. En resumen, la entrevista evidencia la complejidad y los desafíos que enfrenta Ecuador en términos de cooperación internacional para abordar los delitos cibernéticos, resaltando la necesidad de mejorar los tiempos de respuesta y fortalecer el marco legal en este ámbito.

Educación y prevención

El enfoque se centra en la exposición personal y la necesidad de autoprotección, subrayando que la seguridad no solo depende de medidas tecnológicas, sino también del conocimiento y comportamiento individuales. Se plantea la posibilidad de establecer nuevos tipos penales relacionados con delitos cibernéticos, como el phishing, asimilados a la apropiación fraudulenta. Se enfatiza la importancia de adaptar estas medidas al derecho comparado y a los estándares locales para garantizar la seguridad jurídica.

La entrevista revela desafíos en la institucionalización del conocimiento en instituciones públicas, donde la educación se limita a advertir sobre correos sospechosos. Esto destaca la necesidad de invertir en programas educativos y especializaciones. En resumen, es urgente mejorar la educación y conciencia pública sobre delitos cibernéticos en Ecuador, adaptando el marco legal y promoviendo acciones proactivas en la esfera educativa y legal para abordar eficazmente estos desafíos.

4.1.2. Identificar si las normas existentes dentro de la legislación ecuatoriana son adecuadas para sancionar el phishing a través de un derecho comparado con Estados Unidos.

Se pudo determinar que las normas existentes dentro de la legislación ecuatoriana no son completamente adecuadas al momento de sancionar el ciberdelito del phishing. Esto se debe a varios factores que son la falta de tipificación específica del delito de phishing puesto que no se encuentra tipificado de manera expresa en el Código Orgánico Integral Penal (COIP) de Ecuador. Esto genera que los abogados y fiscales deban adecuar estos casos bajo disposiciones más generales relacionadas con el fraude y los delitos informáticos.

Otro aspecto crucial se relaciona con la falta de claridad en las penas contempladas por la legislación ecuatoriana al abordar el phishing. La magnitud de la sanción, que oscila entre 1 y 5 años de prisión, depende de la figura legal en la cual se encuadre el delito, según lo establecido en el Código Orgánico Integral Penal (COIP). En virtud de esta situación, los artículos más frecuentemente invocados son el 190 (apropiación fraudulenta), el 229 (revelación ilegal de bases de datos), el 232 (ataques a la integridad de sistemas), entre otros.

Esta falta de precisión normativa genera una complejidad en la imposición de sanciones que sean adecuadas y proporcionales. La variabilidad en la interpretación al vincular el delito con distintos artículos legislativos dificulta la aplicación de medidas punitivas justas. En este contexto, se evidencia la necesidad imperante de una revisión legislativa que asegure una definición más clara y coherente en la sanción del phishing dentro del marco legal ecuatoriano.

En cuanto a la Ley Orgánica de Protección de Datos Personales al revisarla se pudo palpar que es insuficiente porque no aborda de manera específica delitos como el phishing, que precisamente vulneran la privacidad y seguridad de los datos personales. Del mismo modo la cooperación internacional para perseguir este ciberdelito es limitada por lo que dificulta la persecución extraterritorial de esta conducta delictiva haciendo que existan casos impunes.

4.1.2.1. Derecho Comparado

Tabla 1. *Derecho Comparado entre Ecuador y Estados Unidos.*

Criterio	**Ecuador**	**Estados Unidos**
Definición de *Phishing*	El Código Orgánico Integral Penal (COIP) de Ecuador no tiene una definición específica para el *phishing*, pero puede abordarse bajo disposiciones generales de los siguientes artículos: 168,190,212,230,231,232 y 234.	En Estados Unidos, el *Computer Fraud and Abuse Act* (CFAA) define el acceso no autorizado a sistemas informáticos, abarcando así el *phishing*. Además, se aplican estatutos federales y estatales adicionales, como la Ley de *Phishing* de California, que considera el phishing como la acción de engañar a un usuario a través de correos electrónicos, sitios web, robo de identidad, fraude con tarjetas de crédito por medio del internet para obtener información confidencial.
Penas para *Phishing*	En Ecuador, las sanciones por delitos informáticos varían en función de su gravedad y la categorización legal que les corresponda. Dado que el delito del *phishing* no está específicamente tipificado en el Código Orgánico Integral Penal (COIP), los fiscales y abogados suelen recurrir a encuadrar este delito dentro de los que existen dentro de este cuerpo normativo tomando como referencia el Artículo	En los Estados Unidos, las penas por *phishing* pueden ser relevantes bajo el CFAA, con multas y penas de prisión proporcionales a la gravedad del delito y los daños causados. Por ende, en primer lugar, tenemos la Ley de Phishing de California que divide en dos segmentos: 1.- Ley de robo de identidad de California (Código Penal 530.5 PC) que puede procesar a una persona por un delito menor o grave en el cual depende del comportamiento especifico, es decir, si utilizó la información para cometer un acto ilícito. En cuanto a la pena, se sancionará con una multa o será encarcelado por un año, 16 meses o dos o tres años.

	186 numeral 2 que se refiere al defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. Por otro lado, el articulo 190 el cual estipula una pena privativa de libertad de uno a tres años. Asimismo, tenemos el Artículo 229 que trata sobre la revelación ilegal de bases de datos, estableciendo una pena similar de uno a tres años de privación de libertad. En el caso de la interceptación ilegal de datos, contemplada en el Artículo 230, la pena aumenta a tres a cinco años de prisión. Por otra parte, el Artículo 231 aborda la transferencia electrónica de activo patrimonial, con una pena también de tres a cinco años. El Artículo 232 se enfoca en los ataques a la	Como segundo de subtema de la Ley se trata: 2.- Fraude con tarjeta de crédito (Código Penal 484e) consiste en el uso de correos electrónicos para recopilar números de tarjetas de crédito de otras personas, siendo este sancionado por un año, 16 meses o dos o tres años, por un gran robo. Si es un hurto menor será castigado con seis meses de cárcel del condado y con una multa de hasta $1000.

	integridad de sistemas informáticos, imponiendo una pena de igual duración, de tres a cinco años. De manera similar, el Artículo 234 se refiere al acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, con la misma pena de tres a cinco años de privación de libertad. Asimismo, el Artículo 234.1 detalla la falsificación informática, también sancionada con tres a cinco años de cárcel.	

Protección de Datos	Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales (LOPD), Ley de Comercio Electrónico, Firmas y Mensajes de Datos y el Código Orgánico Integral Penal (COIP), que regula el manejo de la información personal en internet, pero no aborda específicamente el phishing.	Estados Unidos tiene varias leyes estatales y federales que abordan la protección de datos, como la Ley de Privacidad del Consumidor en Línea de California (CCPA), la Ley de Protección de la Privacidad en las Comunicaciones Electrónicas (ECPA), la Ley de *phishing* de california y la Ley federal de *phishing*.
Cooperación Internacional	Ecuador coopera con otras naciones en asuntos de ciberseguridad, como son: -Programa Ciberseguridad del Comité Interamericano contra el Terrorismo, de la Organización de los Estados Americanos (CICTE/OEA). -Proyecto de Resiliencia Cibernética para el Desarrollo, de la Unión Europa (CYBER4DEV), sin embargo, estos pueden mejorar la cooperación específica en	Estados Unidos tiene acuerdos internacionales de cooperación en ciberseguridad y participa en iniciativas globales para combatir el cibercrimen, como: - Convenio de Budapest sobre la Ciberdelincuencia Estados unidos. - Políticas Cibernéticas de la Organización del Tratado del Atlántico Norte (OTAN). - Acuerdo de París (19 de febrero 2021) - ONU (Oficina de Lucha contra el Terrorismo) Políticas internas de Estados Unidos:

	casos de *phishing* (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).	- Estados Unidos el primero en crear políticas de ciberseguridad a nivel nacional, iniciando el primer Equipo de Respuesta a Emergencias Cibernéticas (CERT) en la Universidad Carnegie Mellon (Shackelford & Craig, 2014).
Jurisdicción Extraterritorial	La legislación ecuatoriana puede tener dificultades para perseguir a perpetradores fuera de su jurisdicción, puesto que en el artículo 14 numeral 2 del COIP, menciona que para que una persona sea juzgada fuera del territorio, se debe basar en algunos casos: uno de ellos que tenga efectos en Ecuador o en sitios sometidos a su jurisdicción; por otro lado, si la infracción es cometida en el extranjero hacia una o más personas ecuatorianas y no han sido juzgados en el país de origen donde se cometió; y, cuando se afecte a bienes jurídicos protegidos por el Derecho Internacional y no se haya juzgado en otra jurisdicción, entre otras (Código Orgánico Integral Penal, 2014). Sin embargo, la persecución de delitos informáticos se lo puede hacer por medio de la	Estados Unidos tiene una mayor posibilidad de que estos delitos cibernéticos sean perseguidos extraterritorialmente debido a los convenios y tratados internacionales de los que forma parte. Uno de ellos, es el Convenio de Budapest que hasta junio del 2022 poseía 66 Estados parte que brindan los mecanismos necesarios para que estos ciberdelitos sean sancionados.

	INTERPOL y en el caso, que no se trabaje con esta institución, Fiscalía impulsa a través de escritos con el objetivo de que haya una pronta respuesta favorable de la jurisdicción extranjera.	
Prevención y Educación	En el año 2016, en vista de la falta de conciencia en la sociedad y el aumento significativo de los ataques cibernéticos, la Unidad de Investigación del Cibercrimen de la Dirección Nacional de la Policía Judicial e Investigaciones de delitos informáticos en conjunto con la INTERPOL, incentivan al cambio de información con el sector privado y a la ejecución de una capacitación en pruebas digitales, tanto para la policía, detectives y los tribunales judiciales. Además, la Secretaria de Inteligencia propone solucionar con una campaña denominada "Promoción de una cultura de inteligencia" (Observatorio de Ciberseguridad, 2016). Por otro lado, se llevó a cabo un Acuerdo Ministerial No. 006-2021, emitido en el	Estados Unidos tiene esfuerzos relevantes en la educación pública sobre ciberseguridad y phishing con campañas y recursos disponibles para informar al público, es por ello, que tenemos los siguientes nombres de campañas: - "No muerdas el anzuelo creado" (Internal Revenue Service, 2017) ; - NIST *Cybersecurity Program History and Timeline* (National Institute of Standards and Technolog, 2023) ; - *FBI's Internet Crime Complaint Center* (IC3) desde el 2000 ha realizado campañas, por otra parte, la más reciente fue la *"Top Cyber Actions for Securing Water Systems"* (Federal Bureau of Investigation, 2021); y, - US-CERT *(United States Computer Emergency Readiness Team),* que se encuentra de manera permanente realizando contenido para la prevención de la ciberseguridad (Homeland Security, 2003). Cabe señalar, que Estados Unidos posee un derecho anglosajón por lo que cada Estado crea sus políticas públicas internas siguiendo los lineamientos de la gran Constitución Federal para enfrentar estos informáticos.

	Registro Oficial el 23 de junio de 2021, en el cual se publicó la Política Nacional de Ciberseguridad, con la finalidad de garantizar la protección de los bienes jurídicos del Estado en un ciberespacio seguro (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). En el período de Guillermo Lasso, se dieron a conocer los distintos planes específicos desde 2019-2030 que consistían en: Seguridad Pública y Ciudadana; de Relaciones Exteriores y Movilidad Humana; de Defensa; y, de Defensa Institucional 2017-2021. A pesar de las campañas y estrategias utilizadas para contrarrestar los ataques cibernéticos, incluido el phishing, es necesario mejorar en estos aspectos y poner en práctica la normativa vigente y a su vez ampliar en el ámbito de ciberseguridad.	

Marco Legal Global	Ecuador podría beneficiarse de una mayor alineación con estándares internacionales en materia de ciberseguridad y delitos informáticos, al momento de adherirse a tratados y convenios internacionales.	Estados Unidos sigue siendo un líder en la formulación de estándares internacionales y participa en tratados y convenios relacionados con la ciberseguridad.

Análisis de la tabla comparativa

La creciente amenaza del *phishing* y otros delitos informáticos ha llevado a una evaluación crítica de las respuestas legislativas y de política pública a nivel internacional. En este contexto, la comparación entre las legislaciones de Ecuador y Estados Unidos revela diferencias significativas en definición, penalización, protección de datos, cooperación internacional, jurisdicción extraterritorial, prevención y educación, así como en el marco legal global. A continuación, se destacan las ventajas y desventajas del sistema legal ecuatoriano frente al estadounidense en estas áreas.

Ventajas del Sistema Legal Ecuatoriano

Ecuador muestra un compromiso con la cooperación internacional a través de su participación en programas de ciberseguridad de organizaciones como la OEA y la Unión Europea, lo que sugiere una apertura hacia el fortalecimiento de capacidades mediante alianzas internacionales. Otra de las ventajas, que Ecuador ha iniciado la implementación de políticas y campañas de concientización en ciberseguridad, destacando el esfuerzo por promover una cultura de prevención en la población y en entidades estatales.

Desventajas del Sistema Legal Ecuatoriano

A diferencia de Estados Unidos, donde el phishing está claramente definido y penalizado bajo leyes específicas como el CFAA y la Ley de Phishing de California, en Ecuador, la falta de una definición específica y penalizaciones directas para el phishing en el COIP obliga a una interpretación más amplia de varios artículos para abordar estos delitos, lo que podría complicar la persecución y sanción efectiva.

Aunque Ecuador tiene leyes que regulan el manejo de información personal, la especificidad y el alcance de estas normativas parecen ser menos desarrollados en comparación con las robustas leyes estadounidenses, como la CCPA y la ECPA. De igual forma, la capacidad de Ecuador para perseguir delincuentes fuera de su territorio parece limitada en comparación con Estados Unidos, que cuenta con un marco más extenso para la persecución extraterritorial de delitos informáticos, respaldado por tratados internacionales como el Convenio de Budapest.

Por lo tanto, se destaca la necesidad de que Ecuador fortalezca su marco legal y de política pública en materia de ciberseguridad y phishing. Esto incluye la adopción de definiciones más claras y específicas para delitos informáticos, el establecimiento de penalizaciones más directas, la mejora en la protección de datos personales, y una mayor participación en foros y convenios internacionales. A su vez, la cooperación internacional y las iniciativas de prevención y educación son áreas en las que Ecuador ya está tomando pasos positivos, aunque aún hay margen para mejorar y expandir estos esfuerzos. Contrastando con el sistema estadounidense, se observa la importancia de un enfoque integral que abarque legislación, cooperación internacional, y educación pública para enfrentar eficazmente los desafíos del cibercrimen.

4.1.3. Propuesta de reforma al artículo 190 del Código Orgánico Integral Penal (COIP) para incluir el delito de phishing.

Es necesario proponer soluciones que permitan responder a las necesidades de la sociedad, a través de una propuesta de reforma al Código Orgánico Integral Penal (COIP) específicamente al artículo 190 que habla sobre la apropiación fraudulenta por medios electrónicos, de esta manera, se garantiza una constante evolución de las normas jurídicas convirtiendo a este instrumento legal en moderno y adecuado para combatir las nuevas formas de criminalidad digital como el *phishing* convirtiéndose en una figura penal independiente. A continuación, se presenta de forma textual el artículo anteriormente mencionado y a su vez el apartado en el que consta la propuesta de reforma:

> **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 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. (Código Orgánico Integral Penal [COIP], 2014)

Artículo 190.1. - Phishing: La persona que, valiéndose de tecnologías de la información y comunicación, adquiera información confidencial de terceros mediante artificios, será sancionado con una pena privativa de libertad de 1 a 3 años.

En el caso de que dicho acto resulte en un perjuicio económico para la víctima, ya sea en beneficio personal del perpetrador o para favorecer a terceros, se impondrá una pena privativa de libertad de 3 a 5 años.

Si el delito se comete utilizando de manera masiva y automatizada las técnicas y medios mencionados en el primer inciso, la pena será en la máxima aumentada en un tercio.

Si en el caso de que una entidad pública o privada ha creado el riesgo y ha permitido la vulnerabilidad de su sistema de seguridad a causa de una omisión, insuficiencia o funcionamiento defectuoso, primero se deberá acudir por vía civil sin perjuicio que exista una responsabilidad penal.

4.2. Discusión de resultados

Los resultados del estudio indican que la legislación ecuatoriana no cuenta con las herramientas necesarias para sancionar este ciberdelito, siendo esta postura adoptada por los fiscales entrevistados, quienes evidentemente destacaron la necesidad de reformar la normativa ecuatoriana en materia de ciberdelitos para asegurar una sanción proporcional.

Lo dicho anteriormente es sostenido por los autores Masaquiza (2021) y Bisquert (2006) que utilizaron un análisis crítico-jurídico y doctrinal que les permitió concluir que existe una vulnerabilidad que presenta América Latina en cuanto a la ciberseguridad, específicamente Ecuador, además, de optar por una reforma legal que regule concretamente este delito informático. De igual forma, con la información recabada de fiscalía en cuanto a la seguridad en línea se pudo palpar que uno de los grandes problemas que se tiene es la

pericia técnica informática que en mucho de los casos resulta un limitante para recopilar las pruebas digitales necesarias, puesto que solo existe un perito informático en Chimborazo, Tungurahua, Pastaza, Bolívar y Cotopaxi.

Por otra parte, Divito (2021) destaca cómo el *phishing* constituye una amenaza directa a los bienes jurídicos protegidos por el Estado, en particular, aquellos que conllevan un perjuicio económico debido al uso indebido de información financiera. Esta práctica ilícita compromete el derecho fundamental a la propiedad privada de los individuos. Un ejemplo proporcionado por los entrevistados es el robo de datos de tarjetas de crédito, lo cual afecta directamente el patrimonio de una persona al posibilitar transferencias no autorizadas. Esta actividad ilegal menoscaba el derecho reconocido explícitamente en la Constitución de la República del Ecuador.

También, a través de un análisis bibliográfico entre Ecuador y Estados Unidos se realizó un derecho comparado en la cual se analizó distintos criterios tales como: concepciones, penas, normas que regulan la protección de datos, cooperación internacional, prevención y educación. Tras analizar estos criterios, se ha llegado a la conclusión de que Estados Unidos cuenta con legislación adecuada para abordar las nuevas modalidades del cibercrimen, como lo demuestra la ley Anti-Phishing de 2005, así como con acuerdos internacionales, como el Convenio de Budapest, destinados a combatir este tipo de delitos. Por otra parte, Ecuador requiere una mayor participación en estos convenios y tratados internacionales, dado que la falta de ratificación de algunos de ellos dificulta la persecución de los ciberdelincuentes fuera del país.

Asimismo, los entrevistados manifestaron dentro de la Cooperación Internacional que Fiscalía opera a través de una oficina de coordinación de asuntos internacionales en la ciudad de Quito; sin embargo, los tiempos de respuesta suelen ser prolongados. Es importante destacar que, en algunos casos, muchos gobiernos responden a solicitudes de cooperación internacional, mientras que otros no lo hacen, por no contar con dichos tratados. Esto genera dificultades, dado que algunos países proporcionan información, mientras que en otros casos es necesario insistir para obtener una respuesta adecuada.

Finalmente, diversas instituciones y organizaciones, como la INTERPOL (2020), Microsoft (2021) e IT Digital Security (2020), han expresado su preocupación por este

problema de alcance global. Es evidente que, con el avance de la tecnología, han surgido nuevas técnicas delictivas a través de internet. Por tanto, es imperativo que los Estados ajusten sus normativas para abordar estos ciberdelitos emergentes. En este sentido, el análisis comparativo de las legislaciones de otros países permitió proporcionar ideas y propuestas valiosas sobre los mecanismos utilizados para adaptarse al Ecuador, para que de esa forma como manifestaron los fiscales el *phishing* sea considerado como una figura penal independiente.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El phishing constituye una modalidad de fraude cibernético mediante la cual los atacantes buscan engañar a los usuarios para obtener su información personal, financiera o de cualquier tipo que resulte valiosa. Si bien no está tipificado como tal en la legislación penal ecuatoriana, doctrinariamente se considera un ciberdelito que afecta el derecho a la propiedad que está reconocido en la Constitución de la República del Ecuador al igual que en el Código Civil como una garantía que permite a las personas usar, disfrutar y disponer libremente de sus bienes adquiridos, por lo tanto, este derecho se ve afectado en los delitos informáticos, en el cual se vulnera la propiedad privada de datos personales y económicos de las víctimas sin su consentimiento para obtener un beneficio pecuniario.

Las normas actuales en la legislación ecuatoriana resultan inadecuadas para sancionar el ciberdelito de *phishing*. Al no existir una tipificación penal específica, este tipo de fraude informático queda en la impunidad o son procesados de forma ambigua bajo disposiciones genéricas sobre delitos informáticos puesto que la ausencia de un marco jurídico claro y comprehensivo ocasionan penas discordantes, falta de protección de datos personales, obstáculos para la cooperación internacional, limitaciones de jurisdicción sobre delincuentes transnacionales y carencias en la prevención educativa. Esta situación de vacíos e incertidumbres legales se diferencia de las sólidas herramientas jurídicas desarrolladas contra el *phishing* en países como Estados Unidos que han creado leyes con penas y multas para combatir esta modalidad delictiva que se van presentando en la sociedad con mayor frecuencia.

En base a los resultados obtenidos en las entrevistas realizadas a los fiscales y la tabla comparativa se pudo palpar que es necesario que se realice una reforma al artículo 190 del Código Orgánico Integral Penal puesto que a pesar de que hace referencia a la apropiación fraudulenta por medios electrónicos no aborda de manera específica el *phishing* provocando que la sanción no sea proporcional al delito cometido. Por otro lado, la ausencia de adhesión de Ecuador a tratados y convenios internacionales limita seriamente la mejora de la cooperación internacional. Asimismo, la falta de autoridades especializadas para gestionar eficientemente estos casos.

5.2. Recomendaciones

Se recomienda tipificar el *phishing* como un delito específico dentro del Código Orgánico Integral Penal ecuatoriano, estableciendo sanciones proporcionales que incluyan tanto penas privativas de libertad como multas pecuniarias, con el fin de disuadir esta modalidad de fraude que afecta derechos constitucionales como la propiedad y seguridad jurídica de los ciudadanos. La tipificación clara con penas adecuadas permitiría procesar efectivamente estos casos que actualmente quedan en ambigüedad legal.

Con respecto a la necesidad de mejorar la cooperación internacional y fortalecer la capacitación de autoridades especializadas, se recomienda que Ecuador busque activamente la adhesión a tratados y convenios internacionales pertinentes en el ámbito de la ciberseguridad y la lucha contra ciberdelitos. Además, se sugiere la implementación de programas de capacitación continua para fiscales y otros funcionarios encargados de hacer cumplir la ley, con el fin de mejorar su conocimiento y habilidades en la investigación y el enjuiciamiento de delitos informáticos, incluido el phishing. Esta capacitación debería incluir aspectos técnicos y legales relevantes para abordar eficazmente los desafíos que plantea la delincuencia informática en la actualidad.

El *phishing* constituye una forma de fraude cibernético en la cual los atacantes intentan engañar a los usuarios para obtener información valiosa, ya sea personal o financiera. Es crucial que los usuarios se protejan contra este tipo de ataques estando alerta ante correos electrónicos o mensajes no solicitados. Para ello, es fundamental verificar la autenticidad de los sitios web antes de proporcionar cualquier información personal y mantener actualizado el *software* de seguridad de manera periódica. Algunas señales comunes de *phishing* incluyen la recepción de mensajes que solicitan información confidencial, enlaces o archivos adjuntos sospechosos, así como URL mal escritas.

REFERENCIAS

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). *Phishing happens beyond technology: The effects of human behaviours and demographics on each step of a phishing process*.

Acurio, S. (2016). *Delitos Informáticos: Generalidades*.

Aldaz, Á. (2023). *Metodología para redactar un proyecto de investigación en la ciencia del derecho*. https://doi.org/10.23857/fipcaec.v8i2

Amusan, D., Falohun, A., & Tayo, O. (2023). *DEVELOPMENT OF AN EFFECTIVE SYSTEM FOR DETECTING CYBERCRIMES USING MODIFIED RIPPLE DOWN RULE SYSTEM AND NEURAL NETWORK*. *9*. file:///C:/Users/Jessica/Downloads/5663-Article%20Text-14849-1-10-20230509%20(1).pdf

Asociación de Internautas. (2007). La Asociación de Internautas revela que el «phishing» se cuadruplicó en 2006 con 1.184 ataques. *Libertad Digital*. https://www.libertaddigital.com/internet/la-asociacion-de-internautas-revela-que-el-phishing-se-cuadruplico-en-2006-con-1184-ataques-1276295814/

Bisquert, S. (2006). *´La figura del «phishing» como modalidad delictiva. Problemática en cuanto a su encuadre jurídico*. http://www.saij.gob.ar/doctrina/dacf060096-bisquert-figura_phishing_como_modalidad.htm

Código Orgánico Integral Penal. (2014). *ÁMBITOS DE APLICACIÓN*. https://www.lexis.com.ec/biblioteca/coip

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia Budapest*. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Constitución de la República del Ecuador [C.R.E.]. (2008). *Sección segunda Tipos de propiedad*. Registro Oficial 449 de 20-oct.-2008. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Council of Europe. (2023). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios*. https://rm.coe.int/cyber-buda-benefits-19april2023-es/1680aafa3f

Diccionario panhispánico del español jurídico. (2023). *Bien jurídico*. https://dpej.rae.es/lema/bien-jur%C3%ADdico

Divito, F. (2021). *Skimming y phishing de tarjetas de crédito o débito: ¿actos preparatorios o principio de ejecución de la defraudación cometida mediante tarjeta falsificada o el uso*

de sus datos? https://repositorio.udesa.edu.ar/jspui/bitstream/10908/18343/1/%5bP%5d%5bW%5d%20M.%20Der.%20Penal%20Divito%2c%20Francisco.pdf

El Universo. (2023). *Ecuador es uno de los tres países latinoamericanos con más ciberataques*. https://www.eluniverso.com/noticias/ecuador/ecuador-es-uno-de-los-tres-paises-latinoamericanos-con-mas-ciberataques-nota/

Estuardo, C. (2021). *Ciberdelincuencia: Análisis del Convenio No. 85 de Budapest y el compromiso del Estado de Guatemala*. https://doi.org/10.36314/cunori.v5i2.174

Federal Bureau of Investigation. (2021). *Internet Crime Complaint Center (IC3)*. https://www.ic3.gov/media/news/2024/240221.pdf

Fiscalía General Del Estado. (2020). Fiscalía abrió instrucción fiscal contra 6 procesados por presunto "phishing". *Boletín de presnsa FGE Nº 897-DC-2020*. https://www.fiscalia.gob.ec/fiscalia-abrio-instruccion-fiscal-contra-6-procesados-por-presunto-phishing/#:~:text=El%20delito%20de%20apropiaci%C3%B3n%20fraudulenta,electr%C3%B3nicas%20y%20de%20telecomunicaciones%20para

Gallegos, C. R. M. (2022). *Multidimensionalidad del Derecho a la Propiedad en el Constitucionalismo Ecuatoriano Multidimensionality of the Property Rights in the Ecuadorian Constitutionalism*. *2*(1).

Gisca, V. (2022). *Practical aspects of patrimony functions*. https://irek.ase.md/xmlui/bitstream/handle/123456789/2604/Conf_ASEM_SEPTEMBRIE_2022_p229-235.pdf?sequence=1&isAllowed=y

González, P. (2024). *ORIGEN Y EVOLUCIÓN DE LAS TÉCNICAS DE PHISHING EN EL MUNDO*. https://sellolegal.com/blog/origen-y-evolucion-de-las-tecnicas-de-phishing-en-el-mundo/

Herrera, R. (2021). *La comparación jurídica y su relación con otras disciplinas como metodología de armonización y unificación del derecho privado europeo y su conexión con el derecho romano*. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-R-2021-B0039300422

Homeland Security. (2003). *United States Computer Emergency Readiness Team*. https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

Instituto Español de Estudios Estratégicos. (2021). *Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción*. https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO78_2021_FRANMAR_Ciber.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2007). *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing*.

Internal Revenue Service. (2017). *Security Summit Launches Education Campaign Aimed at Tax Pros; Warns Against Phishing Epidemic with "Don't Take the Bait" series*. https://www.irs.gov/newsroom/security-summit-launches-education-campaign-aimed-at-tax-pros

INTERPOL. (2020). *Ciberdelincuencia: Efectos de la COVID-19*.

It Digital Security. (2020). *Informe sobre Phishing 2020*. https://www.itdigitalsecurity.es/it-whitepapers/2020/09/informe-sobre-phishing-2020

Juca, F., & Medina, R. (2023). *Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. 4*.

Kierszenbaum, M. (2009). *El bien jurídico en el derecho penal. Algunas nociones básicas desde la óptica de la discusión actual*. file:///C:/Users/Jessica/Downloads/07-ensayo-kierszenbaum%20(3).pdf

Ley de Fraude y Abuso Informático. (1986). https://caseguard.com/es/articles/la-ley-de-fraude-y-abuso-informatico-de-1986/

Lozsan, N. (2022). *Tipos de bienes económicos: Clasificación, concepto, características y ejemplos de bienes en economía*. https://www.cinconoticias.com/tipos-de-bienes-economicos/

Lutfor, M., Wali, H., Timko, D., & Neupane, A. (2023). *Users Really Do Respond To Smishing*. 15. https://doi.org/doi.org/10.1145/3577923.3583640

Martínez, I. (2023). Sobre los métodos de la investigación jurídica. *30 de junio 2023, 14*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-21502023000100101#:~:text=M%C3%A9todo%20Exeg%C3%A9tico%3A%20opera%20como%20parte,de%20los%20organismos%20y%20operadores

Masaquiza, L. (2021). *El Phishing como delito informático en la legislación ecuatoriana*. https://dspace.uniandes.edu.ec/bitstream/123456789/13462/1/UA-DER-PDI-026-2021.pdf

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. *44*. http://dx.doi.org/10.4067/S0718-34372017000100011

Microsoft. (2021). *Phishing and other malicious email*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Minori, F. H. (2023). *Phishing y su sanción en el sistema jurídico ecuatoriano.* file:///C:/Users/Jessica/Downloads/T-UCSG-PRE-JUR-DER-1057%20(2).pdf

Mohd, D., Beng, L., Al, H., & Shafiee, Y. (2007). *Managing Legal, Consumers and Commerce*

Montagner, A., & Merkle, C. (2022). *Uma breve analise sobre phishing*. 11. https://doi.org/10.5902/2448190471731

National Institute of Standards and Technolog. (2023). *Cybersecurity Awareness Month*. https://www.irs.gov/newsroom/security-summit-launches-education-campaign-aimed-at-tax-pros

Observatorio de Ciberseguridad. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*

Organización de las Naciones Unidas [ONU]. (s.f.). *Ciberseguridad*. https://www.un.org/counterterrorism/es/cybersecurity

Organización de los Estados Americanos. (2003). *Programa de Ciberseguridad*. https://www.oas.org/ext/es/seguridad/prog-ciber

Pascual, A. (2022). *Estados Unidos y su firme compromiso con la ciberseguridad*. https://www.unir.net/ingenieria/revista/estados-unidos-ciberseguridad-joe-biden/

Primicias. (2023). *Ecuador encabeza el listado de países en la región con más ataques de phishing*. https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-phishing/

Proudhon, P. (2005). *¿Qué es la propiedad?* Editorial Proyección S.R.L., Buenos Aires, 1970. https://www.marxists.org/espanol/proudhon/prop/que-es-la-propiedad.pdf

Rekouche, K. (2011). *Early Phishing*. 9.

Rico, M. (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos*. *VII*(31), 207-222.

Rodríguez, F., & González, J. (2019). *Propuesta de sistematización de los elementos de la investigación jurídica. Resultados de una experiencia*. *6*. https://pedagogiaderecho.uchile.cl/index.php/RPUD/article/view/55298/59077

Rojas, F. (2019). *Método dogmático en Derecho*. https://www.la-epoca.com.bo/2019/10/12/metodo-dogmatico-en-derecho/#:~:text=El%20m%C3%A9todo%20dogm%C3%A1tico%20propone%20estudiar,la%20doctrina%20y%20la%20jurisprudencia.

Salazar, N. (2007). *PHISHING: LA AUTOMATIZACIÓN DE LA INGENIERÍA SOCIAL*. https://repository.eafit.edu.co/server/api/core/bitstreams/906bf7e3-b804-4734-a18d-055fda586df3/content

Salgado, Á. (2012). *Apuntes sobre el concepto de bien jurídico*. file:///C:/Users/Jessica/Downloads/904%20(2).pdf

Santaella, H. (2019). *LA PROPIEDAD PRIVADA CONSTITUCIONAL: UNA TEORÍA*. https://www.marcialpons.es/media/pdf/9788491236405.pdf

Shackelford, S., & Craig, A. (2014). Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. *Revista Stanford de Derecho Internacional*.

Shouq Alnemari, & Alshammari, M. (2023). *Detecting Phishing Domains Using Machine Learning*. https://doi.org///doi.org/ 10.3390/app13084649

Shouse California Law Group. (s.f.). *Fraude en Internet en California – ¿Qué es y puedo ir a la cárcel?* https://www.shouselaw.com/es/ca/defensa/fraude/fraude-en-internet/#3.1.3

Torres, A. (2023). *Responsabilidad administrativa de los bancos en los casos de phishing a propósito de las resoluciones brindadas por Indecopi*. https://tesis.usat.edu.pe/bitstream/20.500.12423/6488/1/TL_TorresChavezAndrea.pdf

Torres, T. (2020). *En defensa del método histórico-lógico desde la Lógica como ciencia*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142020000200016

Toudert, D., & Buzai, G. (2004). *Cibergeografía. Tecnología de la Información y las Comunicaciones (TIC) en las nuevas visiones espaciales.* 240.

UNIR. (2024). *¿Qué son los delitos informáticos o ciberdelitos? Tipos y ejemplos*. https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

Vilela, E., Takeo, E., & Luiz, V. (2022). *Phishing and social engineering: Concept, modalities, techniques of detection and prevention of fraud. A systematic review of the literature*. 22. https://doi.org/10.5748/19CONTECSI/PSE/SEC/7138

ANEXOS

Anexos 1: *Guía de entrevista*

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

Destinatarios: Fiscales del cantón Riobamba de la provincia de Chimborazo

Objetivo:

Comprender la problemática del *phishing* centrándose en el procedimiento legal para la persecución de este ciberdelito, con el objetivo de proponer una reforma en el Código Orgánico Integral Penal que establezca una sanción proporcional a la gravedad del delito cometido.

Consentimiento Informado:

Antes de comenzar la entrevista, es fundamental informar a la persona entrevistada sobre el propósito de la misma, asegurándonos de obtener su consentimiento para participar y registrar la información. La entrevista se centrará en ciberdelitos con énfasis en casos de phishing y su tratamiento en el ámbito penal. ¿Está de acuerdo con participar en esta entrevista sobre ciberdelitos y phishing?

Información del entrevistado

1. Nombre completo:
2. Cargo o posición actual:
3. Experiencia en delitos informáticos:

Guía de entrevista

1. ¿Podría proporcionar una definición técnica de phishing?
2. ¿Cuáles considera que son las características distintivas de un ataque de phishing?
3. En el contexto de un caso de phishing, ¿cuáles son las mejores prácticas para recopilar pruebas digitales?
4. ¿Qué desafíos enfrenta al rastrear la autoría de un ataque de phishing?
5. ¿Cómo se coordina la investigación de casos de phishing entre jurisdicciones, especialmente considerando la naturaleza transnacional de muchos ciberdelitos?
6. ¿Cuáles son los desafíos comunes al trabajar con autoridades internacionales en casos de phishing?

7. ¿Cuál es el procedimiento legal estándar para el enjuiciamiento de un individuo acusado de phishing?
8. ¿Qué leyes y regulaciones específicas se aplican comúnmente en casos de phishing?
9. ¿Existen casos judiciales significativos que hayan sentado precedentes en el enjuiciamiento de casos de phishing?
10. ¿Cómo se promueve la concientización y la prevención del phishing a nivel público y empresarial?
11. ¿Cuáles son las posibles mejoras o cambios legislativos que podrían fortalecer la lucha contra el phishing?
12. ¿Cómo se adaptan las leyes actuales a la evolución de las tácticas de phishing?

Agradezco su disposición para participar en esta entrevista. Le recuerdo que la información proporcionada será utilizada únicamente con fines académicos y de investigación, manteniendo la confidencialidad de su identidad.

Anexos 2: Validación del instrumento

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Julio Alvarado Vélez
Especialidad:

Título de la investigación: El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación ecuatoriana: *phishing*

Objetivo del instrumento (Que pretende medir): Comprender la problemática del phishing centrándose en el procedimiento legal para la persecución de este ciberdelito, con el objetivo de proponer una reforma en el Código Orgánico Integral Penal que establezca una sanción proporcional al delito cometido.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓		✓		✓		✓			
2	✓		✓		✓		✓		✓			
3	✓		✓		✓		✓		✓			
4	✓		✓		✓		✓		✓			
5	✓		✓		✓		✓		✓			
6	✓		✓		✓		✓		✓			
7	✓		✓		✓		✓		✓			
8	✓		✓		✓		✓		✓			
9	✓		✓		✓		✓		✓			
10	✓		✓		✓		✓		✓			
11	✓		✓		✓		✓		✓			
12	✓		✓		✓		✓		✓			

Firma de Validador:
Nombre: JULIO ALVARADO VÉLEZ
Cédula: 1717282675

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Edison Bonifaz
Especialidad: Metodología de la Investigación

Título de la investigación: El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación ecuatoriana: *phishing*

Objetivo del instrumento (Que pretende medir): Comprender la problemática del phishing centrándose en el procedimiento legal para la persecución de este ciberdelito, con el objetivo de proponer una reforma en el Código Orgánico Integral Penal que establezca una sanción proporcional al delito cometido.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn item)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓		✓		✓		✓			
2	✓		✓		✓		✓		✓			
3	✓		✓		✓		✓		✓			
4	✓		✓		✓		✓		✓			
5	✓		✓		✓		✓		✓			
6	✓		✓		✓		✓		✓			
7	✓		✓		✓		✓		✓			
8	✓		✓		✓		✓		✓			
9	✓		✓		✓		✓		✓			
10	✓		✓		✓		✓		✓			
11	✓		✓		✓		✓		✓			
12	✓		✓		✓		✓		✓			

Firma de Validador:
Nombre: Edison Bonifaz
Cédula: 0603036269

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Danny Silva Cruz
Especialidad: Derecho Penal

Título de la investigación: El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación ecuatoriana: *phishing*

Objetivo del instrumento (Que pretende medir): Comprender la problemática del phishing centrándose en el procedimiento legal para la persecución de este ciberdelito, con el objetivo de proponer una reforma en el Código Orgánico Integral Penal que establezca una sanción proporcional al delito cometido.

	Claridad en la redacciòn		Coherencia interna		Introducciòn a la respuesta (Sesgo)		Pertinencia		Calificaciòn de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algùn ìtem)
Preguntas	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	✓		✓		✓		✓		✓			
2	✓		✓		✓		✓		✓			
3	✓		✓		✓		✓		✓			
4	✓		✓		✓		✓		✓			
5	✓		✓		✓		✓		✓			
6	✓		✓		✓		✓		✓			
7	✓		✓		✓		✓		✓			
8	✓		✓		✓		✓		✓			
9	✓		✓		✓		✓		✓			
10	✓		✓		✓		✓		✓			
11	✓		✓		✓		✓		✓			
12	✓		✓		✓		✓		✓			

Firma de Validador:
Nombre: Danny Silva Cruz
Cédula: 0604509968

Anexos 3:Oficio a fiscalía

Riobamba, 04 de marzo del 2024

Ab. Francisco Verduga Romero

Director Provincial de Recursos de Fiscalía Provincial de Chimborazo

Presente. -

De nuestra consideración:

Nosotras, **JESSICA ISABEL GARCÍA ANDRADE** con número de cédula de ciudadanía **2300489644**, **GISSELA ESTEFANÍA PILCO GUAMÁN** con número de cédula de ciudadanía **0606447894**, estudiantes de la **Universidad Nacional de Chimborazo**, Facultad de Ciencias Políticas y Administrativas, **Carrera de Derecho**, solicitamos de la manera más comedida se sirva autorizar a todos los fiscales del cantón Riobamba, a fin de realizar una **entrevista** respecto a nuestro trabajo de titulación denominado: **"Derecho a la propiedad privada y nuevas modalidades en delitos cibernéticos en la legislación Ecuatoriana: Phishing"** previo a la obtención del título a Abogado/a.

Por su gentil atención, reciba nuestro agradecimiento.

Atentamente,

Jessica Isabel García Andrade

C.C. 230048964-4

Gissela Estefanía Pilco Guamán

C.C. 060644789-4

FISCALIA DE CH... FGE Fiscalía General del Ecuador RIOB...

Recibido 04/03/2024