Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XII Número: Edición Especial Artículo no.:113 Período: Diciembre del 2024

TÍTULO: Fundamentos jurídicos para la inclusión del delito de phishing en el código penal ecuatoriano.

AUTORES:

1. Abg. Lisette Odalis Flores Heredia
2. Máster. Kleber Eduardo Carrión León
3. Est. Joselyn Gabriela Rivera Velasco

RESUMEN: Este estudio realiza un análisis teórico del phishing, un delito informático desde 1996 que involucra el envío de correos electrónicos fraudulentos para obtener información personal de forma engañosa. A pesar de su creciente prevalencia, el phishing no está específicamente tipificado en el Código Orgánico Integral Penal de Ecuador, lo que limita su persecución efectiva. La investigación, basada en un enfoque cualitativo con métodos analítico-sintético e inductivo-deductivo, emplea análisis documental y entrevistas para argumentar la necesidad de tipificar este delito en la legislación ecuatoriana. Los hallazgos destacan que la falta de una tipificación adecuada del phishing vulnera derechos constitucionales y su inclusión en la legislación permitiría una protección legal más efectiva contra esta amenaza emergente en el entorno digital.

PALABRAS CLAVES: ciberdelincuentes, phishing, delito informático, legislación, plataformas digitales.

TITLE: Legal grounds for the inclusion of the crime of phishing in the Ecuadorian criminal code.

AUTHORS:

1. Atty. Lisette Odalis Flores Heredia.
2. Master. Kleber Eduardo Carrión León.
3. Stud. Joselyn Gabriela Rivera Velasco.

ABSTRACT: This study performs a theoretical analysis of phishing, a computer crime since 1996 that involves sending fraudulent e-mails to obtain personal information in a deceptive manner. Despite its growing prevalence, phishing is not specifically typified in Ecuador's Organic Integral Criminal Code, which limits its effective prosecution. The research, based on a qualitative approach with analytical-synthetic and inductive-deductive methods, employs documentary analysis and interviews to argue the need to typify this crime in Ecuadorian legislation. The findings highlight that the lack of an adequate typification of phishing violates constitutional rights and its inclusion in the legislation would allow a more effective legal protection against this emerging threat in the digital environment.

KEY WORDS: cybercriminals, phishing, computer crime, legislation, digital platforms.

INTRODUCCIÓN.

En relación con el tema propuesto, la modalidad del phishing comienza a ser conocida aproximadamente en el año 1996, y se origina del término inglés que se asimila a 'fishing', traduciendo a español como 'pescar'; según Jennifer Rueda (2020), en el estudio monográfico "Impacto de la técnica de ataque de phishing en Colombia durante los últimos cinco años" refiere al mismo con el objetivo de pescar a un usuario que caiga en la red, y recibir un beneficio de forma ilícita.

El desarrollo de la tecnología actualmente supone un impacto generalizado en todos los campos y actividades, construyendo un nuevo paradigma global conocido como la "Era Digital", al que la sociedad se adapta continuamente. El uso de los sistemas de información por medios electrónicos refleja tanto ventajas como desventajas, y con el uso de páginas web, los datos personales quedan reflejados en el ciberespacio representando un peligro, ante la presencia de los delitos informáticos, entre ellos; el phishing.

En tanto que Lenin Masaquiza (2021), al realizar un estudio sobre el phishing como delito informático en la legislación ecuatoriana indica, que busca pescar datos confidenciales, considerándolo como delito que data de la década de los noventa tras la creación de la informática e internet, así como la apropiación de información confidencial tales como la identidad de una persona, contraseñas, claves bancarias, entre otros.

Por otra parte, Javier Fernández, autor del libro del Cibercrimen, considera que el phishing es una manifestación de la ingeniería social; es decir, la manipulación de las personas para que a su voluntad realicen actos que no harían, por lo que el atacante aprovecha el desconocimiento de las mismas para engañarlas a su propio beneficio. Además, detalla en que consiste del "envío de correos electrónicos, que aparentando provenir de fuentes fiables, -normalmente entidades bancarias- adoptan su imagen corporativa: con logotipos, imágenes y textos que han sido recogidos del sitio real" (Fernández, 2007, pág. 29).

La acción ilícita del phishing en la normativa ecuatoriana no aparece como tipo de delito, pues las autoridades de justicia lo relacionan y sancionan conforme al artículo 186 del Código Orgánico Integral Penal, en adelante las siglas COIP, clasificado como estafa; sin embargo, la tipicidad que dispone dicha disposición legal no corresponde al phishing específicamente, debido a que el mismo no solo tiene fines de perjuicio patrimonial, ya que involucra la simulación visual y la ingeniería social para obtener los datos personales a fin de usar dicha información y atentar con la intimidad y privacidad contenida en las plataformas digitales. En cuanto al artículo mencionado establece:

Art. 186.- Estafa. La persona, que para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años (…) (Asamblea Nacional del Ecuador, 2014).

Además, en la legislación internacional que abarca los delitos informáticos se señala en el Convenio de Budapest sobre la Ciberdelincuencia (2004), tratado internacional dirigido a combatir el crimen organizado transnacional con relación a los delitos informáticos, siendo un cuerpo normativo vinculante de países que forman parte del mismo, que referente a Ecuador, es un país meramente observador. El Convenio sobre la Ciberdelincuencia con relación al phishing, en el artículo 8 detalla sobre el Fraude Informático: Las Partes

adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos.

b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona (Convenio sobre la Ciberdelincuencia, 2004).

El phishing se plantea como un problema actual con un enfoque distinto en cuanto a la importancia y novedad científica, debido a que busca obtener datos personales que afecta a quienes reciben correos electrónicos que simulan su autenticidad; sin embargo, son falsos y obtienen dicha información a fin de afectar la intimidad y privacidad de las personas.

Por lo que representa vulnerabilidad y riesgo en cuanto a la seguridad informática, ya que se ven afectados derechos constitucionales tales como la protección de datos de carácter personal (referido a la Ley Orgánica De Protección De Datos Personales) y la intimidad personal, como aristas principales contenidos en el artículo 66 numerales 19 y 20, respectivamente de la norma suprema (Asamblea Nacional Constituyente del Ecuador, 2008).

A medida de los avances tecnológicos, los delitos informáticos han adquirido mayor relevancia a nivel mundial; sin embargo, las investigaciones sobre este tipo de delitos en el país son superficiales, puesto que no son reconocidos conforme a sus finalidades específicas como el phishing, de manera que en la normativa legal se vincula a la sanción penal del delito de estafa.

Es así como el phishing es practicado ampliamente hacia los usuarios mediante el envío de correos electrónicos, debido a que los cibercriminales usan formas sutiles de engañar a las personas en actividades digitales, logrando la sustracción de información, uso de claves bancarias y divulgación de datos personales; por lo que la exteriorización e investigación del phishing genera importancia en cuanto al análisis en la legislación penal ecuatoriana; por ende, genera la incógnita de ¿cuál es la importancia de reconocer la

tipificación del phishing en la legislación penal ecuatoriana? siendo el objetivo general del presente artículo científico explicar la importancia de la tipificación del phishing en la legislación penal ecuatoriana.

DESARROLLO.

Materiales y métodos.

Para el desarrollo de la investigación se empleó la modalidad cualitativa, ya que se investigó a partir de información documental contenida en normativas legales, doctrinas, artículos científicos y libros sobre el phishing y la importancia de la tipificación en la legislación penal ecuatoriana. Del mismo modo, se utilizó diseño no experimental teórico fundamentado, puesto que se desarrolla en un marco predominantemente teórico basado en estudios físicos y electrónicos. Se estableció un alcance explicativo, a fin de detallar y explicar aspectos del phishing e importancia con base a material académico y digital.

Con fines de analizar y recopilar información, se aplicaron los métodos analítico – sintético, con el objetivo de seleccionar y compilar información con relación a fuentes teóricas como entrevistas y estudio documental, así como el método inductivo - deductivo, proyectando el phishing en el ámbito nacional como acto ilícito que no aparece como tipo de delito en la legislación penal ecuatoriana, por lo que corresponde a un proceso investigativo de descomponer la información en ideas principales y de contenido específico respectivamente.

El análisis documental y dentro de las ciencias jurídicas, el método dogmático, que caracterizó la investigación por el sustento actual, teórico y práctico, permitió indagar sobre la importancia de reconocer la tipificación del phishing en la legislación penal ecuatoriana a través de argumentos jurídicos y explicativos.

En la recolección de datos se utilizó la técnica documental, con instrumento las fichas bibliográficas, para obtener y registrar información esencial a través de documentación física y digital; entre las fuentes consultadas se revisó en libros de delitos informáticos, artículos científicos y proyectos de investigación con relación al phishing.

De igual modo, se empleó el estudio normativo en lineamientos legales como la Constitución de la República del Ecuador (Asamblea Nacional Constituyente del Ecuador, 2008), Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014), Ley de Comercio Electrónico, Firmas y Mensaje de Datos (Congreso Nacional del Ecuador, 2002), Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021), Ley Orgánica de Transparencia y Acceso a la Información Pública (Congreso Nacional del Ecuador, 2004) y la Ley Orgánica para la Transformación Digital y Audiovisual (Asamblea Nacional del Ecuador, 2023), y a nivel internacional, el Convenio de Budapest sobre la Ciberdelincuencia.

En cuanto a la entrevista, ésta se realizó al representante de la Fiscalía Especializada de Delincuencia Organizada Transnacional e Internacional (FEDOTI) de la ciudad de Santo Domingo, puesto que es competente en ejercer la acción penal pública, dos abogados en libre ejercicio especialistas en derecho informático de la ciudad de Quito, un abogado especialista en Derecho de la Ciberseguridad y Entorno Digital de Colombia, personas expertas en la materia de derecho informático, y un Ingeniero en sistemas de informática de Santo Domingo, ya que es una persona experta en tecnologías de información y recursos tecnológicos, por lo que aportaron elementos relevantes para el estudio del phishing e importancia; para tal fin, se elaboró la correspondiente guía de preguntas con el objeto de guiar la entrevista.

Resultados.

Estudios investigativos del phishing.

De la documentación investigada, es importante destacar, que de acuerdo con Hernández et al. (2022), autores del estudio de “Análisis del crecimiento de phishing en los últimos años” sostienen una clara definición del phishing, el cual consiste en un delito cibernético basado en atraer al usuario para obtener información sensible y personal como datos bancarios, usuarios y contraseñas, tarjetas de créditos y otros, mediante el envío de correos electrónicos que proporciona el atacante.

En el artículo de la Revista Ibérica de Sistemas y Tecnologías de información, los autores Villón et al. (2019) afirman, que el uso de las tecnologías en la actualidad es inevitable, puesto que el mundo está

inmerso en el uso de estos recursos, debido a que la navegación en la web ofrece oportunidades a todas las personas para comunicar ideas y generar cambios en la sociedad; no obstante, también representa desventajas, ya que la información personal se expone por esta red informática.

Según los autores Alcívar et al. (2016), en el libro titulado Análisis Espacial de los Delitos y Aplicación de la Normativa Juridica Ecuatoriana expresan, que el phishing ha desarrollado mutaciones y ha sofisticado sus formas de empleo, por lo que los ciberdelincuentes utilizan y manipulan URLs, cuyas direcciones falsas se agregan texto al final que direccione a otro enlace para capturar los datos e información personal; así mismo, disfrazan enlaces usando direcciones de páginas web oficiales con el símbolo de arroba "@" para crear autenticidad y solicitar usuario y contraseña.

Es importante reiterar, que el phishing en la normativa ecuatoriana no figura como delito, pues las autoridades de justicia del país lo relacionan y sancionan a casos de estafa o apropiación fraudulenta por medios electrónicos, enmarcados respectivamente en los artículos 186 y 190 del Código Orgánico Integral Penal, los cuales establecen:

Art. 186.- Estafa. - La persona, que para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años (…). (Asamblea Nacional del Ecuador, 2014).

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 (Asamblea Nacional del Ecuador, 2014).

Estos tipos de delitos no comprenden al objetivo del phishing, puesto que se presenta a través de la simulación visual, donde el ciberdelincuente envía correos electrónicos que simulan ser legítimos de fuentes como bancos, empresas e instituciones conocidas, adquiriendo logotipos, textos que solicitan información personal o datos bancarios para usar dicha información con fines de perjuicio patrimonial, divulgar información y atentar la privacidad personal. Como es el caso del Banco Pichincha, donde los ciberdelincuentes usan el nombre, logo e información de esta entidad.

Es así, que la página oficial del Banco Pichincha, en la sección de información legal detalla usos y condiciones, acorde al aviso de privacidad para canales electrónicos enmarca niveles de seguridad con el fin de proteger los datos personales de los clientes y usuarios a través de los canales electrónicos, además de señalar el sitio web correspondiente de la entidad siendo www.pichincha.com y canales electrónicos como la Banca Web, Banca Móvil para el conocimiento y práctica de los usuarios, puesto que la entidad financiera hace uso de datos personales, de navegación, sensibles, crediticios a fin de requerir servicios financieros (Banco Pichincha, 2023).

De acuerdo con al informe anual 2022 de la Organización Internacional de Policía Criminal (2023), presentado el 30 de junio del año 2023, los delitos financieros y aquellos cometidos por Internet son las principales preocupaciones de la INTERPOL; según el Informe resumido sobre las tendencias de la delincuencia a escala mundial (2022) revela, que más del sesenta por ciento (60%) de los encuestados calificaron a los delitos como el ransomware, el phishing y las estafas en línea como amenazas delictivas de escala “alta” o “muy alta”, según los datos adquiridos en los 195 países miembros. Además de prever, que en el futuro, a medida del avance tecnológico, los delitos informáticos aumenten.

Con base a las estadísticas obtenidas de la Dirección de Estadística y Sistemas de Información de Fiscalía General del Estado en el año 2022, a nivel nacional se han registrado noticias del delito del tipo penal de apropiación fraudulenta por medios electrónicos de un total de 3.136 casos y en el tipo penal de estafa 22.733 casos, por lo que se presenta un total de 25.869 noticias del delito en el país ecuatoriano.

Referente al año 2023, a nivel nacional, las noticias de delitos tipo penal de apropiación fraudulenta por medios electrónicos y estafa representan 3.443 y 24.367 casos respectivamente, con un total de 27.810 casos.

En cuanto a la provincia de Santo Domingo de los Tsáchilas, en el año 2022 se registra un total de 121 noticias de delito tipo penal apropiación fraudulenta por medios electrónicos y un total de 644 en casos de estafa. La suma de dichos casos representa una totalidad de 765 noticias de delito. En el año 2023, las noticias de delitos tipo penal de apropiación fraudulenta por medios electrónicos registró 131 casos, y estafa 585 casos, presentando un total de 716 noticias (Dirección de Estadística y Sistemas de la Información de Fiscalía General del Estado, 2023).

Por consiguiente, es importante destacar, el principio de legalidad de conformidad con la Convención Americana sobre Derechos Humanos (Organización de los Estados Americanos, 1969), el artículo 9 señala que ninguna persona puede ser condenada por acción u omisión que no fuera conducta delictiva al momento de cometerse según el derecho aplicable correspondiente. Conocido a través de las locuciones latinas formuladas “nullum crimen, nulla poena sine lege praevia” (no hay delito ni pena sin ley previa), que enfatiza la importancia de que exista una ley previa que defina las conductas delictivas y señale las penas respectivas.

Así mismo, reiterando el principio de legalidad que establece la norma suprema del Ecuador:

Art. 76.- En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas:

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

En concordancia con el Código Orgánico Integral Penal, que refiere entre los principios procesales, se destaca el principio de legalidad que define:

1. Legalidad: no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla (Asamblea Nacional del Ecuador, 2014).

Además, la Corte Constitucional del Ecuador analiza respectivamente del principio de legalidad en la Sentencia 1364-17-EP/23, Caso 1364-17-EP, la cual: "representa una garantía del debido proceso en cuanto limita el poder punitivo del Estado en el juzgamiento de una infracción y otorga previsibilidad y seguridad a las personas respecto al marco de actuación de los operadores de justicia" (Corte Constitucional del Ecuador, 2023).

Por tanto, el phishing al presentarse como un problema actual y dado a la conceptualización y riesgos que representa, se ven afectados derechos constitucionales, como la protección de datos de carácter personal y la intimidad personal, entre otros bienes jurídicos, como aristas principales, en relación a los derechos constitucionales:

Art. 66.- Se reconoce y garantizará a las personas:

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

20. El derecho a la intimidad personal y familiar (Asamblea Nacional Constituyente del Ecuador, 2008).

La autora Lisbeth Baños (2022) refiere, que el phishing utiliza técnicas de camuflaje, irreconocible para el usuario y se manifiesta mediante correos electrónicos como Gmail, Outlook, con enlaces vinculados a una página fraudulenta con el fin de extraer información o datos personales de los usuarios para vulnerar la seguridad de los mismos.

Dicho de otro modo, el phishing implica el uso de correos electrónicos con enlaces falsos que abarcan formatos, paleta de colores y textos similares a las instituciones legítimas, cuyos ataques encaminan a las personas a dichos sitios para extraer datos personales sobre las cuentas de los usuarios como contraseñas, tarjetas de crédito, números de teléfonos, bancarios u otra información útil para obtener beneficios económicos, divulgar detalles personales y vulnerar la seguridad y privacidad.

De acuerdo con Mishell Ventura (2021), el phishing es una de las técnicas más clásicas de ciberdelincuencia donde los atacantes simulan ser entidades legítimas, sean bancarias o empresas, mediante el envío de correos electrónicos que abarcan enlaces falsos con el fin de obtener información personal, prevaleciendo el uso de medios digitales; adicionalmente, hace mención al Consejo de la Unión Europea que adoptó medidas para garantizar que esas conductas sean delitos penales.

Es así, que en el contexto internacional, Ecuador forma parte como un país meramente observador al Convenio de Budapest sobre la Ciberdelincuencia del Consejo de la Unión Europea; es decir, que no forma parte del mismo, puesto que aún no completa el proceso de ratificación al Convenio, el cual establece medidas legislativas necesarias para tipificar delitos en el marco nacional; por tanto, en el artículo 8 detalla sobre el fraude informático: Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos.

b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona (Convenio sobre la Ciberdelincuencia, 2004).

Ecuador no forma parte del Convenio de Budapest sobre la Ciberdelincuencia; sin embargo, en el período de gobierno del expresidente Guillermo Lasso se ha considerado la armonización con instrumentos legales internacionales como es el Convenio sobre la Ciberdelincuencia en cuanto a los delitos informáticos, cuyo proceso de adhesión requiere la aplicación en la legislación nacional, según lo señala la Estrategia Nacional de Ciberseguridad del Ecuador del Ministerio de Telecomunicaciones y de la Sociedad de la Información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

En la normativa nacional, la Ley Orgánica de Protección de Datos Personales garantiza el derecho a la protección de datos personales, e integra definiciones esenciales, como lo señala en el artículo 4: "Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente" (Asamblea Nacional del Ecuador, 2021), en concordancia con la Ley Orgánica de Transparencia y Acceso a la Información Pública (Congreso Nacional del Ecuador. 2004), que reitera dicha definición en el artículo 4, cuyo objeto es garantizar y regular el derecho de acceso a la información pública.

En cuanto al principio de confidencialidad de los datos referido en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (Congreso Nacional del Ecuador, 2002), el cual dispone de sanción de acuerdo a la ley en cuanto refiere a la intrusión electrónica, transferencia ilegal de mensajes de datos, puesto que el objetivo del mismo es regular los mensajes de datos y proteger a los usuarios en los sistemas electrónicos.

De igual manera, en el año 2023 se aprobó el Proyecto de Ley Orgánica para la Transformación Digital y Audiovisual (Asamblea Nacional del Ecuador, 2023), la cual posee varios puntos entorno a las definiciones, a fin de profundizar en el tema, destacando el literal f) del artículo 5:

f. De la Identidad Digital. - La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. Los atributos de la identidad digital son otorgados por

distintas entidades de la Administración Pública, que en su conjunto, caracterizan al individuo (Asamblea Nacional del Ecuador, 2023).

Es necesario comprender respectivamente de la identidad digital, el cual está constituido por lineamientos, especificaciones y estándares entorno a la identificación y autenticación de los ciudadanos respecto a los servicios digitales, como el acceso a servicios en línea y la conexión con otras personas, cuyos datos personales navegan en el ciberespacio, por lo que supone la protección y validación de los mismos.

Resultados de las entrevistas.

En cuanto al uso de la técnica de entrevista, se obtuvo criterios de representante de la Fiscalía Especializada de Delincuencia Organizada Transnacional e Internacional (FEDOTI) de la ciudad de Santo Domingo, dos abogados en libre ejercicio especialistas en derecho informático de la ciudad de Quito, un abogado especialista en Derecho de la Ciberseguridad y Entorno Digital de Colombia, y un Ingeniero en sistemas de informática de Santo Domingo, quienes son factores importantes para determinar la importancia del phishing en la legislación penal ecuatoriana, y en la cual señalan:

La fiscal, representante de la Unidad de Fiscalía Especializada de Delincuencia Organizada Transnacional e Internacional (FEDOTI) indica, que el phishing se presenta dependientemente del acto que realicen al momento de usar datos de las personas, de los cuales no se ha autorizado para realizar actos delictivos. Señala que el phishing dentro de la unidad se vincula a delitos de estafa o apropiación fraudulenta por medios electrónicos, y a pesar de existir una serie de delitos que se cometen en el país, con leyes que protegen los derechos, en Ecuador no existen del todo garantías para evitar estos tipos de delitos.

El abogado experto en derecho informático considera un concepto más amplio referente al phishing como una práctica altamente perjudicial y engañosa que representa una seria amenaza para la seguridad en línea de los usuarios. Al aprovechar la ingeniería social y la falsificación de sitios web legítimos, los ciberdelincuentes engañan a las personas para que divulguen información personal y confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios, lo que puede llevar a la pérdida de identidad,

robo de fondos, acceso no autorizado a cuentas, y en general, afectar negativamente la confianza y la seguridad de los usuarios en línea.

Como abogado en libre ejercicio ha tenido casos de clientes y familiares que han recibido correos falsos, específicamente de la entidad del Banco Pichincha, a través de los cuales les piden que actualicen la información personal; sin embargo, al ser de correos no oficiales o sospechosos, proceden a la inmediata eliminación, por lo que no va más allá a un proceso; por tanto, refiere que existen riesgos para los usuarios al exponerse ante el phishing como la pérdida financiera, la suplantación de identidad, malware y ransomware, pérdida de acceso a cuentas, daño a la reputación y propagación de spam, lo que conllevaría a derechos vulnerados como la protección de datos de carácter personal y la integridad personal.

A su vez, abogado experto en la misma materia afirma, que en una realidad social que se vive a nivel mundial, el phishing ha sido desarrollado con el auge tecnológico, es más, con la inteligencia artificial, en la cual la delincuencia organizada, experta en delitos informáticos, podría desarrollar un mejor método de engaño, y reconoce que si bien en el Ecuador no se encuentra tipificado, generalmente dicha figura legal es vinculado al artículo 190 del Código Orgánico Integral Penal.

En el mismo sentido, ha recibido casos de phishing en los que a través de correos electrónicos falsos de empresas privadas que solicitan actualizaciones de datos personales, o de que ha sido bloqueado de cuentas bancarias, donde requieren claves personales, de redes sociales, números de tarjeta, e información personal, para que mediante esta modalidad, y con aquellos datos, acceder a través de tarjeta de crédito, o ingresar a banca web y hacer transferencias en entidades bancarias con enlaces fraudulentos, aunque usualmente el caso no avanza más allá de una denuncia.

En cuanto a los riesgos manifiesta, que existe la pérdida de datos por uso fraudulento de los mismos, donde se expone a que los datos recopilados a través de esta modalidad sean vendidos por internet para el cometimiento de delitos informáticos, consecuentemente afectando derechos constitucionales como la protección de datos de carácter personal y la intimidad personal.

El abogado Magister en Derecho de Ciberseguridad y Entorno Digital enfatiza que el phishing es la modalidad delictiva más usada en la actualidad por los ciberdelincuentes, por la eficacia dada a la falta de cibercultura en las personas; es decir, que las personas no conocen del todo delitos informáticos que emergen con el desarrollo, además de no saber actuar frente a estos casos.

En la Firma de abogados donde ejerce señala, que obtiene casos respecto a la llegada de correos phishing, y que a través de las herramientas digitales e investigaciones llegan a la detección del mismo, considerando fundamentalmente a la normativa internacional del Convenio de Budapest. Los riesgos que presenta el phishing recaen ante el hurto de información y datos, así como la suplantación de la imagen personal y el entorno digital, en consecuencia, se ven afectados derechos como la protección de datos de carácter personal, ya que hace uso de la informática y datos personales.

El Ingeniero en sistemas de informática puntualiza, que desde un enfoque tecnológico, el phishing es una herramienta útil para hacer daño a otra persona, donde la persona que comete el daño se favorece de la ignorancia y falta de conocimientos de la persona afectada, y por ese medio atacar y generar daños. Afirma, que debe ser considerado como un delito informático, porque la finalidad no es únicamente obtener la información de otro usuario, es de obtener sus datos para robar sus cuentas bancarias, y de perjudicar o inmiscuirse en la vida de otro.

En el ejercicio de la profesión ha presenciado casos del phishing, incluso en instituciones educativas, donde correos electrónicos son enviados a estudiantes, que mismos que desconocen acceden al link o enlace, afectando a las plataformas estudiantiles, generando una especie de bola de nieve que va perjudicando de estudiante a estudiante: por ello, ante los riesgos, recomienda revisar detenidamente los remitentes de los correos electrónicos, si es una persona de confianza o desconocida, así como tener en cuenta los enlaces que contienen dichos correos, las intenciones o finalidades de los mismos, enlaces o imágenes extrañas, la paleta de colores que no correspondan a la institución, y faltas ortográficas; por tanto, es importante ser

cauteloso en cuestión del uso de la información de los datos de la persona a través de los medios informáticos.

Discusión.

En esta investigación, con base a los resultados obtenidos de las técnicas de investigación empleadas, se determina que la creciente dependencia de la tecnología en la sociedad ha creado un nuevo entorno digital, donde la información personal se almacena en sistemas electrónicos, por lo que surgen delitos entorno al medio digital como es el phishing.

Según indica Javier Fernández, en el libro titulado Cibercrimen, el phishing es una manifestación de la ingeniería social, basado en la manipulación hacia las personas para realizar actos que no harían por su propia voluntad, por lo que se ve afectado el deber objetivo de cuidado de la persona, ya que se vulnera el consentimiento al no cumplir con las características correspondientes de ser libre, especifica, informada e inequívoca, término comprendido en el artículo 4 de la Ley Orgánica de Protección de Datos Personales, (Asamblea Nacional del Ecuador, 2021).

De la misma forma, la ingeniera Alabdan (2020) coincide en lo que se ha analizado del phishing, como una técnica de ingeniería social, que mediante el uso de diversas metodologías, tiene como objetivo influir en el objetivo del ataque de engaño para revelar información personal, mediante el envío de un correo electrónico, y así obtener nombre de usuario, contraseña o información financiera.

El phishing funciona en que los ciberdelincuentes envían correos electrónicos simulando ser instituciones legítimas y solicitan datos personales, creando enlaces que suplantan la página web, por lo que las URLs se encuentran manipuladas, redirigidas a otros portales que no son propias de las instituciones.

En la legislación penal ecuatoriana, el phishing no figura como delito, ya que comprende distintas conductas ilícitas a las establecidas en los delitos de estafa y apropiación fraudulenta por medios electrónicos correspondientes al Código Orgánico Integral Penal, la tipicidad que dispone dichas disposiciones legales no corresponden a la naturaleza del phishing, debido a que el mismo involucra una simulación visual a

través de plataformas digitales, donde el sujeto pasivo se aleja del deber objetivo de cuidado puesto que se manifiesta mediante la ingeniería social, la simulación de ser instituciones verdaderas como el Banco Pichincha, Gmail, Outlook, para obtener los datos personales a fin de usar dicha información como la divulgación, y atentar con la intimidad y privacidad de la o las personas, a más del perjuicio patrimonial.

Es importante destacar, que las instituciones financieras como el Banco Pichincha, a través del portal oficial, brinda avisos de privacidad y seguridad en las cuales recomienda no ingresar a través de los enlaces enviados por correos electrónicos; por ello, sugiere dirigir a la página oficial digitando de manera manual www.pichincha.com, verificando empezar con https:// donde la letra "s" indica que es un sitio web seguro. La entidad financiera del Banco Pichincha dispone de aviso de privacidad para canales electrónicos con el fin de proteger los datos personales de los usuarios, con la disposición de medidas técnicas, físicas y jurídicas.

A nivel internacional, los delitos financieros e informáticos, como el phishing, junto con el ransomware, son considerados como ciberdelitos de acuerdo con el informe de la Organización Internacional de Policía Criminal (INTERPOL) (2023), percibido por varios países como amenaza de categoría alta a nivel mundial de acuerdo con la encuesta resultante del sesenta por ciento (60%) de los encuestados países miembros.

Al conocer las estadísticas obtenidas de Dirección de Estadística y Sistemas de la Información de Fiscalía General del Estado, que se citan en este artículo, se puntualiza que en el año 2022 a nivel nacional el registro noticias del delito del tipo penal de apropiación fraudulenta por medios electrónicos, de un total de 3.136 casos y en el tipo penal de estafa 22.733 casos, representando el total de 25.869 noticias del delito en el país ecuatoriano. Referente al año 2023, a nivel nacional, las noticias de delitos tipo penal de apropiación fraudulenta por medios electrónicos y estafa representan 3.443 y 24.367 casos respectivamente, con un total de 27.810 casos.

En la provincia de Santo Domingo de los Tsáchilas, hay un total de 121 noticias de delito tipo penal apropiación fraudulenta por medios electrónicos y un total de 644 en casos de estafa, con una totalidad de

765 noticias de delito. En el año 2023, las noticias de delitos tipo penal de apropiación fraudulente por medios electrónicos registró 131 casos y de estafa 585, presentando un total de 716 noticias. Lo que denota que en el año 2022 se presentaron mayores noticias de estos delitos en la provincia, debido al uso continuo de plataformas digitales; sin embargo, a nivel nacional ha existido un incremento en dichos casos en el año 2023.

Por consiguiente, en materia penal, la interpretación de la ley se rige por el principio de legalidad, por lo que implica una interpretación literal, como expresa la Constitución de la República del Ecuador (Asamblea Nacional Constituyente del Ecuador, 2008) en el artículo 76 numeral 3, garantías básicas del derecho al debido proceso donde "nadie podrá ser juzgado ni sancionado por un acto u omisión, que al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza", y consecuentemente reitera, que "ni se le aplicará una sanción no prevista por la Constitución o la ley" (Asamblea Nacional Constituyente del Ecuador, 2008).

Esta garantía del debido proceso tiene concordancia con el principio de legalidad señalada en la Convención Americana sobre Derechos Humanos (Organización de los Estados Americanos, 1969) y establecida en el Código Orgánico Integral Penal (Asamblea Nacional del Ecuador 2014), artículo 5 numeral 1, "no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla", destacando que la Corte Constitucional del Ecuador enfatiza al principio de legalidad como punto limitante al poder punitivo del Estado (Corte Constitucional del Ecuador, 2023).

Si bien es cierto, el Consejo de la Unión Europea adoptó medidas para garantizar qué conductas delictivas entorno a la informática sean delitos penales en el Convenio de Budapest (2004), en el cual establece medidas legislativas necesarias para tipificar delitos en el marco nacional de cada país miembro; sin embargo, Ecuador es un país meramente observador al Convenio, cuyo proceso de ratificación aún no se ha completado, por lo que es esencial optar medidas para ratificar y adherir con este Convenio, puesto que

el vínculo de cooperación internacional y la actualización del marco legal de Ecuador en materia de ciberdelincuencia garantiza la seguridad ciudadana y la protección de los datos en el ciberespacio.

Como siguiente punto, tras entrevistar a la fiscal de la Fiscalía Especializada de Delincuencia Organizada Transnacional e Internacional (FEDOTI) de Santo Domingo considera, que ya hay ese delito, porque lo relacionan con los delitos de tipo penal de estafa y apropiación fraudulenta por medios electrónicos; sin embargo, con base a lo investigado, en materia penal, la interpretación es literal, porque la Constitución de la República del Ecuador (2008) señala en el artículo 76 numeral 3, garantías básicas del derecho al debido proceso, principio de legalidad citado anteriormente.

El Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014), en el artículo 13 refiere a la interpretación en materia penal que se realiza en sentido más ajuste a la Constitución de la República del Ecuador y los instrumentos internacionales de derechos humanos, donde los tipos penales y penas se interpretan de forma estricta, en el sentido literal de la norma.

Por otra parte, abogados expertos en derecho informático de la ciudad de Quito coinciden en que el phishing es una práctica altamente perjudicial y engañosa que representa una seria amenaza para la seguridad en línea de los usuarios. Como se ha mencionado previamente, el phishing busca no solo el perjuicio patrimonial, los ciberdelincuentes engañan a las personas para que divulguen información personal, como contraseñas, números de tarjetas de crédito o datos bancarios, lo que puede llevar a la pérdida de identidad, robo de fondos, acceso no autorizado a cuentas, afectando de forma negativa la confianza y la seguridad de los usuarios en línea. Los casos que suelen presentarse quedan simplemente a conocimiento del abogado puesto que lo más recomendable es el bloqueo al remitente del correo, a más de que los usuarios desconocen o no tienen la intención de iniciar un proceso.

Esta realidad social, que se vive a nivel mundial, de acuerdo con el abogado quien concuerda con el criterio anterior, de que el phishing tiene la posibilidad de mayor desarrollo con el auge tecnológico y la inteligencia artificial, por lo que la delincuencia organizada, experta en delitos informáticos, desarrollarían un mejor

método del mismo, destacando que se favorece de la falta de cibercultura de las personas. Además, reconoce que si bien en el Ecuador no se encuentra tipificado, generalmente dicha figura legal es vinculado a otros tipos penales.

Desde el enfoque tecnológico, el ingeniero en sistemas de informática enfatiza que el phishing es una herramienta útil para ocasionar daños, cuyos fines abarcan no solo obtener datos bancarios, sino busca también perjudicar o divulgar información de otras personas, en el cual el envío de correos electrónicos solicitando información personal genera amenaza en la protección de datos en el ciberespacio, por lo que es recomendable revisar e inspeccionar los remitentes, textos, y logos.

Reconocer la importancia del phishing para la tipificación en la legislación penal de Ecuador es necesaria, porque permite la protección a los usuarios y brinda una mayor protección a los ciudadanos y usuarios en línea al tratarse como delito especifico. Esto permite que las autoridades puedan investigar y perseguir legalmente a los perpetradores, disuadiendo así a posibles delincuentes y reduciendo la incidencia de este tipo de ataques, y la responsabilidad legal, en cuanto los autores del phishing puedan ser procesados ante la justicia de manera adecuada, asegurando que los delincuentes enfrenten las consecuencias de sus acciones y sean responsables por el daño causado a las víctimas.

Además, la relevancia recae en la prevención y disuasión, ya que la existencia de un tipo penal sirve como un elemento disuasorio para quienes planean cometer este tipo de delitos. También es elemento esencial mantener una relación o vínculo con modelos internacionales de lucha contra el cibercrimen para facilitar la cooperación con otros países en investigaciones y enjuiciamientos de casos internacionales de phishing, porque puede suceder el caso de que el ciberdelincuente se encuentre fuera del país.

Del mismo modo, el fortalecimiento de la seguridad digital que motive a empresas y organizaciones a mejorar sus medidas de seguridad en línea, ya que estarán más comprometidas a proteger a sus usuarios y clientes de posibles ataques. Como dispone la Política de Seguridad de Información, Ministerio de

Telecomunicaciones, el cual acuerda la implementación de medidas preventivas y reactivas que permitan la protección de la información enfocada en las entidades públicas.

La importancia de la tipificación del phishing conlleva a que muchas de las actividades tecnológicas que violentan cuestiones de seguridad en la red sean sancionadas, ya que los ciberdelincuentes usan formas sutiles de envío de correos electrónicos con fines de perjuicio patrimonial, violentar la intimidad y privacidad del usuario a través de la simulación visual e ingeniería social; por lo que el uso de la red, al ser una herramienta de gran utilidad para efectuar tareas cotidianas y al no encontrarse regulado en el sistema penal ecuatoriano, no es posible configurarlo al momento de realizar la persecución del delito.

CONCLUSIONES.

Al finalizar la investigación se pudo corroborar de la importancia de que se reconozca el phishing en la legislación penal de Ecuador, ya que no figura como delito, puesto que la tipicidad que disponen los delitos de estafa y apropiación fraudulenta por medios electrónicos, comprendidos en los artículos 186 y 190 del Código Orgánico Integral Penal, no corresponden explícitamente al phishing, como es el perjuicio patrimonial, ingeniería social y la simulación visual a través de plataformas digitales, simulando ser instituciones legítimas para obtener datos personales y usar dicha información. Enfatizando que en materia penal, la interpretación es literal determinada por el principio de legalidad, artículo 76 numeral 3 de la Norma Suprema.

La falta de conocimiento sobre los delitos informáticos dificulta el manejo de determinadas situaciones y riesgos a los que se exponen los usuarios frente al phishing, lo cual vulnera la intimidad y la protección de datos de carácter personal, por lo que al reconocer al phishing como delito específico brinda mayor protección a los ciudadanos, permitiendo la investigación a los posibles ciberdelincuentes y la responsabilidad legal correspondiente.

Conforme a los resultados obtenidos, se concluye que el phishing es una herramienta actual y eficaz que representa una amenaza para la seguridad de las personas, que tiene como objetivo el envío de correos

electrónicos que simulan autenticidad de instituciones legítimas, adoptando logos, textos, con el fin de obtener información como datos personales o bancarios, favoreciendo de la ingeniería social, simulación visual y falta de cibercultura; esto es, referente al entorno digital.

Finalmente, debido al auge tecnológico y el desarrollo de la tecnología, ante la presencia del phishing, se debne considerar los riesgos, por lo que es esencial generar un aporte a las ciencias jurídicas, y un precedente para investigaciones futuras, así como comprobar la dirección del remitente del correo electrónico, verificar los enlaces que contienen los mismos, siendo importante ingresar a la página oficial de la institución; así mismo, tener en cuenta el contenido, imágenes, diseño y paleta de colores de los remitentes.

REFERENCIAS BIBLIOGRÁFICAS.

1. Alabdan, R. (2020). Ataques de phishing: tipos, vectores y enfoques técnicos. Future Internet, 12, 1-39. https://www.mdpi.com/1999-5903/12/10/168
2. Alcívar, C., Tarquino, J., Blanc, G., & Duchi, B. (2016). Análisis Espacial de los Delitos y Aplicación de la Normativa Jurídica Ecuatoriana. Obtenido de Universidad Tecnológica ECOTEC: https://libros.ecotec.edu.ec/index.php/editorial/catalog/download/32/29/315-1?inline=1
3. Asamblea Nacional Constituyente del Ecuador. (2008). Constitución de la República del Ecuador. Registro Oficial N. 449. https://zone.lexis.com.ec/lts-visualizer?id=PUBLICO-CONSTITUCION_DE_LA_REPUBLICA_DEL_ECUADOR&codRO=DB5034772D272296BBEF9AEC2C929B38CB5836C5&query=%20constitucion&numParrafo=none
4. Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento N. 180. https://zone.lexis.com.ec/lts-visualizer?id=PENAL-CODIGO_ORGANICO_INTEGRAL_PENAL_COIP&codRO=CF6C511AAF5495521ABE80E34CF27C4AE35073D6&query=%20coip&numParrafo=none. Última Reforma 05 de enero de 2024

5. Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
6. Asamblea Nacional del Ecuador. (2023). Ley Orgánica para la Transformación Digital y Audiovisual. Registro Oficial Suplemento N. 245. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2023/02/7e52b3d7-0ba5-4c58-a474-00e19fcbe127.pdf
7. Banco Pichincha. (2023). Aviso de privacidad para canales electrónicos. (sitio web Banco Pichincha). Obtenido de: https://www.pichincha.com/content/published/api/v1.1/assets/CONTE8BFBA9217154E93B872D4328300BCF4/native?download=false&channelToken=712a6518832146c488cdf196228d8c00
8. Baños, L. (2022). Análisis y simulación de un ataque de phishing en el uso de un Framework Gophish en la Cooperativa de Taxis "San Fernando de Babahoyo", del 2022. Universidad Técnica de Babahoyo: http://dspace.utb.edu.ec/bitstream/handle/49000/11697/E-UTB-FAFI-SIST.INF-000003.pdf?sequence=1&isAllowed=y
9. Congreso Nacional del Ecuador. (2002). Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Registro Oficial Suplemento 557. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf
10. Congreso Nacional del Ecuador. (2004). Ley Orgánica de Transparencia y Acceso a la Información Pública. Registro Oficial Suplemento N. 337. https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf
11. Convenio sobre la Ciberdelincuencia. (2004). Convenio sobre la ciberdelincuencia de Budapest. Obtenido de Council of Europe: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

12. Corte Constitucional del Ecuador. (2023). Sentencia 1364-17-EP/23, Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic2NDhjN2U1OS03ZWVhLTQ5MzEtYTliZC1jMDllYTE0MjFiYWUucGRmJ30=y
13. Dirección de Estadística y Sistemas de la Información de Fiscalía General del Estado. (2023). Número de Noticias del delito por estafa y apropiación fraudulenta por medios electrónicos. Santo Domingo.
14. Fernández, J. (2007). Cibercrimen: Los delitos cometidos a través de Internet. España: Constitutio Criminalis Carolina.
15. Hernández, W., Osuna, C., Núnez, B., Vázquez, M. (2022). Análisis del crecimiento de phishing en los últimos años. Revista Digital de Tecnologías Informáticas y Sistemas, 6(1), 7-7. https://www.redtis.org/index.php/Redtis/article/view/132/122
16. Masaquiza, L. (2021). El phishing como delito informático en la legislación ecuatoriana. (Repositorio Institucional UNIANDES): https://dspace.uniandes.edu.ec/bitstream/123456789/13462/1/UA-DER-PDI-026-2021.pdf
17. Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador.. Obtenido de Ministerio de Telecomunicaciones y de la Sociedad de la Información: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf
18. Organización de los Estados Americanos. (1969). Convención Americana sobre Derechos Humanos. Convención Americana sobre Derechos Humanos. Organización de los Estados Americanos: https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf
19. Organización Internacional de Policía Criminal (INTERPOL). (2022). Informe Resumido sobre las tendencias de la Delincuencia a Escala Mundial - INTERPOL 2022. Obtenido de INTERPOL: https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20SP.pdf?inLanguage=esl-ES

20. Organización Internacional de Policía Criminal (INTERPOL). (2023). Informe Anual 2022. Obtenido de INTERPOL: https://www.interpol.int/es/content/download/19843/file/INTERPOL%20%20Annual%20Report%202022_SP.pdf

21. Rueda, J. (2020). Impacto de la técnica de ataque de phishing en Colombia durante los últimos cinco años. Repositorio Institucional UNAD: https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1&isAllowed=y

22. Ventura, M. (2021). La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020. (Repositorio Institucional Universidad Privada del Norte): https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

23. Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2019). Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana. Revista Ibérica de Sistemas e Tecnologias de Informação , (E17), 671-677. https://media.proquest.com/media/hms/PFT/1/sJDZ8?_s=feWuO8%2F2uO81ziahbEAGELNkO2s%3D

DATOS DE LOS AUTORES.

1. **Lisette Odalis Flores Heredia.** Abogada en libre ejercicio. Egresada de la Universidad Regional Autónoma de Los Andes, Sede Santo Domingo de los Tsáchilas, Ecuador. E-mail: ds.lisetteofh72@uniandes.edu.ec

2. **Kleber Eduardo Carrión León.** Magister en Derecho Constitucional. Docente de la Universidad Regional Autónoma de Los Andes, Sede Santo Domingo de los Tsáchilas, Ecuador. E-mail: us.klebercarrion@uniandes.edu.ec

3. **Joselyn Gabriela Rivera Velasco.** Estudiante de la Universidad Regional Autónoma de Los Andes, Sede Santo Domingo de los Tsáchilas, Ecuador. E-mail: joselyngrv12@uniandes.edu.ec

RECIBIDO: 30 de septiembre del 2024. **APROBADO:** 28 de octubre del 2024.