UNIVERSIDAD DE OTAVALO

PROGRAMA DE MAESTRÍA EN DERECHO PENAL
MENCIÓN DERECHO PROCESAL PENAL

TRABAJO DE TITULACIÓN

LOS CIBERDELITOS BANCARIOS Y SU INSUFICIENTE LEGISLACIÓN EN EL ECUADOR CON LA SEGURIDAD FINANCIERA

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
MAGÍSTER EN DERECHO PENAL
MENCIÓN DERECHO PROCESAL PENAL

HERNÁN PATRICIO ROSERO GONZÁLEZ

TUTOR: MSc. RODRIGO DURANGO CORDERO

Otavalo, febrero, 2024

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

DECLARACIÓN DE AUTORÍA

Yo, Hernán Patricio Rosero González, declaro que este trabajo de titulación es de mi total autoría y que no ha sido previamente presentado para grado alguno o calificación profesional. Así mismo declaro que dicho trabajo no infringe el derecho de autor de terceros, asumiendo como autor la responsabilidad de las reclamaciones que pudieran presentarse por esta causa y liberando a la Universidad de cualquier responsabilidad al respecto.

Que de conformidad con el artículo 114 del Código Orgánico de la Economía Social, conocimientos, creatividad e innovación, concedo a favor de la Universidad de Otavalo licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra con fines académicos, conservando a mi favor los derechos de autoría según lo establece la normativa de referencia.

Se autoriza además a la Universidad de Otavalo para la digitalización de este trabajo y posterior publicación en el repositorio digital de la institución, de acuerdo a lo establecido en el artículo 144 de la ley Orgánica de Educación Superior. Por lo anteriormente declarado, la Universidad de Otavalo puede hacer uso de los derechos correspondientes otorgados, por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Firmado electrónicamente por:
HERNAN PATRICIO
ROSERO GONZALEZ

_____

HERNÁN PATRICIO ROSERO GONZÁLEZ

C.C. 1204638603

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

CERTIFICACIÓN DEL TUTOR

Certifico que el trabajo de investigación titulado" LOS CIBERDELITOS BANCARIOS Y SU INSUFICIENTE LEGISLACIÓN EN EL ECUADOR CON LA SEGURIDAD FINANCIERA" bajo mi dirección y supervisión, para aspirar al título de Magíster en Derecho Penal, mención Derecho Procesal Penal, del estudiante Hernán Patricio Rosero González, cumple con las condiciones requeridas por el programa de maestría.

Firmado electrónicamente por:
RODRIGO FRANCISCO DURANGO CORDERO

_____

RODRIGO FRANCISCO DURANGO CORDERO
CC. 1711087831

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

DEDICATORIA

Este trabajo investigativo lo dedico a mis padres; Cap. Aviac. Hernán Bayardo Rosero Rosero, por ser el ejemplo en casa que dio a sus hijos trabajando, también a mi señora madre Jenny Patricia González Pozo por su cariño incondicional. A mi hermana Karla Berenice Rosero González.

A quienes han sido parte fundamental de toda mi educación aportando significativamente con un granito de arena para que se cumpla con el objetivo y aprender algo que va a servir profesionalmente en el futuro. A ellos con mucho cariño dedicamos este esfuerzo.

Hernán Patricio Rosero González

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

AGRADECIMIENTOS

En primer lugar, agradecer a Jehová Dios por darme todas las facultades necesarias para cumplir con esta meta tan anhelada. A mi familia por el apoyo económico y el aporte anímico. De todo corazón les agradezco.

También a la Universidad de Otavalo por permitirme ser parte de su institución en calidad de alumno. Y agradecido con la modalidad en línea que se implementó, por lo que nos dio la comodidad de estudiar desde el hogar y precautelar nuestra salud por la pandemia.

Al Mgs. Rodrigo Durango, quien fue mi tutor, el cual aporto con críticas constructivas para el desarrollo de este articulo profesional. De igual manera, al tribunal de defensa de la maestría de Derecho Procesal Penal por sus consideraciones.

Agradecerles a todos los compañeros que mediante sus comentarios nutrieron las clases a través de sus experiencias, y sin egoísmo compartían y explicaban a los de menos experiencia.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

1. TÍTULO DEL ARTÍCULO PROFESIONAL DE ALTO NIVEL

LOS CIBERDELITOS BANCARIOS Y SU INSUFICIENTE LEGISLACIÓN EN EL ECUADOR CON LA SEGURIDAD FINANCIERA

BANKING CYBERCRIMES AND ITS INSUFFICIENT LEGISLATION IN ECUADOR WITH FINANCIAL SECURITY

2. AUTOR Y TUTOR

2.1. AUTOR

Ab. Hernán Patricio Rosero González*

*Maestrante en Derecho Penal, mención Derecho Procesal Penal por la Universidad de Otavalo
Correo:

ep_hprosero@uotavalo.edu.ec

2.2. TUTOR

Dr. Rodrigo Francisco Durango Cordero
Tutor

3.- RESUMEN

El presente artículo profesional describe los diferentes tipos de ciberdelitos bancarios desde el punto de vista del derecho comparado y su creciente frecuencia en el Ecuador, con el propósito de determinar si en la legislación ecuatoriana se encuentran normas inherentes a las clases de ciberdelitos o en su defecto si se ha regulado para no dejarlos en la impunidad. Pese a existir organizaciones internacionales destinadas a la identificación de estas conductas ilícitas, en el Ecuador no se encuentran descritas por un correcto verbo rector propiamente dicho, tipificándolo en otras categorías que no corresponden. La metodología utilizada fue una investigación documental y descriptiva; a través de la investigación exhaustiva de múltiples documentos nacionales e internacionales que tratan el tema; y de campo, sin dejar de lado la técnica de observación científica con el caso específico del país. Los resultados obtenidos indican que el Ecuador requiere con brevedad de una legislación que permita proteger a sus ciudadanos de los crecientes ciberdelitos bancarios, así como también de la implementación educativa y cultural en instituciones educativas y en la sociedad en general. La conclusión más destacada ha sido que el Ecuador tiene una insuficiente legislación al respecto; tratándolo en su mayoría como un delito de estafa, lo cual no resulta pertinente por varios argumentos legales.

Palabras clave: ciberdelito, ciberespacio, ciberdelincuencia, banca virtual, legislación.

4.- ABSTRACT

This professional article describes what are the banking cybercrimes from the point of view of comparative law and its constantly increasing frequency in Ecuador, with the purpose of determining if in the Ecuadorian legislation there are norms inherent to the classes of cybercrimes or in their defect if it has been regulated so as not to leave them unpunished. Despite the existence of international organizations dedicated to the identification of these illegal conducts, in Ecuador they are not described by a correct governing verb itself, typifying it in other categories that do not correspond. The methodology used was a documentary investigation with a qualitative focus; through the exhaustive investigation of multiple national and international documents that deal with the subject; and field, without neglecting the technique of scientific observation with the specific case of the country. The results obtained indicate that Ecuador soon requires legislation to protect its citizens from increasing banking cybercrime, as well as educational and cultural implementation in educational institutions and in society in general. The most outstanding conclusion has been that Ecuador has insufficient legislation in this regard; treating it mostly as a crime of fraud, which is not relevant for various legal arguments.

Keywords: cybercrime, cyberspace, cyberdelinquency, virtual banking, legislation.

5.- INTRODUCCIÓN

Hoy en día la facilidad de los usuarios de contar con una aplicación de banca en línea donde pueda acceder desde su móvil o computadora a realizar pagos, transferencias a nivel nacional e internacional y revisar sus movimientos bancarios sin la necesidad de trasladarse a la institución financiera ha traído consigo comodidad para el usuario y rapidez en los trámites; sin embargo, implica también una serie de problemas que los pueden afectar económica y hasta legalmente, siendo víctima de delitos cibernéticos.

En el derecho internacional existe la identificación de varios ciberdelitos de acuerdo a su tipología y por los diferentes modos de cometer esta infracción penal. Dentro de estos se encuentran los ciberdelitos de especialidad bancaria que se consumen mediante el uso de engaños cibernéticos que afectan al bien protegido como por ejemplo la propiedad. Por esto, la presente investigación busca aportar información desde el derecho comparado consecuentemente con el derecho de organizaciones internacionales.

En primer lugar, se han estudiado los aspectos más controvertidos en cuanto a la clasificación de los ciberdelitos. Así mismo, se indicarán los métodos y técnicas que utilizan los ciberdelincuentes y como combaten las diferentes legislaciones internacionales con este problema global desde la detección, investigación, y prevención de estos delitos. En segundo lugar, se revisarán cada uno de los artículos del Código Orgánico Integral Penal (COIP) que más se asemejan a los ciberdelitos bancarios en la legislación ecuatoriana. Y, en tercer lugar, se analizará la sentencia dentro del Juicio No. 09286-2014-6178.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

6.- METODOLOGÍA

Según el nivel de profundización, la presente investigación es descriptiva, ya que busca relatar los diferentes aspectos del delito cibernético. Arias (2012), lo define como: "la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento." (p.22). En el presente artículo se representan la clasificación de este tipo de delito, así como también el *modus operandi*, la frecuencia de los mismos y la regularización internacional y nacional del tema.

Asimismo, la presente investigación adopta un enfoque cualitativo, buscando comprender y analizar los fenómenos relacionados con los ciberdelitos bancarios y la insuficiente legislación en Ecuador. Este enfoque se orienta hacia la descripción e interpretación de la estructura y comportamiento de estos delitos, más allá de las estadísticas, profundizando en sus motivaciones y contextos específicos.

Según el manejo de los datos, el presente artículo se clasifica como una investigación mixta. Rus (2020), define como aquella que une los métodos cualitativos y cuantitativos, con el fin de disponer de las ventajas de ambos y minimizar sus inconvenientes. Precisamente, se hacen los análisis específicos a partir del apoyo de estadísticas internacionales. En cuanto a la modalidad, se clasifica como no experimental, lo que implica que la investigación se realiza sin intervenciones controladas. Se observa y describe la realidad existente, sin manipulación directa por parte del investigador. Esto permite abordar de manera más fiel y contextualizada el tema de los ciberdelitos bancarios en el entorno ecuatoriano (Arias, 2012).

A tales efectos, la estrategia utilizada respecto al diseño de la investigación es, en primer lugar, documental. Arias (2012) define como:

> La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresos, audiovisuales o electrónicos. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos. (p.27)

A tales efectos, este proceso se realizó con el objetivo de recopilar información sustancial que contribuya a una comprensión integral del tema bajo investigación. Es crucial destacar la importancia del Código Orgánico Integral Penal (COIP, 2023) en este contexto, ya que, si bien aborda normativas penales nacionales relacionadas únicamente con los delitos contra la seguridad de los activos de los sistemas de información y comunicación, no incluye disposiciones específicas sobre delitos cibernéticos bancarios. En este sentido, se hace imperativa una investigación minuciosa y profunda con el propósito de desarrollar una normativa que aborde adecuadamente esta área específica.

En segundo lugar, la investigación es de campo, Arias (2012) define como:

> La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

investigador obtiene la información, pero no altera las condiciones existentes. (p.31)

En el caso objeto de estudio, la investigación es de campo con el estudio de caso específico de Ecuador, ya que el tema describe con amplitud la realidad legal ecuatoriana respecto a los ciberdelitos bancarios con datos obtenidos a través de la técnica de observación, Sabino (2017) define como: "la observación científica consiste en el uso sistemático de nuestros sentidos en la búsqueda de los datos que se necesitan para resolver un problema de investigación" (p.38)

Asimismo, la técnica principal utilizada es el análisis documental, basado en la búsqueda, recuperación, procesamiento y crítica de datos secundarios provenientes de fuentes como leyes, doctrina, informes, jurisprudencia y otros documentos relacionados con la legislación y los casos de ciberdelitos bancarios en Ecuador. Esta técnica contribuye a la caracterización y comprensión detallada del fenómeno. Del mismo modo, se emplea la técnica de estudio de caso, enfocándose específicamente en el contexto legal ecuatoriano. Este enfoque implica una investigación profunda y detallada sobre el fenómeno, utilizando datos obtenidos directamente de la realidad, sin intervención directa del investigador (Baena, 2019).

7.- LOS CIBERDELITOS BANCARIOS Y SU INSUFICIENTE LEGISLACIÓN EN EL ECUADOR CON LA SEGURIDAD FINANCIERA

La identificación y descripción de estos ciberdelitos es una labor llevada a cabo por diferentes organismos internacionales como la ONU, la UE, la OTAN, INTERPOL, OEDI, UIT, FELABAN, y a nivel nacional ASOBANCA, quienes se han visto obligados a adaptar sus legislaciones y estandarizar la identificación y descripción de ciberdelitos. Otra institución que se manifiesta al respecto es la Unión Internacional de Telecomunicaciones (UIT), es un ente regulador que corresponde a la Organización de las Naciones Unidas, y como tal tiene entre sus competencias principales, regular la reglamentación entorno al ciberdelito y sus respectivas estadísticas. Además, el FBI (2022) también ha desarrollado informes en esta área; tanto en su forma de ejecutarse como el aumento en diferentes áreas.

En 2001, el Consejo de Europa creó el Convenio de Budapest sobre Ciberdelincuencia. Es un tratado internacional con el objetivo de aumentar la cooperación entre diferentes países del mundo y crear marcos legales armónicos entre países y hacer frente a los delitos informáticos y a la actividad criminal en internet (Consejo de Europa, 2001).

Por su parte, en Ecuador, según ha manifestado la Dirección de Política Criminal de la Fiscalía General del Estado desde agosto 2014 hasta mayo 2015, reconoció 626 denuncias por delitos informáticos. Y en el 2021, la cifra aumentó a 1851 denuncias. Según el fiscal provincial de Pichincha, Wilson Toainga, las investigaciones concernientes a los delitos informáticos se realizan de forma técnica y conlleva mucho tiempo para establecer la responsabilidad de aquellos que trasgreden la ley sentados frente a un monitor. Así mismo, el fiscal Edwin Pérez, especialista en infracciones informáticas, indicó que en Ecuador existen dificultades durante la investigación de delitos atenuados por el uso de la tecnología, debido a que la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país (Fiscalía General del Estado, 2015).

De allí que, el tema abordado en este estudio requiere una comprensión profunda de la realidad nacional y la legislación penal ecuatoriana. Es imperativo conocer estos aspectos

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

para implementar las correcciones necesarias, asegurando así la realización de investigaciones efectivas y la contención de este delito moderno que avanza de manera acelerada.

7.1.- Clasificación de los Ciberdelitos

7.1.1.- Phishing

Este ciberdelito es identificado principalmente dentro del derecho inglés y posteriormente estudiado y aplicado en Europa, pero no identificado exactamente en el Código Orgánico Integral Penal (COIP), ya que el mismo ha sido causa de muchas reformas, pero poco tratado en el ámbito de los ciberdelitos bancarios. Sampedro (2022), lo define como:

> Este término phishing proviene de los vocablos en inglés *password, harvesting y fishing*, que hace alusión a "cosecha y pesca de contraseñas". Justamente este delito persigue apropiarse de datos confidenciales de los usuarios para, en base a ellos, conseguir menoscabar patrimonios ajenos. (p. 1)

Este ciberdelito bancario funciona con envío de correos electrónicos, similar al de una entidad bancaria, en la que contiene espacios en blanco con el fin de que el usuario complete con: claves de acceso, números de tarjetas de crédito y débito, direcciones físicas y electrónicas, o direcciones de trabajo y domicilio, nombres completos, números de cédula de ciudadanía, y otros datos que ayuden con la información financiera. De esta manera, Fernández (2013) destaca que el ciberdelincuente adquiere información personal de la víctima la cual no se percata de que ha entregado su información a una persona ajena a la institución bancaria. Aunque el origen de este delito data de la década de los noventa, ha ido evolucionando junto con la tecnología y la sociedad, llegando actualmente a redes sociales.

Además, es conocido también de forma universal como *spam* o correo basura, radica principalmente en el envío de correos a un gran número de usuarios con el objetivo de perjudicar a quien lo recibe. Este *spam* actúa como medio de transporte del *phishing*; principalmente en mensajes publicitarios enviados de forma masiva procedente de personas desconocidas que venden un servicio o producto fraudulento.

El *phishing* es un tipo de cibercrimen de réplica, significa que se replican páginas bancarias. Son de los más comunes ya que utilizan fraudes de tarjetas de crédito, cheques, estafas de inversión piramidales, de lotería, ventas online defraudatorias, y ofertas fraudulentas. Este tiene una gran cantidad de definiciones erróneas que se encuentran en muchas páginas oficiales de bancos, organizaciones e inclusive en artículos o revistas de investigación. Como, por ejemplo, ASOBANCA (2022) define: "Aunque el correo electrónico es el medio más usado por los ciberdelincuentes para este tipo de fraudes, el phishing puede utilizar otros medios, como los SMS, mensajes por WhatsApp, Facebook y otras redes sociales" (pág.2).

Lo cierto es que el *Phishing* solo actúa a través de correos electrónicos y los ya mencionados *spams* (propagandas falsas). Además, en lo más reciente, figuran las redes sociales como medio preparatorio para sacar información del usuario y no por mensajes de texto (SMS), ni por mensajes de *whatsApp*, esto corresponde a otro tipo de delito que se verá más adelante.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

En consecuencia, lo que más llama la atención en las páginas oficiales de diferentes bancos nacionales es que, dicha definición no cuenta con sustento jurídico, nada más, una breve explicación para prevenir a sus clientes con el correcto uso de claves, lo que hace en muchos casos que su descripción se encuentre errónea. Esto pese a existir una nueva reforma normativa con fecha 11 de octubre 2022, sobre políticas institucionales para el Sistema de Gestión de Seguridad de la Información (2020)., cuya misión es dirigir y administrar procedimientos en materia de seguridad de la información estableciendo mecanismos y ejecutando controles para su cumplimiento contribuyendo al desarrollo de los procesos que se desarrollan en la Corporación Financiera Nacional (CFN).

La vinculación poco clara y comprensible de los ciberdelitos con el delito de estafa, como se presenta en el COIP (2023), que se limita a describir un acto perjudicial para el patrimonio de una persona o tercera Entidad, dificulta la obtención de una definición precisa. Esta carencia abarca las diversas tipologías, características, sujetos y bienes jurídicos protegidos involucrados en estos delitos cibernéticos. Por lo tanto, se hace necesaria una investigación profesional para proponer una clasificación detallada y una descripción exhaustiva de estos nuevos tipos penales.

El Observatorio Español de Delitos Informáticos (OEDI) desempeña un papel crucial en la definición y análisis de diversos ciberdelitos que aún no han sido debidamente tipificados. Sus informes, que incluyen estadísticas anuales, son de especial relevancia para esta investigación. Estos documentos no solo contribuyen a una regulación más eficaz del delito, sino que también ofrecen valiosas recomendaciones de acciones legislativas para los estados, orientadas a prevenir la comisión de estos delitos.

En la legislación española, éste se encuentra de manera general como delito de fraude informático, pese a que ya se ha dictado sentencias en el caso del *phishing*. Estadísticamente estos ciberdelitos se encuentran en aumento, lo que hace posible su análisis desde la posición de organizaciones internacionales, hasta empresas y profesionales de la ingeniería en sistemas cuyas páginas web son dedicadas al estudio de estos casos.

En el caso de América Latina y el Caribe, los riesgos informáticos más relevantes que se presentaron en la banca fueron la clonación de tarjetas, la suplantación de identidad en compras no presenciales y el *phishing*. Estos criminales cibernéticos ampliaron su operación en la región al percatarse de la fragilidad de las infraestructuras y de la respuesta reactiva por parte de las entidades bancarias. Como consecuencia, los esfuerzos preventivos eran insuficientes (Organización de los Estados Americanos, 2018).

Según datos de la Organización Internacional de Policía Criminal (INTERPOL) (2020), la práctica de phishing experimentó un marcado aumento durante la pandemia, impulsado por la elevada demanda de mascarillas quirúrgicas y otros productos médicos. La dificultad para encontrar estos artículos en tiendas físicas llevó a la proliferación en línea de diversas tiendas, sitios web, cuentas de redes sociales y direcciones de correo electrónico falsos que aseguraban ofrecer estos productos, pero en realidad tenían como único propósito el robo de dinero.

De aquello, se desprende con claridad meridiana que aún no existe una legislación en este sentido que norme y sancione, aún a sabiendas que con la tecnología avanzada seguirán apareciendo nuevos ilícitos bancarios. Por lo mismo, es de trascendental importancia que, tanto a nivel internacional y nacional, se legisle en pro de contrarrestar esas

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

ilicitudes, poner precedentes jurisprudenciales y establecer sanciones drásticas desde luego con cooperación y asistencia penal internacional.

La diferencia de los ciberdelitos con los delitos tradicionales es que requiere de implementación y nuevos modelos de investigación para condenar esta conducta, lo que hace más compleja su investigación y la prueba. Resulta totalmente ilógico que un ciberdelito bancario utilice prueba física debido a que el ciberdelincuente en muchas ocasiones no se encuentra dentro del territorio que se está investigando, lo que hace necesario la cooperación internacional. Por esto y más, no se puede comparar con los delitos tradiciones como el de suplantación de identidad o la estafa ya que estos no son ciberdelitos.

De acuerdo con lo registrado, se deduce que, tanto en la perpetración de delitos a nivel internacional como nacional, estos son llevados a cabo por redes que operan desde otros países, con la participación de bandas u organizaciones especializadas en informática. Dado que estas actividades provienen del extranjero hacia el ámbito nacional, resulta prácticamente imposible establecer un proceso penal que tome en consideración tanto la jurisdicción como la competencia legal, elementos fundamentales para sancionar la comisión de cualquier ilícito.

7.1.2.- *Smishing*

Otro ciberdelito bancario a considerar es el *smishing*; consiste en que la víctima recibe un mensaje de texto manifestando que son acreedoras de algún premio, sorteo, concurso, o suma de dinero, para luego obtener información privada de sus cuentas. Este método puede ser únicamente a través de mensajería instantánea como la aplicación *whatsApp* o simplemente por la línea celular de mensajería, con el propósito de que el sujeto activo contacte al sujeto pasivo quien es la víctima y se comunique mediante mensajes de texto a un número determinado (Ventura, 2021).

Según el Instituto Nacional de Ciberseguridad (2021) "El nombre de este ciberdelito hace énfasis en sus abreviaturas de mensajes de texto, también conocidos como SMS, estos mensajes son del mismo modo que el phishing por eso la combinación de Smishing". Estos mensajes enviados por ciberdelincuentes buscar de alguna manera astuta obtener información bancaria, pueden enviar enlaces para suscribirnos a una página o recomendar la instalación de un programa, pero con la limitante que los mensajes de texto ocultan la identidad propia de la persona.

A manera de ejemplo se encuentra otra negligencia inherente a este delito internacional, esta vez del Banco Santander de España, de la cual se reseña lo siguiente:

> Un caso judicializado con fecha de sentencia; 24 de mayo de 2022, reconoce que el Banco Santander tendrá que devolver los 18.500€ sustraídos desde Lituania a su cliente. Esta estafa se realizó con el método del SMS en el que se alertaba al cliente de un problema de seguridad y que debía restablecer su contraseña accediendo al enlace que se le proporcionaba. Al proporcionar las claves al estafador que procedió a realizar dos operaciones de transferencia por un total de 18.500€ desde Lituania. (El Mundo, 2022)

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Cabe señalar que este caso se califica como smishing sin embargo la página en la cual se cita lo identifican erróneamente como phishing. Lo que evidencia que los conceptos en cuanto a ciberdelitos bancarios no están claros. El objetivo de estas sentencias en materia de ciberdelincuencia debería ser materia de análisis. Por lo que la responsabilidad penal es compartida por la falta de negligencia del usuario al no conocer estos nuevos casos de delitos. Y por otro lado la entidad se ve obligada a crear mecanismos de seguridad en casos de no contar con sustento jurídico que posiblemente no sea negligentes y sea un complot.

Al respecto, Ortiz (2022) expresa:

> Hay sentencias que hablan de la responsabilidad de las entidades bancarias cuando el engaño viene por enlaces facilitados por vía email o SMS. Entre otras, cabe mencionar la Sentencia de la Audiencia Provincial de Ciudad Real, de 20 de mayo de 2021 (nº rec. 528/2019), en la cual se establece que la entidad bancaria debe emplear mayor cuidado cuando la orden de transferencia tiene su origen en un enlace obtenido por vía email o fax dado el riesgo inherente que conllevan dichas formas de comunicación. (para. 9)

El presente fallo judicial internacional da a entender que las entidades bancarias deben poseer directrices y un sistema informático muy seguro al momento de realizar transferencias de dineros de cuenta ahorristas, para que una vez cerciorados bien y verificado la pertenencia y licitud efectivamente se realice transferencia dineraria alguna caso contrario ya se alertaría y se evitaría estas ilegalidades, lo que conllevaría a la no afectación del peculio personal del dueño de la cuenta bancaria.

Establecer prácticas seguras al compartir información personal es esencial para prevenir el delito. Una estrategia clave consiste en evitar la divulgación de datos a través de mensajes de texto, optando en su lugar por comunicarse directamente con la entidad solicitante con la debida precaución. En caso de persistencia en mensajes no deseados, es posible tomar medidas como reportar o bloquear el contacto en cuestión. Aunque algunas páginas de instituciones financieras implementan medidas de seguridad, se observa la necesidad de promover políticas públicas que promuevan la conciencia sobre la importancia de resguardar la información personal (Lorite, 2021).

7.1.3.- **Vishing**

El término *vishing* hace referencia a la voz humana como medio principal en la llamada telefónica. El objetivo sigue siendo la obtención de información delicada que podría usarse para el robo de identidad, obtener beneficios financieros o apoderarse de cuentas (Fiscalía General de la Nación (Colombia), 2019). El *modus operandi* consta de dos partes, en primer lugar, el delincuente ha obtenido previamente información de la víctima, como sus datos personales, correo electrónico, dirección, entre otros; segundo lugar, se hace la llamada telefónica en el que se hace pasar por la entidad financiera, una empresa de mensajería o un servicio técnico para que la víctima confíe en él y conseguir que éste instale alguna aplicación o realice algún pago.

Un claro ejemplo de cómo actúan este ciberdelito es cuando las bandas cibernéticas realizan llamadas telefónicas a través de un mensaje alarmista al usuario desde un aparente *call center* del banco, donde el cliente mantiene su cuenta, siendo así que comunican al

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

usuario que ha sufrido un desfalco y transfieren la llamada a un supuesto ejecutivo bancario que continúa el juego. El usuario al ver la urgencia y al estar en una situación de angustia, proporciona sus datos, por lo que el sujeto activo tiene la oportunidad de cometer este acto ilícito.

Estas llamadas pueden ser hechas por números del propio país de residencia, pero esos números en algunas ocasiones no son del mismo país ya que se puede tratar de ciberdelincuente que se encuentran en otra parte del mundo y que tienen una línea telefónica nacional sin percatarse de donde realmente procede.

La plataforma digital del Ministerio Público del Perú comparte una publicación del diario El Peruano (2022), misma que indica:

> La Fiscalía de Ciberdelincuencia de Lima, consiguió que el Poder Judicial dictara sentencia en terminación anticipada por delito de estafa agravada en la modalidad conocida como "vishing". La pena contenida en el artículo 196°-A del Código Penal inciso 5 fue declarada contra Carmen Anita Berna Polinar, quien fue sentenciada a 3 años y 9 meses de libertad suspendida. Además, deberá cumplir reglas de conducta y el pago de una reparación civil a favor de la agraviada por el monto de S/3 300.00 soles y 85 días multa. (para. 1)

De la lectura de este fallo dentro de la legislación peruana el Ministerio Público identifica ya en el sistema de justicia este ciberdelito de vishing, por lo mismo el fallo contiene la dogmática penal ya que interpreta gramaticalmente a este ciberdelito por su medio comisivo, siendo esto poco visto dentro del presente estudio puesto que las diferentes legislaciones confunden estos tipos penales.

La lucha contra este ciberdelito se ve fortalecida al comprender su modalidad, lo cual destaca la importancia de tipificarlo y difundir ese conocimiento entre la población. Es crucial instar a la ciudadanía a tomar medidas proactivas, como verificar la autenticidad de las llamadas y, en caso de duda, desplazarse personalmente a la institución correspondiente. Por ejemplo, ante una solicitud urgente de información por parte de alguien que asegura ser del banco, se aconseja a los clientes finalizar la llamada si surge alguna duda, ya que las entidades financieras están al tanto de las tácticas empleadas por los ciberdelincuentes y no solicitan datos personales por teléfono, donde la información podría ser interceptada (Lorite, 2021).

En algunos casos, cuando se reciben llamadas telefónicas de alguna operadora de planes o institución, aparece el nombre sin la necesidad de tener registrado como contacto, esto se ha establecido como consecuencia del *vishing*. No obstante, la manera más segura si no se cuenta con el tiempo suficiente para ir hacia el banco, se puede realizar una llamada al número oficial que se encuentra en la página web del banco para verificar si se trata de este ciberdelito.

7.1.4.- *Pharming*

Este ciberdelito, además de tener como objetivo la recolección de datos, agrega el secuestro de datos mediante un malware que infecta la computadora a través de una serie de virus, lo cual impide que el usuario tenga acceso a sus archivos hasta que realice un pago. El primer lugar, un hacker instala en la computadora un virus que cambia los archivos a un

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

sitio *web* falso. En segundo lugar, el usuario puede estar visitando un sitio *web* falso sin percatarse de ello (Oxman, 2013).

Según Rodríguez (2016), en este tipo de delito los ciberdelincuentes se apropian de claves en equipos donde tiene bajos niveles de seguridad. Estos virus pueden infectar, por así decirlo, a la computadora *tablet* o teléfono celular al descargar de manera gratui*ta software*, películas o música que llegan a ofrecer al correo electrónico y sin pagar las licencias legales. Para que esto no ocurra es recomendable que los usuarios tengan sus equipos electrónicos con todas las licencias actuales y legales para no caer en este ciberdelito.

El *pharming* como ciberdelito bancario es el más complicado describir por los términos técnicos y los diferentes medios de ataque que tiene los cibercriminales, envían virus, remplazan números de identificación IP de cada dispositivo o modificar software. Requiere de *hackers* expertos por su complejidad a diferencia de los otros ciberdelitos. Su base primordial es dirigir al usuario a páginas web propias del ciberdelincuente que pueden ser similares a una entidad bancaria para acceder a información financiera.

Su comportamiento va desde suplantación de identidad, secuestro, robo de información o dinero, estafa, acceso no consentido a sistemas informáticos, adulteración de páginas financieras y en fin una gran variedad de verbos rectores y delitos. Estos delitos superan a los demás, pero para recurrir a su disminución necesitamos recurrir a la educción para prevenir su incremento.

En Ecuador la normativa sobre Política de Seguridad de la Información (2022) considera que el concepto de "Malware" o software malicioso abarca un espectro amplio, englobando cualquier programa o código con intenciones perjudiciales para los sistemas. Pero esta definición está dentro del ciberdelito llamado *pharming*, por lo que la ausencia de legislación en el sistema ecuatoriano se debe a que aún no se tienen claro los diferentes métodos del *pharming* y las políticas públicas por parte del Estado no incentivan al estudio de las ciberseguridades y a los ciberdelitos bancarios por lo que incrementa la vulnerabilidad a los usuarios de la banca.

En este orden de ideas, la actividad delictiva en el ámbito cibernético se ha consolidado como una de las empresas ilícitas más rentables a nivel global, alcanzando un estimado de 6 billones de dólares en costos durante el año 2021. Las proyecciones indican que para el año 2025, se anticipa un aumento significativo en las pérdidas, llegando a aproximadamente 10,5 billones de dólares en todo el mundo (Dirección General de Comunicación Social, 2022). Por tal motivo, resulta necesario que en el Ecuador se pueda contar con la tipificación de los actos ilícitos que perjudican la seguridad económica de las personas

En el medio nacional no se cuenta con cursos que capaciten en la importancia de las seguridades tecnológicas, dejando en total indefensión al usuario de la banca por lo que la entidad encargada en este caso es el Sistema Nacional de Datos Públicos (SINARDAP), debería implementar cursos gratuitos al ser el organismo estatal de protección de datos, con la finalidad de prevenir ilícitos cibernéticos.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Cabe mencionar que los ciberdelitos vienen siendo objeto de análisis y estudios frecuentes, es así que una empresa americana en *sofware* hace referencia a la falta de competencias en ciberseguridad a nivel internacional, mencionando lo siguiente:

> La escasez mundial de talento cualificado en ciberseguridad agrava la tarea ya difícil de proteger contra el volumen creciente de amenazas avanzadas y sofisticadas. El CSIS (del inglés, Center for Strategic and International Studies, Centro de estudios estratégicos e internacionales) ha realizado un estudio para cuantificar la escasez de profesionales especializados en ciberseguridad en ocho países (Alemania, Australia, Estados Unidos, Francia, Israel, Japón, México y Reino Unido). Se ha encuestado a los responsables de la toma de decisiones (TI), tanto del sector público como del sector privado, en relación a cuatro áreas clave del desarrollo de la plantilla en el ámbito de la ciberseguridad: gasto en seguridad, programas de formación, estrategias del empleador y políticas públicas. (McAfee,2016, p 1)

Esto conlleva a entender que a nivel de todo el mundo aún no existe grupo humano experto en un cien por ciento en materia de ciberseguridad constituyendo una gran preocupación mundial, alertando a que tantos gobiernos, sectores públicos y privados deben invertir presupuestos para programas de prevención y seguridad.

7.2.- Estado de la cuestión sobre los ciberdelitos bancarios en el Ecuador

7.2.1.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

La Constitución protege el uso abusivo de acceder sin consentimiento a los sistemas personales para luego obtener información de cuentas bancarias o para directamente vulnerar el sistema. Esto, sobre la base del Art. 16 de la Constitución de la República del Ecuador (2008) cuando menciona que: "Toda persona tiene derecho de forma individual o colectiva del acceso universal a las tecnologías de información y comunicación" (p. 22).

Este delito amenaza gravemente a la economía del país al igual que los ciberdelitos bancarios, al modificar un portal *web*, desviar o redireccionar el tráfico de datos, trae consigo serios problemas económicos para los usuarios y empresas. Al no garantizar adecuadamente el uso de sistemas informáticos de comunicación con instituciones jurídicas adecuadas no se está fomentado la pluralidad y la diversidad en la comunicación a la sociedad.

Estas actividades ilícitas tienen diferentes conductas penales, pero están entrelazados con los ciberdelitos bancarios por lo que utilizan aparatos electrónicos para acceder sistemas informáticos confidenciales. En tal razón, el estudio de varios países con legislaciones más avanzadas y especificas dan confianza a los usuarios de las comunicaciones, gracias a las leyes específicas que los amparan.

El establecimiento de normativas apropiadas se convierte en un componente esencial del marco jurídico requerido para abordar las conductas emergentes. En este contexto, incumbe al Estado reforzar tanto los medios de comunicación públicos como los privados, con el propósito de asegurar otro derecho fundamental, como es el derecho al buen vivir. Esto implica garantizar que todos los individuos gocen de la certeza de un acceso universal a las tecnologías de la información y comunicación, facilitando así la realización de actividades cotidianas, entre las cuales se incluye el uso de plataformas bancarias.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

7.2.2. Apropiación fraudulenta por medios electrónicos

Este delito se encuentra en el COIP (2023), al respecto el Art. 190, indica que:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicación para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en prejuicio 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 telecomunicación, será sancionada con pena privativa de libertad de uno a tres años. (p.83)

En su inciso primero refiere además que: la misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimientos o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadoras, utilización de controles o instrumentos de apertura a distancia, violación de seguridades electrónicas, informáticas u otras semejantes.

Este delito antes referido reviste una similitud con todos los delitos informáticos y por ende los ciberdelitos bancarios por su conducta penalmente relevante, sin embargo, la falta de claridad y comprensión del contenido, deja entrever que es imperioso la necesidad de normatizar y reformar normas que incluyan a los ciberdelitos en la legislación ecuatoriana. En lo que tiene que ver con transferencias electrónicas del activo patrimonial, el Art. 231 del COIP (2023) indica que:

> La persona que, con ánimo de lucro, altere, manipule, o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. (p.99)

Además, refiere la norma legal antes citada que con igual pena será sancionada la persona que suministre datos de su cuenta bancaria con la intención de obtener, recibir o atraer de forma ilegítima un activo patrimonial a través de una transferencia electrónica consecuencia de este delito para sí mismo o para otra persona.

De aquello se desprende que dicho marco normativo no se encuentra actualizado ni profundizado por lo que muchos delitos informáticos tienen similitud, lo que hace que se llegue a una confusión y por ende no se tenga claras reglas legales para frenar y contrarrestar este tipo de delitos, debido a su ineficiente etapa probatoria dentro de la investigación.

7.2.3.- Estafa

En el COIP (2023) encontramos en el Art. 186, inciso primero numeral 1, respecto al delito de estafa reformado por el Art. 2 de la Ley s/n R.O. 598- 3S, 30-IX-2015; y reformado por el art. 42 de la Ley s/n R.O. 107-XII-2019 lo concerniente a imposición de la pena por el cometimiento del mencionado delito, a saber:

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

> La pena máxima se aplicará a la persona que: defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para captura, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. (p.81)

Al respecto, juristas comparten el concepto de que en la estafa interviene un elemento importante como es la protección de bienes jurídicos, asemejándose en este caso que la transferencia del patrimonio tiene compatibilidad con los ciberdelitos bancarios, pero hacen falta otros dos elementos básicos para incluirlos dentro del delito de estafa, que es el engaño y el error en el perjudicado misma que debe ser objeto de análisis e inclusión por parte del legislador puesto que en su defecto se incluye otras conductas diferentes al tipo penal elemental y básico.

Los ciberdelitos bancarios se asemejan al delito de estafa, sin embargo, no puede encajarse únicamente bajo este supuesto, porque los ciberdelitos tienen consigo varios tipos penales y verbos rectores diferentes, por lo que son cometidos de otra forma totalmente distinta. Los ciberdelitos reúnen los tipos penales de uso de claves de acceso, falsedad de documentos, daños a la propiedad y a bienes informáticos, el robo de patrimonio, secuestro de datos, y la suplantación de identidad, en la que sus verbos rectores son: suplantar, engañar, secuestrar, ocultar, bloquear y dañar, en consecuencia, el delito de estafa genéricamente no constituye un ciberdelito menos aun tratándose de delito bancario, por lo que mal podría tomarse en cuenta a los ciberdelitos bancarios como estafa, por no contener normas penales y tipificación que vayan en tal sentido.

Cedeño (2019) considera que:

> El delito de estafa informática no se puede configurar dentro de la concepción tradicional de estafa, puesto que el verbo rector de engaño no se adapta a las Tecnologías de la Información y Comunicación (Tics), puesto que los sistemas sólo realizan actos que le han sido programados, no se puede afirmar que una computadora ha robado datos a través del engaño, puesto que no existe voluntad para la realización de dicho delito. Para que exista engaño, debe darse un proceso de toma de decisiones basado en supuestos falsos que lleven a una conclusión o resultado diferente del que esperaba el individuo embaucado. (p. 5)

Pese a esto, el COIP (2023) implementa dentro de la estafa a los ciberdelitos bancarios no en sentido muy amplio, reiterando que es necesario una adecuada tipificación que individualice las serie de conductas antijuridicas y con un nexo causal acorde al cometimiento de los mismos, puesto que a falta de tipificación quedan vacíos legales a sabiendas que la tecnología cada día entra en un proceso de adelantos lo que conlleva a que se legisle en relación a estos ilícitos en aras de aplicación de una correcta administración de justicia.

El Convenio Internacional de Budapest sobre ciberdelincuencia, trata de equiparar las diferentes acciones jurisdiccionales con el delito de fraude informático, también es verdad que existen otras tipologías no contempladas en dicho convenio que es importante estudiar y observar cuando los medios empleados en su comisión sean las nuevas tecnologías, dado el volumen y la importancia que están adquiriendo.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

En el COIP, no se encuentran tipificados específicamente los ciberdelitos bancarios, tampoco en otras normativas, pero la Normativa de Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información, hace una breve descripción en el índice de palabras de lo que es el *malware* y anti *phishing*. Sin embargo, no son todos los que existen y tampoco se encuentra descrito cada uno a detalle. Cabe señalar, que esta normativa hace énfasis en sistemas de seguridad de la información con la contratación de personal externo y programas para mitigar todos los tipos de ciberdelitos.

En el Artículo 76 numeral 3 de la Constitución de la Republica del Ecuador (2009) indica:

> 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. (p.91)

Esto conlleva, a que para que una conducta sea considerada como delito debe necesariamente estar tipificada como infracción penal anterior al hecho; o lo que es más, debe estar contemplado el cometimiento de un ilícito informático en el COIP, mismo que tomando en consideración al numeral tercero de la Carta Magna *íbidem* se desprende que en la actualidad al no haber una tipicidad clara y concreta respecto a los delitos ciber informáticos no cabría por parte de los operadores de justicia aplicar el artículo 25 del COIP, peor aún, determinar un juicio de reproche acorde a lo que prescribe el artículo 34 *íbidem*.

Según Narváez (2021), hasta el momento, el delito de Phishing aún no ha sido debidamente clasificado, siendo este un acto delictivo que conlleva necesariamente la utilización de Tecnologías de la Información y Comunicación Social. Estas herramientas se emplean para llevar a cabo acciones ilícitas de manera repetitiva dirigidas contra otro individuo. Si bien es cierto, que consta en el Libro Primero, inherente a la infracción penal, en el Título IV, capítulo tercero, sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación que van desde el Art. 229 hasta el Art. 234.4. misma que refiere a revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicaciones, falsificación informática, agravación de las penas, responsabilidad de personas jurídicas, definiciones de contenido digital, datos de tráfico, proveedor de servicios y sistema informático, nada dice al respecto al delito informático propiamente bancario.

Pérez y Montenegro (2022) en una publicación del Congreso señala: "También estipula reglas procesales para incorporar los medios digitales que permitan la obtención de evidencias, pruebas electrónicas en el proceso penal y la creación de órganos competentes para una investigación eficaz". Sin embargo, tomando en cuenta que los ciberdelitos bancarios poseen información y protocolos para su investigación esta requiere de profesionales y peritos calificados en la materia a fin de que determinen la ilicitud, puesto que sería importante incorporar los términos ya referidos anteriormente, en razón de que, a más del engaño, debe estar precedido de otras conductas ilegales.

Miró (2013), refiere sobre la estafa informática que:

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

> No se exige que sea el propio sujeto pasivo el que realice el acto de disposición patrimonial, sino que, más bien a la inversa, debe ser el propio sujeto activo el que transfiera dinero a su cuenta. De este modo, al igual que para que haya estafa es necesario que sea el propio sujeto engañado el que realice el acto de disposición patrimonial, para que haya estafa informática es necesario que eso no ocurra, esto es, que haya una transferencia "no autorizada", siendo irrelevante si la transferencia la realiza el propio sujeto activo o un tercero. Y esa diferencia va a ser determinante… a la hora de concretar el régimen punitivo del delito en relación con los ataques al patrimonio que se realizan a través de Internet, pues dejará fuera del mismo a aquellos comportamientos defraudatorios que logren que sea el propio usuario el que autorice la transferencia, aunque no sepa que es en su propio perjuicio. (p.13)

Se colige entonces que sin importar quien cometió la transferencia, es decir, ya sea el sujeto activo o pasivo o una tercera persona, ya sea intelectual o coautor, ha actuado en contra de su voluntad, sin dolo, no existe delito de estafa, peor aún cometimiento de fraude informático, como ocurre en otras formas de ciberdelito tratándose de *pharming*, mismo que tiene diferentes tipos de software maliciosos como espiar, copiar o atacar con virus informáticos.

En la legislación penal ecuatoriana no se encuentra normatizado respecto a tipificación en forma concreta que guarden relación a delitos informáticos bancarios como se menciona anteriormente, pues, únicamente existe legislación penal inherente al delito de estafa, igualmente se encuentran dentro de las conductas penalmente relevantes las acciones u omisiones que producen resultados lascivos, descriptibles e inembargables conforme preceptúa el artículo 22 del COIP, es decir, que el momento en que se lesiona un bien jurídico protegido tanto patrimonial como de intimidad se estarían violentando sistemas informáticos siempre y cuando el antecedente sea en este sentido.

Acotando también que ciberdelitos bancarios han desplazado completamente a las estafas tradicionales, por la comodidad desde donde se puede cometer sin correr riesgo físico alguno y por los grandes ingresos económicos que representa, esto hace ver la necesidad de una reforma legislativa en la que ya no sólo consta su diferente tipología en los ciberdelitos bancarios sino además su *modus operandi* con el propósito de obtener medios probatorios adecuados.

7.2.4.- Revelación ilegal de base de datos

Al respecto Paz y Bordachar (2021) mencionan que:

> A pesar de la garantía de la privacidad consagrada en la Constitución, el Ecuador carece de una normativa legal y de una autoridad técnica e independiente que permita una adecuada protección de datos personales conforme a estándares internacionales de derechos humanos. (p.2)

Se colige que pese a estar constitucionalmente protegido datos personales pues en la práctica no se cumple, aún más, tomando en cuenta que la Ley de Protección de Datos Personales garantizan el uso adecuado de los datos personales y el derecho de acceso a estos, con un sin número de categorías en el ámbito genético, personal, crediticio y de salud, desde luego, regulada por la Agencia de Regulación y Control de las Telecomunicaciones

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

(ARCOTEL), entidad que regula información de entidades públicas de telecomunicaciones, siendo la única y la más actual publicada en el año 2021 en el Registro Oficial. Pero esta norma actúa específicamente en el ámbito público más no en el sector financiero privado.

El Ecuador consagra a la protección de datos como un derecho fundamental establecido constitucionalmente encaminado al respeto de los derechos humanos, mismos que no se cumplen por ser atentatorio y violatorio a tales derechos, lo que, es más, por no existir mecanismos adecuados o una legislación penal adecuada respecto a los ciberdelitos ya referidos anteriormente (Aguilar et al., 2022).

Las normas de protección de datos en la jurisdicción ecuatoriana como en otras, generan dificultades al momento de investigar esta clase de delitos, debido a que los ciberdelincuentes utilizan encriptaciones para ser anónimos, ya que al momento de hacer una prolija investigación se requiere de medios probatorios apropiados con experticias, mismos que resultan inoficiosos al momento de practicar y obtenerlos aún más tratándose que se deriva de ámbitos internacionales que lesionan intereses nacionales de particulares por lo que se requiere necesariamente de una cooperación internacional para llegar al origen de la ciberdelincuencia.

Además, Paz y Bordachar (2021) referente a la protección de datos expresan:

> Ecuador sufre de una paradoja: reconoce la protección de datos personales como derecho fundamental, basado en su Constitución, así como en tratados internacionales de derechos humanos que protegen la privacidad, pero carece de una estructura legal interna para garantizar dicha protección, lo que deja a ecuatorianas y ecuatorianos en la práctica en la indefensión, ante situaciones y medidas como las descritas. (p.4)

En lo anterior se desprende que a pesar de estar constitucionalmente respaldado como también con normas supra nacionales, el Ecuador no ha normatizado aún para contrarrestar estos ilícitos, dejando en indefensión al agente perjudicado, por lo que es imperioso una normativa que delimite toda esta clase de ciberdelitos.

El Art. 229 del COPI respecto a la revelación ilegal de dase de datos preceptúa que la persona que en provecho propio o de un tercero revelare información registrada ya sea por medio de sistemas electrónicos, informáticos, telemáticos o telecomunicaciones violando el secreto de la persona, su intimidad, y privacidad será sancionada con pena privativa de libertad de uno a tres años. Igualmente consta que si estas conductas cometen funcionarios públicos o empleados bancarios la pena será de tres a cinco años.

Es menester, señalar que la norma legal antes invocada refiere tanto a personas naturales como en ejercicio de cargos públicos, en especial estos últimos bancarios serán objeto de juicio de culpabilidad o reproche con penas respectivas según su acto ilegal cometido, nada dice con claridad meridiana respecto a los ciberdelitos bancarios.

7.2.5.- Suplantación de identidad

De acuerdo con Carriedo (2022), esta artimaña delictiva se vale de la confianza de las personas para usurpar identidades y hacerse dueños de sus posesiones. En otras palabras, este acto delictivo se engloba en la categoría de los delitos de suplantación de identidad. La

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

suplantación de la identidad se asemeja al ilícito llamado *phishing*, por la confiscación de la identidad a través medios telemáticos con el propósito de obtener lucro económico, conducta penalmente desaprobada, que de manera somera se relaciona con el delito de estafa en el COIP, mismo que no es tan claro su contenido jurídico, por lo que reitero es importante que conste el hecho antijurídico de suplantación de identidad ya sea de manera amplia en el delito de estafa o en su defecto el legislador reforme el COIP, considerando esta serie de actos ilícitos que se originan dentro de los ciberdelitos bancarios.

Por su parte, López (2019) señala que, aunque existe cierta semejanza entre este tipo de delito y el phishing bancario en línea, el correo de suplantación de identidad se distingue por su denominación única en inglés, conocida como "*Spoofing email*". Esta técnica se emplea con astucia por parte de los atacantes, quienes ocultan la verdadera dirección del remitente en un correo malicioso y la reemplazan con una dirección legítima, suplantando así la identidad de una empresa o un usuario mediante el uso de un dominio auténtico. Esta artimaña es comúnmente utilizada en campañas maliciosas de phishing o spam, con el propósito de aumentar su efectividad al eludir los controles antispam y conferir a los correos una apariencia más convincente.

Aquí el problema radica en la investigación de evidencias, ya que dicha información personal al ser restringida traería complicaciones a la hora de investigar, por lo que resulta un nuevo desafío probatorio a la hora de identificar la identidad del *phisher*. Por esto se ve necesaria su correcta tipificación ya que a la par se necesita de peritos que se encuentren especializados y actualizados en el tema por lo que requiere un arduo trabajo, siendo que en los años venideros estos delitos se generalizaran por completo en el sistema punitivo nacional e internacional.

7.3.- Propuesta de regulación normativa de los ciberdelitos bancarios

Es importante encontrar informes y reuniones de organismos internacionales que recomiende este tipo de acciones legislativas por parte de los estados para prevenir el cometimiento de estos delitos. En la ciudad de Quito, en el año 2016 se realizaron dinámicas y estrategias del organismo internacional UNASUR para frenar diferentes tipos penales. En esta reunión se trató específicamente sobre la situación de los delitos trasnacionales por parte de los estados miembros a través de fiscales y procuradores para prevenir el cometimiento de estos delitos.

Al respecto dentro del derecho comparado la Fiscalía de Chile respecto al Ciberdelito, manifestó:

> Que estos delitos, al cometerse por medios electrónicos, son recurrentes las 24 horas del día, por lo tanto, no tienen fronteras y supone nuevos desafíos. “El Ciberdelito se lo puede entender como el conjunto de actividades ilícitas al amparo del uso de la tecnología”, dijo el fiscal chileno. Además, explicó que el más recurrente en ese país es el phishing (obtención de información bancaria de forma fraudulenta) y el *pharming* (acceso fraudulento a una computadora, a través de un virus que actúa para extraer la información). Para investigar esta modalidad delictual, que surge con la evolución tecnológica, es necesaria la construcción de manuales o guías conjuntas, para no dejar estos tipos penales en la impunidad. (Fiscalía General del Estado, 2016, p. 1)

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Constituyéndose este país sudamericano en unos de los primeros en dar importancia y validez a estos hechos ilegales cometidos llamados ciberdelitos, para ello crean en el año 2022, programas de estudio y materializaciones de conformidad con la Ley de Delitos Informáticos adecuándolos conforme al convenio internacional de ciberdelincuencia de Budapest.

A pesar de que los estados se adhieran al Convenio de Budapest, que busca abordar y combatir los delitos cibernéticos a nivel internacional, la rápida transformación tecnológica está generando la necesidad de adaptar y modificar las metodologías y clasificaciones de casos en el ámbito nacional. Según Pons (2017), estas transformaciones ponen de manifiesto deficiencias en la legislación existente, especialmente en lo que respecta a la sanción de delitos cibernéticos.

En este contexto, la prueba digital asociada a los delitos cibernéticos difiere significativamente de las pruebas físicas convencionales. Esta diferencia radica en la naturaleza de los delitos cibernéticos, que a menudo dejan rastros digitales y requieren herramientas especializadas para su detección y análisis. Sin embargo, la normativa nacional, que es la que establece las reglas y sanciones a nivel local, puede no estar actualizada para abordar adecuadamente estos aspectos específicos de la evidencia digital y los delitos cibernéticos.

Por lo tanto, aunque exista un compromiso internacional a través del Convenio de Budapest, la efectividad de la sanción de los delitos cibernéticos dependerá en gran medida de la capacidad de los sistemas legales nacionales para adaptarse y abordar las particularidades de estos delitos. Si la normativa nacional no contempla de manera adecuada los delitos cibernéticos o no proporciona las herramientas necesarias para su persecución, la eficacia del convenio puede verse comprometida.

Para suscribir este convenio internacional como La Convención sobre Cibercrimen es necesario la participación de la función ejecutiva inherente a su suscripción y si el caso amerita si es necesario para su aprobación se requiere de la función legislativa pues considero que se debe contar con un criterio constitucional, mismo que estará a cargo de la Corte Constitucional a efectos de la emisión de un dictamen. Con aquello al suscribirse este tipo de convenio el Ecuador entraría a formar parte de beneficios legales para contrarresta estos ciberdelitos incluidos los bancarios ya que operaría tanto la justicia nacional como internacional en contra de la delincuencia organizada y bandas transnacionales dedicadas a esta serie de ilícitos, lo que es más daría paso a implementación de normas que sancionen la ciberdelincuencia, o en su defecto legislando, reformando leyes penales que vayan en este sentido.

7.4.- Creación de nuevos delitos

Los estados miembros del Convenio de Budapest tienen como objetivo crear y unificar los tipos penales sobre ciberdelincuencia lo que hace que se puedan integrar métodos de investigación y sea más fácil la cooperación entre países. Estos ciberdelitos, aunque ya cuentan con más de 20 años de su creación, se encuentran un poco desfasados por el avance de la tecnología. Aunque la legislación ecuatoriana no contiene implementado a cabalidad estos artículos, acoplar al código punitivo la identificación de estos delitos va a ser de gran ayuda para esa cooperación internacional y el fortalecimiento en la región.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

En el presente gráfico procedente de la Fiscalía General del Estado, tomado del Diario El Universo se demuestra el número de denuncias respecto a delitos informáticos que se producen en el Ecuador concerniente los años 2014-2015-2016-2017-2018 y 2019 y 2020 estos han venido cada año en aumento; y en el año 2020 casi disminuye en un cincuenta por ciento en relación al crecimiento del año 2019, lo cual da a entender que talvez por la importancia y necesidad de contrarrestar estos delitos delincuentes nacionales se asociaron con delincuentes internacionales constituyendo una organización delincuencial internacional con el propósito de no dar acción a las acciones penales respectivas en el país y en tratándose de que los delitos se incidan en el extranjero y se concreta en el Ecuador, conllevaría a que se inicie la investigación y juzgamiento en el país que se inició el cometimiento del ilícito.

En este contexto, se podría argumentar la necesidad de crear nuevos delitos o actualizar la legislación existente para abordar estos fenómenos emergentes de delincuencia organizada a nivel internacional. Los cambios en la legislación podrían permitir una mayor cooperación entre los países para perseguir y castigar eficazmente a los responsables de delitos informáticos transfronterizos. Además, la adaptación de las leyes a la rápida evolución de las tecnologías y las tácticas utilizadas por los delincuentes cibernéticos es esencial para mantenerse a la par con la complejidad de estos crímenes.

Figura N° 1: Denuncias de delitos informáticos 2014-2020.

NÚMERO DE DENUNCIAS SOBRE DELITOS INFORMÁTICOS EN ECUADOR

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24 052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17 913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	**3118**	**8230**	**8796**	**8421**	**9571**	**10 279**	**5048**	**53 463**

*Desde agosto - **Hasta agosto

Fuente: Fiscalía General del Estado

EL UNIVERSO

Fuente: Diario El Universo (2020).

Ciertamente, el aumento considerable de los ciberdelitos en Ecuador, reflejado en el notable incremento de solicitudes de investigación de 682 en 2020 a 1.851 en 2021, destaca la amenaza que estos representan para la seguridad financiera del país. A pesar de los esfuerzos de los bancos ecuatorianos, que están realizando inversiones significativas en tecnología y medidas de seguridad, la persistencia y evolución de los ciberdelitos plantean un riesgo latente que podría minar la confianza en el sistema financiero y resultar en pérdidas económicas considerables. Un dato revelador indica que, por cada dólar defraudado a un cliente, la entidad financiera sufre una pérdida aproximada de $3,68, subrayando así el impacto financiero sustancial de estos delitos tanto para los bancos como para la economía en general (Asobanca Ecuador, 2023).

Una estrategia crucial para abordar este problema es la tipificación específica de los ciberdelitos en la legislación del país. Establecer leyes claras y específicas relacionadas con los delitos cibernéticos permitiría una persecución legal más efectiva y proporcional a la gravedad de cada infracción. Al tipificar los ciberdelitos, se proporcionaría un marco legal que permitiría sancionar a los delincuentes de manera adecuada, tomando en cuenta factores como el monto de las pérdidas y el impacto económico. Esto no solo actuaría como un

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

disuasivo más fuerte, sino que también facilitaría la cooperación entre las instituciones financieras y las autoridades encargadas de hacer cumplir la ley. Además, la tipificación de los ciberdelitos permitiría una mejor recopilación de datos y estadísticas precisas sobre la magnitud del problema. Esto sería crucial para desarrollar estrategias más efectivas y adaptativas a medida que evolucionan las amenazas cibernéticas.

Por otro lado, la creación de ciberdelitos a través de las nuevas tecnologías es lo más perpetrado en la actualidad. Por ello la necesidad de tipificar nuevos tipos penales que estén acorde a los verbos rectores que se utiliza, esto con el fin de contar con normas procesales actuales a la realidad. El ciberfraude es uno de los delitos tipificados por muchos países que engloba a todos los ciberataques que hay y los que aparecerán en el futuro, un poco cambia su nombre en relación al género que es el ciberespacio, la informática o nuevas tecnologías de la información y comunicación (Tics).

Su concepto en sí es a través de sistemas digitales. Lo que ocurre es que no se da una correcta diferenciación de los nuevos delitos que están apareciendo por lo que en algunas naciones han creado organizaciones específicamente destinadas a catalogar los diferentes tipos de delitos informáticos para no dejar en la impunidad esta conducta y siendo parte de la red internacional INTOCC, por sus siglas en ingles que traducen; al Observatorio Internacional de Delitos Informáticos.

Teniendo en cuenta esto, los ciberdelitos bancarios constituyen una realidad en constante crecimiento en Ecuador, representando un desafío tanto para las instituciones financieras como para sus clientes. Aunque los bancos están a la vanguardia en el desarrollo de servicios innovadores y estrategias de gestión de incidentes en ciberseguridad, la posición del país en el puesto 119 de 182 en cuanto a vulnerabilidad a los ataques cibernéticos sugiere que aún hay un camino significativo por recorrer para proteger de manera efectiva a las instituciones financieras y a sus clientes. La realidad actual demanda una atención constante y una respuesta integral para fortalecer la resiliencia del sistema financiero ecuatoriano frente a las amenazas digitales en evolución (Asobanca Ecuador, 2023).

Otro aspecto crítico que contribuye a la vulnerabilidad ante los ciberdelitos en Ecuador es la insuficiencia legislativa. Varios informes señalan la urgente necesidad de reformas en el código penal y la implementación de leyes más dinámicas que permitan una respuesta más efectiva a estos crímenes. Según González et al. (2018), la carencia de un marco legal adecuado no solo dificulta la labor de las autoridades, sino que también limita su capacidad para actuar de manera eficaz contra los ciberdelincuentes. Se destaca, además, que la jurisprudencia frente a los ciberdelitos ha sido insuficiente, al tratarlos como delitos contra el patrimonio en lugar de reconocer su especificidad y gravedad, lo que subraya la necesidad de una revisión profunda en este ámbito.

En ese contexto, la legislación ecuatoriana es insuficiente puesto que en la regulación normativa de Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información describe sobre los medios de protección contra los ciberdelitos bancarios como el anti *phishing* y el *ransomware*; que es uno de varios softwares que utiliza el *pharming* para robar contraseñas. Pero esta normativa no especifica de qué delitos protege a los usuarios o cuáles son las conductas tipificadas. Esta norma sólo hace referencia a la protección de los ciberdelitos y no existe otra normativa jurídica en el país que lo indique.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Esto requiere la tipificación porque no se tiene claro un delito adecuado y no sabe en qué delito encasillarlo, ya que los ciberdelitos reúnen varios tipos penales y sería incoherente añadirlo a un delito tradicional. Por lo que requiere ponerse a la medida internacional que implica estos delitos, por ejemplo, en cuestión de penas cuando un delito es transfronterizo es importante que los países puedan equilibrar sus penas y se necesita que se establezca al menos en alguna norma supletoria para identificarlos.

Muchos de estos ciberdelitos se originan en el comercio electrónico por la mera confianza y desconocimiento de la sociedad que lo único que hacen es tomar desprevenidos a fin de pescar a la víctima. Muchas personas que utilizan a diario sus redes sociales no tienen ni la mínima idea que como pueden ser víctimas de una transferencia ilícita de sus cuentas bancarias, por el hecho de que éstas no se encuentran tipificadas ni tampoco cuentan con una difusión.

7.5.- La tipificación de los ciberdelitos bancarios

La tipificación de los ciberdelitos bancarios en el país ayudaría con el estudio de nuevas formas de investigación para identificar quién es el ciberdelincuente y dónde se encuentra, así como el uso de tecnologías para acceder de forma más temprana a las evidencias. Permitiría tener una normativa adecuada a la hora de sancionar una pena privativa de libertad y así no caer en una desproporcionalidad de la pena, al encontrarse en el art. 186 del delito tipificado por Estafa; inciso dos, numerales uno y dos, del Código Orgánico Integral Penal, con una máxima de la pena a los que efectúen estos nuevos delitos.

Quijano (2021) respalda la tipificación de los ciberdelitos bancarios con lo que siguiente:

> En este sentido, debemos tener en cuenta que la implementación de estas modalidades de comisión de fraudes informáticos servirá para mitigar la comisión de los delitos informáticos, y lograr identificar el espacio virtual donde se computan dichos ilícitos; ya que debido a su naturaleza exige que los agentes de justicia se encuentren meramente calificados para su tratamiento. Para ello, deberían realizar especializaciones para distinguir las diferentes modalidades mediante las cuales se comisionan estos ilícitos penales, de modo tal que se rompa con aquellas directrices habituales para la imputación de un delito tradicional. (p.9)

También, mediante la tipificación se podría resolver otro problema procesal, al saber quién será el órgano jurisdiccional competente en razón del territorio, puesto que muchos de estos ciberdelitos radican fuera de la República del Ecuador, puesto que en muchas ocasiones se desconoce el lugar o sitio dónde se perpetraron y no hay una determinación concreta de competencias.

De tal manera, que urge una directriz por parte del legislativo a fin de que mediante reformas o implementación de nuevas normas o disposiciones penales se tipifique en la legislación penal ecuatoriana actual; esto es, en el COIP y, se incluyan los ciberdelitos bancarios, materia de la presente investigación tales como: *phishing, pharming, smishing y vishing*. De esta forma existiendo normas claras y tipificadas, los operadores de justicia al momento de sancionar y juzgar esta clase de delitos lo harán en base a preceptos legales y constitucionales, sin contravenir la Carta Magna en lo que regla el Art. 82 sobre la seguridad jurídica, aquello que conlleva a que los ciudadanos del país y por ende extranjeros

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

nacionalizados conozcan sobre la existencia de normas jurídicas previas, claras, públicas y aplicadas por la autoridad competente.

Consecuentemente a lo anterior, al exigir normas y reglas claras, se estaría también en aras del debido proceso conforme preceptúa el Art. 76 , numerales 1,2,3,4,5,6, y 7 de la Constitución de la República (2008) accionando judicialmente por parte de los operadores de justicia en materia penal y Ministerio Público garantizando el derecho de las partes, la garantía de inocencia, principio de tipicidad, principio de legalidad, principio de taxatividad, principio de proporcionalidad, y lo más fundamental derecho a la defensa, lo que conlleva a que las partes procesales se vean protegidas dentro de un proceso judicial penal y no ser objeto de indefensión.

Al igual que las transacciones civiles o contratos mercantiles que se llevan en el ciberespacio es necesario contar con adecuadas normas legales civiles, a más de sentido de conciencia, moral y ética, la cual tiene que ser creada por el Legislativo y Ejecutivo en pro de la sociedad mediante creación de normas y directrices en áreas que sean de su competencia.

A fin de determinar la existencia de esta clase de delitos cibernéticos bancarios a los referidos anteriormente, es importante entrar a un análisis del delito, que no es sino la conducta humana, tipificada en la Ley penal con la amenaza de una pena, la cual debe lesionar y poner en peligro un bien jurídico, por lo mismo he aquí la necesidad de determinar las formas de comisión de los delitos, a sabiendas que se puede cometer delitos por acción o por omisión conforme indica el Art. 23 del COIP, entrando a los elementos o categorías dogmática del delito como son tipicidad, antijuricidad y culpabilidad. Acción por cuanto el delincuente al perpetrar el ilícito ya sea enviando mensaje sea por cualquier medio de comunicación, correo electrónico, mensajes de texto *WhatsApp*, llamadas telefónicas entre otras, para llegar al receptor, infringe las normas constantes en la ley penal so pena de ser juzgado y sancionado conforme al grado de responsabilidad en el respectivo juicio de reproche o culpabilidad.

8.- ANÁLISIS DE CASOS

8.1.- Sentencia N° 16/2022 (2022)

La sentencia presentada guarda relación con el tema del phishing, ya que el demandante alega que la transferencia no autorizada de fondos se produjo debido a una deficiencia en el sistema de seguridad informático del Banco Bilbao Vizcaya Argentaria S.A. (BBVA). El phishing es una técnica de fraude en línea donde los estafadores intentan engañar a las personas para que revelen información confidencial, como contraseñas o detalles de cuentas bancarias, haciéndose pasar por entidades de confianza.

En el caso mencionado, se describe que la demandante fue dirigida a instalar un token en la página de la entidad bancaria días antes de la transferencia fraudulenta. La demandante, al encontrar esto sospechoso, buscó aclaraciones, pero las instrucciones la llevaron a realizar modificaciones en su cuenta. La sentencia destaca que estas acciones fueron parte de un intento de phishing, ya que la entidad bancaria afirma que la operación se realizó correctamente y desde la IP habitual del cliente.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

La jueza considera que la entidad bancaria no ha logrado demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, según lo establecido en el artículo 44 del Real Decreto-ley 19/2018. Además, se hace hincapié en que la defensa del banco basada en la supuesta negligencia del demandante no se sostiene, ya que no se demostró que la actora incumplió sus obligaciones de seguridad.

Este caso destaca la importancia de la seguridad en línea y la responsabilidad de los proveedores de servicios de pago para proteger a sus clientes contra posibles fraudes, como los derivados del phishing. La sentencia se basa en la normativa legal relacionada con la autenticación de operaciones y la obligación del proveedor de servicios de pago de devolver el importe en casos de operaciones no autorizadas, aspectos directamente vinculados a la protección contra prácticas fraudulentas, como el phishing.

8.2.- Sentencia N° 32/2022 (Sentencia N° 32/2022, 2022)

En el caso presentado ante el Juzgado de Primera Instancia n.º 10 de Oviedo, la sentencia aborda un incidente relacionado con el phishing, una técnica cibernética utilizada para engañar a las personas y obtener información confidencial, como contraseñas y detalles de cuentas bancarias. El término "phishing" se refiere a un conjunto de técnicas mediante las cuales los ciberdelincuentes se hacen pasar por entidades confiables, como bancos, para manipular a las víctimas y lograr que revelen información sensible.

En este caso concreto, el demandante, Jaime Fernando Suárez Lobo, recibió mensajes fraudulentos a través de la línea de mensajes utilizada habitualmente por su banco, Banco Santander, S.A. Estos mensajes le informaban que su cuenta había sido bloqueada y lo redirigían a un sitio web falso que imitaba la apariencia del sitio legítimo del banco. Posteriormente, el demandante recibió otro mensaje que indicaba la activación de su cuenta y la existencia de una compra por un monto considerable.

A pesar de estos eventos, la entidad bancaria no contactó al demandante ni tomó medidas para verificar la autenticidad de las operaciones. En consecuencia, se realizaron transferencias no autorizadas desde la cuenta del demandante hacia Lituania.

La sentencia aborda la responsabilidad del banco en casos de phishing, destacando que la entidad financiera tiene la obligación de implementar medidas de seguridad para prevenir fraudes informáticos. La resolución subraya que la responsabilidad de la banca en línea es cuasi-objetiva, y la entidad solo estará exenta de responsabilidad si demuestra que el usuario actuó con negligencia grave.

En este contexto, se concluye que el banco no proporcionó un sistema de banca en línea seguro y no cumplió con sus deberes de seguridad frente a los riesgos asociados con el funcionamiento de su plataforma de banca digital. La sentencia resalta que el demandante no actuó de manera negligente y que la entidad financiera debió prevenirse ante la situación anormal, adoptando medidas concretas.

Finalmente, la resolución condena al banco a restituir la cantidad indebidamente extraída de la cuenta del demandante (18.500€) y a pagar los intereses legales. Además, impone las costas judiciales a la parte demandada. Este caso sirve como ejemplo de cómo los tribunales pueden abordar y decidir asuntos legales relacionados con el phishing y la responsabilidad de las entidades financieras en la protección de la seguridad de sus clientes en línea.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

8.3.- Juicio No. 09286-2014-6178

El análisis del caso se centra en la disputa sobre la responsabilidad del Banco Pichincha en el fraude electrónico que resultó en la transferencia no autorizada de fondos. La defensa del banco se basa en una sentencia previa en un proceso penal que eximió al banco de responsabilidad, mientras que Austro Distribuciones argumenta que el banco no proporcionó las medidas de seguridad adecuadas. En relación a los hechos relevantes, la empresa Austro Distribuciones Austrodis C. Ltda., representada por Jorge Eduardo Vintimilla Rodas, presentó una denuncia contra el Banco Pichincha C.A. por un servicio defectuoso, específicamente una transferencia no autorizada de $29.806,00 ocurrida el 13 de julio de 2012. La transferencia se realizó a una cuenta interna del mismo banco, y posteriormente se emitieron dos cheques a terceros desde esa cuenta. Ante estas irregularidades, Austro Distribuciones notificó al Banco Pichincha y presentó una denuncia (Juicio No. 09286-2014-6178, 2020).

La Superintendencia de Bancos y Seguros del Ecuador concluyó que el Banco Pichincha no había vulnerado los derechos financieros del cliente ni incumplido sus obligaciones de custodia de fondos. No obstante, Austro Distribuciones sostiene que, a pesar de contar con el dispositivo Token para transacciones, se llevó a cabo una transferencia no autorizada, argumentando que el banco falló en sus medidas de seguridad tecnológicas y no cumplió con el plazo para atender reclamos. En su defensa, el Banco Pichincha C.A. afirma que no es responsable del fraude, ya que el cliente fue víctima de delincuencia común, y que las medidas de seguridad electrónicas estaban en conformidad con la normativa vigente.

El Juez de Primera Instancia dio lugar a la denuncia de Austro Distribuciones, condenando al Banco Pichincha al pago de una multa y daños y perjuicios. El Banco apeló la decisión, alegando nuevamente su falta de responsabilidad, y la audiencia de apelación se llevó a cabo el 6 de enero de 2020, donde la Procuradora Judicial del Banco reiteró esta posición. El caso se sustenta en la Ley Orgánica de Defensa del Consumidor y la Constitución de la República del Ecuador. Se evidencia la aplicación de principios legales como la justicia, el respeto a los derechos constitucionales y las garantías del debido proceso. La decisión del juez de primera instancia sugiere que se consideró que el banco tenía cierta responsabilidad en el fraude. La apelación del Banco Pichincha y la resolución final del caso no se encuentran disponibles, lo que impide determinar el desenlace del proceso de apelación. Sin embargo, el caso subraya la importancia de la seguridad en las transacciones electrónicas y la responsabilidad de las instituciones financieras en la protección de los fondos de sus clientes.

Ciertamente, este caso aporta significativamente al abordaje de los ciberdelitos bancarios y la aparente insuficiencia legislativa en Ecuador en relación con la seguridad financiera. La situación expuesta pone de manifiesto la vulnerabilidad de los clientes frente a posibles fraudes electrónicos y la necesidad de contar con un marco legal robusto para proteger los derechos financieros de las personas y las empresas.

En primer lugar, la transferencia no autorizada de fondos en este caso específico destaca la sofisticación y la amenaza constante de los ciberdelitos bancarios. La utilización de un dispositivo Token, que se supone debería ser una medida de seguridad adicional, no impidió el acceso no autorizado a la cuenta de Austro Distribuciones. Este incidente subraya la

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

necesidad de actualizar y fortalecer las medidas de seguridad tecnológicas en el ámbito bancario.

Además, la respuesta de las autoridades judiciales y la Superintendencia de Bancos y Seguros del Ecuador plantea interrogantes sobre la suficiencia de la legislación existente para abordar casos de ciberdelitos bancarios. Aunque la Superintendencia concluyó que el banco no vulneró los derechos financieros del cliente, la decisión del Juez de Primera Instancia en favor de Austro Distribuciones y la imposición de multas sugieren que existen lagunas o interpretaciones ambiguas en la legislación vigente.

La defensa del Banco Pichincha, alegando que el cliente fue víctima de delincuencia común, resalta la importancia de una legislación específica que aborde los ciberdelitos bancarios de manera adecuada. La evolución de la tecnología requiere una legislación que se ajuste a las nuevas formas de fraude electrónico y garantice una protección eficaz de los fondos de los clientes.

En este contexto, el caso resalta la necesidad de revisar y fortalecer la legislación relacionada con la seguridad financiera y ciberdelitos bancarios en Ecuador. Esto implica considerar medidas más específicas para proteger a los clientes, así como garantizar que las instituciones financieras cumplan con estándares de seguridad tecnológica más rigurosos. Además, puede servir como un llamado a la actualización constante de la legislación para hacer frente a las cambiantes amenazas cibernéticas en el ámbito financiero.

9.- CONCLUSIONES

La necesidad de establecer normativas específicas para abordar los ciberdelitos bancarios se justifica por diversas razones. En primer lugar, la legislación ecuatoriana actual carece de disposiciones precisas que regulen estos delitos, lo que dificulta la persecución y sanción correspondiente. La ausencia de disposiciones precisas en la legislación ecuatoriana actual crea un vacío legal que dificulta la persecución efectiva y la imposición de sanciones adecuadas. Ciertamente, al carecer de una definición clara y detallada de los ciberdelitos bancarios, se generan obstáculos para la identificación y comprensión de estos actos por parte de los operadores de justicia. La falta de criterios específicos puede dar lugar a interpretaciones ambiguas, lo que complica la aplicación de medidas punitivas proporcionadas.

De allí que, la tipificación de los ciberdelitos bancarios a través de normativas específicas permitiría no solo establecer claramente qué conductas se consideran delictivas, sino también dotar a las autoridades de herramientas legales efectivas para combatir, prevenir y sancionar dichas acciones. Este marco normativo proporcionaría una base sólida para la investigación y persecución de los responsables, contribuyendo así a la disminución de la impunidad en este ámbito. Del mismo modo, la complejidad creciente de los ciberdelitos bancarios también contribuye a la necesidad de medidas legislativas específicas. Estos delitos se vuelven cada vez más sofisticados y complejos, lo que representa un desafío para las autoridades judiciales y financieras. La introducción de nuevos tipos penales específicos permitiría una mejor identificación y sanción de estas prácticas delictivas, adaptándose a las nuevas técnicas y estrategias utilizadas por los delincuentes.

A tales efectos, la protección de los clientes bancarios es una prioridad fundamental. Los ciberdelitos bancarios constituyen una amenaza para la seguridad financiera de los clientes,

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

quienes pueden sufrir pérdidas económicas significativas como resultado de estas actividades ilícitas. La implementación de nuevos tipos penales específicos no solo facilitaría una sanción más efectiva, sino que también fortalecería la defensa de los derechos financieros de los clientes bancarios.

Los delitos cibernéticos, sin importar su naturaleza, han sido motivo de creciente preocupación a nivel tanto internacional como nacional en los últimos tiempos. aún más tratándose de hechos bancarios en donde se juegan intereses dinerarios, que, por supuesto perjudican a la cuenta ahorrista o tenedor a cualquier título de dineros en un banco, he inclusive yendo más allá de la responsabilidad del mismo banco.

Ciertamente, dentro de la legislación penal ecuatoriana, a más de constar normas, reglas y sanciones para delitos contemplados en la misma, esta nueva modalidad de delitos cibernéticos bancarios o delitos bancarios propiamente dicho ha hecho nada más que llevar a la confusión con otros delitos informáticos que tienen diferentes finalidades a la hora de cometer un hecho ilícito, y acoplarlos en una conducta penal como la estafa, es un error delicado por parte del legislador.

A falta de una legislación nacional en este sentido conlleva a una serie de denuncias en el ejercicio de la acción pública por parte de Fiscalía y un gasto mayor al contratar un defensor particular o público, como consecuencia una irreparable pérdida de recursos por parte del Estado y del ciudadano, esto sin contar, que, al ser delitos transnacionales, su tiempo y complejidad traen consigo pérdidas económicas irreparables e inclusive inimputables.

Si bien nuestra normativa hace uso de profesionales que venden programas de protección y detección temprana de ciberdelitos bancarios, falta una descripción sobre cuáles son los delitos que se buscan castigar y cuáles son los medios que utilizan, porque como se vio anteriormente algunos tiene diferentes fines.

En la legislación ecuatoriana no se encuentran tipificados concretamente los ciberdelitos bancarios y confunde su tipología. Pero el problema también parte por la falta de políticas públicas que no ayudan a la ciudadanía a conocer y difundir cómo se perpetran estos delitos. Esto con el único fin de proteger a los usuarios de la banca y combatir la ciberdelincuencia.

Por tal motivo, la problemática presentada resalta la urgente necesidad de establecer nuevos tipos penales que se enfoquen de manera específica y eficaz en los ciberdelitos bancarios en Ecuador. La sofisticación de los fraudes electrónicos, como lo evidencia el caso de transferencia no autorizada de fondos, pone de manifiesto las limitaciones actuales de la legislación para hacer frente a las amenazas digitales en constante evolución.

La ausencia de una normativa específica en el ámbito de los ciberdelitos bancarios genera lagunas interpretativas que pueden comprometer la salvaguarda de los derechos financieros de los clientes. La respuesta de las autoridades judiciales y la Superintendencia de Bancos y Seguros subraya la imperiosa necesidad de contar con un marco legal más claro y actualizado para abordar los desafíos tecnológicos en el sector financiero.

En este contexto, resulta crucial que los legisladores se involucren en la creación de nuevas disposiciones legales que aborden de manera precisa las amenazas digitales en el ámbito financiero, teniendo en cuenta las innovaciones tecnológicas y los riesgos asociados. Estas actualizaciones legislativas son esenciales para garantizar una protección efectiva de

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

los derechos de los clientes y la seguridad financiera en un entorno digital en constante evolución. La implementación de nuevos tipos penales específicos para ciberdelitos bancarios no solo podría proporcionar claridad jurídica, sino que también enviaría un mensaje contundente sobre la seriedad con la que se aborda la protección de la integridad financiera en la era digital.

En consecuencia, la introducción de normativas específicas para los ciberdelitos bancarios es imperativa para garantizar una persecución adecuada y una sanción efectiva de estos delitos. Esta medida también se vuelve esencial para proteger a los clientes bancarios, quienes enfrentan riesgos financieros considerables. La adaptación de la legislación a la sofisticación de los delitos y la implementación de disposiciones más claras contribuirían significativamente a mantener la integridad del sistema financiero y a hacer frente a los desafíos emergentes en el ámbito de los ciberdelitos bancarios.

10.- RECOMENDACIONES

Del estudio y análisis del presente artículo profesional, recomiendo**:**

Se recomienda al Estado ecuatoriano suscribirse al Convenio Internacional de Ciberdelincuencia de Budapest debido a que prevé una normativa que respalda la cooperación internacional en investigaciones de ciberdelitos. Esto permitirá alcanzar el esclarecimiento de los hechos y la imposición de una sanción justa al emitir un fallo judicial en contra del procesado.

Que la Asamblea Nacional del Ecuador tome cartas en el asunto respecto a los ciberdelitos bancarios y legisle en el sentido que se incorpore normativas a efectos de su investigación, juzgamiento y sanción con la prueba pertinente, a fin de que no se cuente únicamente con convenios internacionales, sino con una legislación inherente a estos delitos bancarios dentro del Código Orgánico Integral Penal.

A tales efectos, se recomienda con urgencia la creación y actualización de tipos penales específicos para abordar los ciberdelitos bancarios en Ecuador, los cuales deben ser detallados y adaptarse a las dinámicas cambiantes de la tecnología, garantizando una clara distinción entre ciberdelitos bancarios y delitos convencionales. Se insta a la colaboración estrecha entre legisladores, expertos en ciberseguridad y el sector financiero para desarrollar leyes que reflejen las amenazas digitales actuales y proporcionen una base jurídica robusta para la persecución efectiva de los delincuentes cibernéticos, fortaleciendo así la seguridad financiera y la confianza en el sistema bancario.

Es necesario implementar nuevas estrategias y tomar como ejemplo modelos de otros países que cuente con un complejo judicial destinado para este tipo de delitos y para la conformación de una unidad especializada en ciberdelitos bancarios. Ello a pesar de contar recientemente en el Ministerio Público con una subdirección de delitos informáticos,

Que los órganos inmersos a la banca, esto es la Junta de Política y Regulación Monetaria, los mismos bancos tanto públicos como privados difundan programas de prevención a los clientes bancarios y demás personas inmersas en este ámbito, a fin de evitar ser objeto de ciberdelitos y perjudicados en su patrimonio a causa de estos delitos bancarios e informáticos en general.

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Que la Corte Nacional de Justicia cree jurisprudencia relevante a fin de que tanto representantes del Ministerio Público como operadores de justicia tengan claros conocimientos jurídicos de los ciberdelitos bancarios ya sea a nivel nacional e internacional y sobre todo al momento de sustentar los elementos de convicción el primero y dictar fallos los segundos no se cometerán yerros al tipificar el delito bancario y una sanción justa y equitativa para el procesado.

10.- Referencias bibliográficas

Instituto Nacional de Ciberseguridad . (15 de enero de 2021). *Smishing: el fraude de los SMS*. Obtenido de INCIBE: https://www.incibe.es/ciudadania/blog/smishing-el-fraude-de-los-sms

Agencia Peruana de Noticias. (7 de junio de 2022). *Agencia Peruana de Noticias*. Obtenido de Fiscalía logró sentencia por caso de ciberdelincuencia conocida como vishing: https://andina.pe/agencia/noticia-fiscalia-logro-sentencia-caso-ciberdelincuencia-conocida-como-vishing-896347.aspx

Aguilar, M., Gordillo, D., Paredes, J., & León, G. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina, 10*(Especial 1), 369-382. Retrieved from https://revistas.uh.cu/revflacso/article/download/3594/3138

Ángel, H. C. (mayo de 2016). *UNIVERSIDAD CENTRAL DEL ECUADOR.* Obtenido de El Phishing como Delito Informático y su Falta de Tipificación en el Código: http://www.dspace.uce.edu.ec/bitstream/25000/8132/1/T-UCE-0013-Ab-399.pdf

AO Kaspersky Lab. (2022). *Kaspersky*. Obtenido de ¿Qué es un troyano y qué daño puede causar?: https://latam.kaspersky.com/resource-center/threats/trojans

Arias, F. (2012). *El Proyecto de Investigación: Introducción a la metodología científica (6ta edición).* Caracas: Editorial Epísteme, C.A.

Asamblea Nacional Constituyente del Ecuador. (2008, octubre 20). Constitución de la República del Ecuador. *Decreto Legislativo 0, Registro Oficial 449, Ultima modificación 25-ene.-2021 Estado: Reformado*. Retrieved from http://tinyurl.com/5x7ynbxh

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Monetario y Financiero.* Registro Oficial Nº 332, Segundo Suplemento, Viernes 12 de septiembre de 2014. Obtenido de http://www.pge.gob.ec/documents/Transparencia/antilavado/REGISTROOFICIAL332.pdf

Asamblea Nacional del Ecuador. (2023). *Código Orgánico Integral Penal.* Quito: Registro Oficial 180, Suplemento, 10 de febrero de 2014. Retrieved from http://tinyurl.com/mr4xjm3p

ASOBANCA. (2022). *Cuidado con el phishing ¡No muerda el anzuelo!* (Asociación de Bancos del Ecuador ASOBANCA) Obtenido de ¿Cómo sucede el phishing?: https://asobanca.org.ec/innovacion-y-tecnologia/cuidado-con-el-phishing-no-muerda-el-anzuelo/

Asobanca Ecuador. (08 de noviembre de 2023). *Bancos están a la vanguardia en ciberseguridad*. Obtenido de Asobanca Ecuador: https://asobanca.org.ec/bancos-ecuador-vanguardia-ciberseguridad/

Baena, G. (2019). *Metodología de la Investigación.* México: Grupo Editorial Patria. Retrieved from http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Bermúdez, L. (2019). *PHISHING Y PHARMING "La problemática de la determinación de competencia en casos extraterritoriales.".* Universidad Siglo 21. Obtenido de https://repositorio.21.edu.ar/bitstream/handle/ues21/17778/BERMUDEZ%20LUCIANO.pdf?sequence=1

Bocetta, S. (16 de noviembre de 2018). *GlobalSign Blog*. Obtenido de Aviso: Kits de Phishing Avanzados Disponibles en la Dark Web: https://www.globalsign.com/es/blog/warning-advanced-phishing-kits-now-available-on-the-dark-web

Bocetta, S. (08 de mayo de 2019). *Aviso: Kits de Phishing Avanzados Disponibles en la Dark Web*. Obtenido de GlobalSign Blog: https://www.globalsign.com/es/blog/warning-advanced-phishing-kits-now-available-on-the-dark-web

Bordachar, M. P. (22 de enero de 2021). *Derechos Digitales*. Obtenido de Protección de datos personales en Ecuador: El momento es ahora: https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

Bordachar, M. P. (22 de enero de 2021). *Drechos Digitales América Latina*. Obtenido de Protección de datos personales en Ecuador: El momento es ahora: https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

C. Pérez, H. M. (04 de agosto de 2022). Prensa Libre Guatemala. *Congreso aprueba Ley de prevención y protección contra la ciberdelincuencia y esto se sabe de la normativa*.

Carriedo, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México.* INFOTEC. Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Cedeño, I. (2019). *Fraude Informático.* UNEMI.

Comité de Seguridad de la Información. (2022). *Política de Seguridad de la Información.* Secretaria Técnica del Comité Interinstitucional de Prevención de Asentaminetos Humanos Irregulares. Obtenido de https://www.asentamientosirregulares.gob.ec/wp-content/uploads/2021/03/POLITICA-DE-SEGURIDAD-DE-LA-INFORMACION.pdf

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia.* Serie de Tratados Europeos N° 185. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Derechos Digitales. (16 de mayo de 2022). *Derechos Digitales*. Obtenido de Convenio de Budapest sobre la Ciberdelincuencia en América Latina: https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/

Derechos Digitales. (16 de mayo de 2022). *Derechosdigitales Derechos Humanos y Tecnoligía en América Latina*. Obtenido de Convenio de Budapest sobre la Ciberdelincuencia en América Latina: https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/#:~:text=El%20Convenio%20de%20Budapest%20sobre,los%20delitos%20inform%C3%A1ticos%20y%20a%20la

Dirección General de Comunicación Social. (10 de octubre de 2022). *DELITOS CIBERNÉTICOS en aumento y con números exorbitantes*. Obtenido de Gaceta

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

UNAM: https://www.gaceta.unam.mx/delitos-ciberneticos-en-aumento-y-con-numeros-exorbitantes/

El Mundo. (24 de mayo de 2022). *El Banco Santander deberá devolver 18.500 euros a un cliente que fue estafado a través del método 'phishing'*. Obtenido de El Mundo: https://www.elmundo.es/economia/2022/05/24/628cb0adfc6c83ee5b8b45a5.html

ESET. (2023). *ESET Security Report Latinoamerica 2023.* ESET. Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

ESET Internet Smart Security. (2022). *ESET Security Report.* Obtenido de ESET Latinoamérica: https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

F. García, D. L. (2022). La sociedad de los algoritmos y el derecho digital. *IUS ET SCIENTIA*, 5-7.

FEDERAL BUREAU OF INVESTIGATION. (2022). *I. VIOLATIONS OF THE FEDERAL BANK ROBBERY AND INCIDENTAL CRIMES STATUTE, TITLE 18, UNITED STATES CODE, SECTION 2113.* Department of Justice. Obtenido de https://www.fbi.gov/file-repository/bank-crime-statistics-2021.pdf

Fernández, M. A. (9 de julio de 2013). Phishing. *Delitos Informáticos, Ediciones Legales EDLE S.A.*, 2. (F. M. Ángel, Ed.) Editorial La Ley.

Fernández, Y. (2 de junio de 2020). *Xataka Basics*. Obtenido de Malware: qué es, qué tipos hay y cómo evitarlos: https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Fiscalía General de la Nación (Colombia). (2019). *Cartilla metodológica de atención de delitos informáticos.* Fiscalía General de la Nación (Colombia). Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

Fiscalía General del Estado. (13 de junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Obtenido de Fiscalía General del Estado: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Fiscalía General del Estado. (2016, septiembre 14). *La situación de los delitos transnacionales fueron analizados en el Encuentro de Fiscales y Procuradores de la Unasur*. Retrieved from Fiscalía General del Estado: https://www.fiscalia.gob.ec/la-situacion-de-los-delitos-transnacionales-fueron-analizados-en-el-encuentro-de-fiscales-y-procuradores-de-la-unasur/

Fiscalía General del Estado FGE. (diciembre de 2021). Ciberdelitos. (D. S. Tapia, Ed.) *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FGE*(30), 1-33. doi:2661-6920

Francklin Rivas, C. M. (agosto de 2020). *Revista Ibérica de Sistemas y Tecnologías de la Información.* (RISTI, Ed.) doi:1646-9895

GlobátiKa Lab. (2022). *Sentencia a favor de los clientes estafados por phishing*. Obtenido de GlobátiKa Lab: https://peritosinformaticos.es/caso-de-exito-sentencia-a-favor-de-los-clientes-estafados-por-phishing/

GlobátiKa Lab Peritos Informáticos Judiciales. (2022). *Phishing*. Obtenido de Caso de éxito: Sentencia a favor de los clientes estafados por phishing: https://peritosinformaticos.es/caso-de-exito-sentencia-a-favor-de-los-clientes-estafados-por-phishing/

Gobierno de Perú. (07 de julio de 2022). *Ministerio Público logró sentencia por modalidad de cberdelincuencia conocida como Vishing*. Obtenido de El Peruano: https://www.gob.pe/institucion/mpfn/noticias/618876-ministerio-publico-logro-sentencia-por-modalidad-de-ciberdelincuencia-conocida-como-vishing

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Gonzáles, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). Delitos informáticos: una revisión en Latinoamérica. *Conference Proceedings UTMACH, 2*(1), 178-190. Obtenido de https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262

Harán, J. (14 de octubre de 2021). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios*. Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Heredia, S. C. (17 de agosto de 2022). *¿La nueva problemática? Hacerles frente a los nuevos delitos*. Obtenido de Comercio y Justicia: https://comercioyjusticia.info/opinion/la-nueva-problematica-hacerles-frente-a-los-nuevos-delitos/

Innova Perú Gold Group. (14 de octubre de 2020). Delito de Fraude Informático. *Hablemos de Derecho*. Perú. Obtenido de https://www.youtube.com/watch?v=P5-R3f9ID5s

INTERPOL. (04 de agosto de 2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Joaquín, B. L. (2019). *Universidad Siglo 21.* Obtenido de PHISHING Y PHARMING "La problemática de la determinación de competencia en casos extraterritoriales": https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/17778/BERMUDEZ%20LUCIANO.pdf?sequence=1&isAllowed=y

Juicio No. 09286-2014-6178, 09286-2014-6178 (Unidad Judicial Norte 2 con sede en el Cantón Guayaquil 16 de marzo de 2020).

Kaspersky Latam. (2021). *Kaspersky Lab*. Obtenido de ¿Qué es el pharming y cómo evitarlo?: https://latam.kaspersky.com/resource-center/definitions/pharming

llinares, f. m. (2012). *el cibercrimen.* Madrid, España: Marcial Pons, Ediciones Jurídicas y Sociales. doi:9788415664185

Llinares, F. M. (2013). La Respuesta Penal al Ciberfraude. *Revista Electrónica de Ciencia Penal y Criminología*, 1-56. Obtenido de http://criminet.ugr.es/recpc/15/recpc15-12.pdf

Llinares, F. M. (2013). LA RESPUESTA PENAL AL CIBERFRAUDE. *Revista Electrónica de Ciencia Penal y Criminología*, 56. doi:1695-0194

López et al, F. S. (2020). *INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA.* Secretaria de Estado de Seguridad, Dirección General de Coordinación y Estudios. Ministerio del Interior - Gobierno de España. doi:126-20-021-2

López, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing.* UOC. Obtenido de https://openaccess.uoc.edu/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf

López, M. (23 de marzo de 2021). *Welivesecurity By ESET*. Obtenido de Qué es email spoofing: la suplantación de identidad en correos electrónicos: https://www.welivesecurity.com/la-es/2021/03/23/que-es-email-spoofing-suplantacion-identidad-correos-electronicos/

Lorite, M. (2021). *Delitos Informáticos.* Policía Local de Alhama de Granada. Obtenido de https://escuelapolicia.com/wp-content/uploads/2021/04/Delitos-Informaticos.pdf

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

Malwarebytes. (2022). *Suplantación de identidad (phishing)*. Obtenido de Acerca de phishing: https://es.malwarebytes.com/phishing/

Masedo, A. (12 de febrero de 2022). *Derecho de la Red*. Obtenido de Breve historia del primer Spam.: https://derechodelared.com/breve-historia-del-primer-spam/

McAfee, LLC. (s.f.). *La escasez de talento en ciberseguridad.* Obtenido de Un estudio de la falta de competencias en ciberseguridad a nivel internacional: https://www.mcafee.com/enterprise/es-mx/assets/executive-summaries/es-hacking-skills-shortage.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador. (2020). *Guía para la implementación del esquema gubernamental de seguridad de la información.* Gobierno del Ecuador. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GUÍA-PARA-LA-IMPLEMENTACIÓN-DEL-EGSI-ABRIL2020.pdf

Miró, F. (2013). LA RESPUESTA PENAL AL CIBERFRAUDE: Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología, 15*(12). Obtenido de http://criminet.ugr.es/recpc/15/recpc15-12.pdf

Montes, A. (14 de septiembre de 2016). *Fiscalía General del Estado*. Obtenido de La situación de los delitos transnacionales fueron analizados en el Encuentro de Fiscales y Procuradores de la Unasur: https://www.fiscalia.gob.ec/la-situacion-de-los-delitos-transnacionales-fueron-analizados-en-el-encuentro-de-fiscales-y-procuradores-de-la-unasur/

Morgan, S. (13 de noviembre de 2020). *Cybercrime*. Obtenido de El cibercrimen costará al mundo 10,5 billones de dólares anuales para 2025: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Narváez, B. (2021). *El PHISHING como delito informático en la legislación Ecuatoriana.* Uniandes. Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/13462

Observatorio Español de Delitos Informáticos OEDI. (25 de noviembre de 2021). *OEDI Observatorio Español de Delitos Informáticos*. Obtenido de Información, análisis, estadísticas y ayuda contra los delitos informáticos: https://oedi.es/

Organización de los Estados Americanos. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* OEA. Obtenido de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Organización Internacional de Policia Criminal INTERPOL. (02 de septiembre de 2019). *Noticia Purpura INTERPOL*. Obtenido de Delincuencia financiera – ¡No sea la próxima víctima!: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Delincuencia-financiera-!No-sea-la-proxima-victima

Ortiz, N. (17 de febrero de 2022). *JLCasajuana abogados*. Obtenido de Smishing, estafa informática por SMS: https://jlcasajuanaabogados.com/smishing-estafa-informatica-por-sms/

Ortiz, N. (17 de febrero de 2022). *Smishing, estafa informática por SMS*. Obtenido de JLCasajuana abogados: https://jlcasajuanaabogados.com/smishing-estafa-informatica-por-sms/

OSI Oficina de Seguridad del Internauta. (17 de noviembre de 2021). *Oficina de Seguridad del Internauta*. doi:094-20-028-1

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. *Revista de Derecho (Valparaiso)*(XLI), 211-262. Obtenido de https://www.redalyc.org/pdf/1736/173629692007.pdf

Paz, M., & Bordachar, M. (2021). *Protección de datos personales en Ecuador: El momento es ahora*. Obtenido de Derechos Digitales:

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

Pérez, C., & Montenegro, H. (04 de agosto de 2022). Congreso aprueba Ley de prevención y protección contra la ciberdelincuencia y esto se sabe de la normativa. *Presna Libre*. Obtenido de https://www.prensalibre.com/guatemala/politica/congreso-aprueba-ley-de-prevencion-y-proteccion-contra-la-ciberdelincuencia-y-esto-se-sabe-de-la-normativa/?fbclid=IwAR0ka1RFx0IlFR8atjJ0ew0sk7zbQOjy3ZkfYmrvNh4josKvZchdagzMA9k

Pino, S. A. (2016). *Pontificia Universidad Católica del Ecuador PUCE.* Obtenido de Delito Informaticos: Generalidades: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Pons Gamón, V. (20 de junio de 2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. doi:DOI: https://doi.org/10.17141/urvio.20.2017.2563

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito,ciberterrorismo,legislación y ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. doi:10.17141/urvio.20.2017.2563

Posada, R. (14 de agosto de 2019). Cibercrimen y nueva teoría del delito. *LP Pasión por el Derecho.* (F. Chuquicallata, Entrevistador) @LPPasionporelderecho. Obtenido de https://www.youtube.com/watch?v=rJ_F10txD2k&t=71s

Proofpoint. (2022). *Proofpoint*. Obtenido de ¿Qué es el vishing?: https://www.proofpoint.com/es/threat-reference/vishing

Publicaciones Semana S.A. (22 de agosto de 2022). *Ciberseguridad*. Obtenido de Ciberdelitos e inclusión financiera: dos cosas que crecen de la mano: https://www.semana.com/finanzas/consumo-inteligente/articulo/ciberdelitos-e-inclusion-financiera-dos-cosas-que-crecen-de-la-mano/202241/

Quijano, M. A. (29 de octubre de 2021). *Universidad Privada del Norte.* Recuperado el 2020, de La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020.: https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

Redacción El Orientadero. (03 de marzo de 2022). *El Orientadero*. Obtenido de ¿Sabes cuál es el origen de la palabra spam? ¡Una lata de carne!: https://www.elorientadero.com/sabes-cual-es-el-origen-de-la-palabra-spam-una-lata-de-carne/#:~:text=La%20palabra%20spam%20viene%20de,hay%20hasta%20un%20sketch%20c%C3%B3mico.

Redacción El Universo. (27 de septiembre de 2020). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. *Diario El Universo*. Obtenido de https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador/

Riva, A. d. (06 de abril de 2020). *Peritos Judiciales Forenses*. Obtenido de La calificación jurídica del phising, smishing, vishing, pharming y spoofing como estafas informáticas: https://peritosjudicialesforenses.com/blog/la-calificacion-juridica-del-phising-smishing-vishing-pharming-y-spoofing-como-estafas-informaticas/

Rodríguez, F. (2016). *Nuevos delitos informáticos: Phising, pharming, hacking y cracking.* Ilustre Colegio de la Abogacía de Madrid: SP/DOCT/3705. Obtenido de

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador

https://web.icam.es/bucket/Faustino%20Gudín%20-%20Nuevos%20delitos%20informáticos.pdf

Rodríguez, S. F. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* Federación Latinoamericana de Bancos (FELABAN), Presidente Comité Latinoamericano de Seguridad Bancaria. Secretaría General de la Organización de Estados Americanos (OEA). Obtenido de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Ron, M. (21 de octubre de 2019). *Derecho Ecuador* . Obtenido de Estafa Informática: https://derechoecuador.com/estafa-informatica/

Rus, E. (01 de noviembre de 2020). *Investigación mixta*. Obtenido de Economipedia: https://economipedia.com/definiciones/investigacion-mixta.html

Sabino, C. (2017). *El proceso de investigación.* Ed. Panapo. Obtenido de https://www.perio.unlp.edu.ar/tif/wp-content/uploads/2021/04/CarlosSabino-ElProcesoDeInvestigacion_0.pdf

Sampedro, E. (14 de noviembre de 2022). *Fexlaw abogados*. Obtenido de Phishing: El delito informático de estafa en auge.: https://fexlaw.com/articulos/phishing-el-delito-informatico-de-estafa-en-auge/#:~:text=El%20t%C3%A9rmino%20phishing%20proviene%20de,ellos%2C%20conseguir%20menoscabar%20patrimonios%20ajenos.

Sampedro, E. (2022). *Phishing: El delito informático de estafa en auge*. Obtenido de FexLaw Abogados: https://fexlaw.com/articulos/phishing-el-delito-informatico-de-estafa-en-auge/

Sánchez, D. B. (23 de mayo de 2021). *Universidad de León.* Obtenido de ASPECTOS TÉCNICOS DEL DELITO DE PHISHING: https://buleria.unileon.es/bitstream/handle/10612/13693/SANTOS%20S%C3%81NCHEZ%2C%20BLANCA%20IRIS.pdf?sequence=1&isAllowed=y

Schwartz, M. J. (julio de 2020). *Banco Interamericano de Desarrollo; Organización de los Estados Americanos.* Obtenido de Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Sentencia N° 16/2022, 16/2022 (Juzgado de Primera Instancia e Instrucción N° 2 de Redondela 25 de enero de 2022).

Sentencia N° 32/2022, 32/2022 (Juzgado De Primera Instancia N° 10 de Oviedo 02 de febrero de 2022). Obtenido de https://www.newtral.es/wp-content/uploads/2022/06/20220207-Sentencia-estimatoria-sin-datos.pdf?x97555

Significados. (2022). *Tecnología e Innovación*. Obtenido de Significado de Encriptación: https://www.significados.com/encriptacion/

Ventura, M. (2021). *La Tipificación del Phishing, Smishing Y Vishing en nuestro Sistema Penal Peruano, para la lucha contra la Ciberdelincuencia en Lima, 2020.* Universidad Privada del Norte. Obtenido de https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2C%20Mishell%20Alisson.pdf

Ciudadela IOA, Av. de los Sarances s/n y Pendoneros
593 (06) 2920 009 / 593 (06) 920 461 / 593 (06) 2 923 850
Otavalo - Ecuador