UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

ABOGADO

AUTOR:

Aldecoa Jimenez, Milagros del Rosario (ORCID: 0000-0002-8067-857X)

ASESOR:

Dr. Prieto Chávez Rosas Job (ORCID: 0000-0003-4722-838X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, procesal penal, sistema de penas, causas y formas del fenómeno criminal.

LIMA – PERÚ

2020

Dedicatoria:
“La única vez que el éxito esta antes del trabajo es en diccionario”

Harvey Specter (personaje de ficción)

Agradecimiento:
Agradezco a mis padres que estuvieron todo este tiempo apoyándome, sin interrupción para conseguir este logro, agradezco a mi tío, Carlos Aldecoa, quien sin desmayo me ha apoyado todos estos años. Agradezco a Dios, a mis abuelos que se fueron muy pronto al cielo y a mi familia en general por sus casos que ayudaron en mi práctica.

Índice de contenidos

Índice de tablas

Resumen

La presente investigación tiene como finalidad determinar de qué me manera favorecen los medios informáticos la comisión del delito de suplantación de identidad, asimismo, desarrolla algunos tipos de tecnologías de la información y la comunicación.

Es de tipo cualitativa, por lo tanto, está orientada a la búsqueda de mejoras en base al estudio socio – económico – jurídico, para lograr nuestro objetivo se tuvo a 04 participantes que con sus condiciones y conocimientos contribuyeron al desarrollo de este trabajo.

Este delito se ve a menudo en los tiempos que estamos viviendo puesto que actualmente la sociedad usa mucho las tecnologías de la información y la comunicación para disminuir el tiempo que les puede tomar hacer las cosas presencialmente, asimismo las entidades del sector financiero brindan sus productos por estos medios informáticos para tener una vinculación contractual más rápida con el cliente, siendo importante su regulación y fiscalización del uso de estos medios para evitar el delito de suplantación de identidad.

La investigación fue respaldada con diferentes instrumentos documentales, la cual brindará algunos aportes y recomendaciones que ayudará a perfeccionar la regulación del delito de suplantación de identidad y el favorecimiento en su comisión por medios informáticos.

Palabras clave: suplantación de identidad, medios informáticos, Ley Nº 30096

Abstract

The purpose of this investigation is to determine how computerized means help me to commit the crime of identity theft, and also to develop some types of information and communication technologies.

It is of qualitative type, therefore, it is oriented to the search of improvements based on the study socio - economic - legal, to achieve our objective we had 04 participants that with their conditions and knowledge contributed to the development of this work.

This crime is often seen in the times we are living since nowadays society uses a lot of information and communication technologies to reduce the time it can take them to do things in person, also the financial sector entities offer their products by these computer means to have a faster contractual link with the client, being important its regulation and control of the use of these means to avoid the crime of identity theft.

This research was supported with different documentary instruments, which will provide some contributions and recommendations that will help to improve the regulation of the crime of identity theft and the favoring of its commission by computer means.

Keywords: identity theft, computer media, Law No. 30096

I. INTRODUCCIÓN

A diario vemos en las noticias nacionales diferentes denuncias en las que se atribuye la vulneración del derecho a la identidad, pero que estas se encuentran efectivizadas de distintas formas.

Navegar en redes para todas las personas ayuda a que evitemos la pérdida de tiempo en vez de acudir a las entidades bancarias u operadores móviles haciendo un sinfín de colas para que puedan ser atendidos, estas entidades se encargaron de aminorar esta carga tanto para ellos como para las personas que desean adquirir sus diferentes productos ofrecidos, ofreciendo sus sistemas informáticos o apps a través de medios informáticos para que de forma virtual puedan adquirir los diferentes productos y así el cliente se vea beneficiado de varias formas.

Durante las últimas décadas las nuevas tecnologías han sido un instrumento esencial en la sociedad, incluso algunas naciones integran el derecho a internet como un derecho fundamental en sus constituciones; asimismo, la denominan una necesidad básica; sin embargo, el sector más favorecido es el económico, visto desde un enfoque más directo, el sistema financiero, la innovación de estas nuevas tecnologías, el uso de estas es constante y no hace más que “beneficiar el vínculo cliente – entidad”, pero así como puede presentar beneficios, presenta retos, retos que no solo estarán a cargo del Estado fiscalizarlos, sino también de la misma entidad.

En agosto del 2018 se informó de un ataque a nivel global en donde se iba a emitir un hackeo masivo en el sistema financiero que permitiría a estos cyber criminales robar millones de dólares, dicho ataque se efectuaría hackeando a la entidad bancaria para adquirir información de sus clientes, de esa forma suplantar la entidad de estas personas y clonar sus tarjetas para que en uso de su identidad puedan retirar o realizar transferencias masivas generándoles una pérdida económica de gran magnitud. Asimismo, muchos usuarios denunciaban en redes sociales que estaban presentando inconvenientes con sus cuentas bancarias, así como el acceso a los cajeros automáticos, dándose un indicio de que este cyber crimen se podría estar efectuando.

El 17 de agosto, la Asociación de Bancos del Perú, tomó conocimiento de estos problemas y emitió un comunicado mencionando lo referido: “ASBANC informa que, como parte de su labor de velar por el óptimo funcionamiento del sistema financiero nacional, detectó que desde las 3 de la mañana de hoy se vienen realizando una serie de ataques cibernéticos contra distintos agentes del sistema financiero mundial. En el caso peruano, ni bien se recibió la alerta, los asociados de ASBANC activaron sus protocolos de seguridad y han monitoreado sus sistemas para prevenir cualquier situación que afecte el normal desenvolvimiento de las actividades bancarias en el Perú (ASBANC, 2018)

Desde el 21 de octubre del año 2013 existe la Ley Nº 30096 que regula los delitos informáticos, siendo el artículo 9 de dicha ley que tipifica el delito de suplantación de identidad como el delito en que una persona puede suplantar la identidad de una persona jurídica o natural ocasionando un perjuicio material o moral, a raíz de ello y siendo un delito casi nuevo gracias a la integración de estas nuevas tecnologías existe la necesidad de investigar esta realidad debido a que hasta el año en curso existen muchas personas que se ven afectadas gracias a la facilidad que tienen algunas personas en usanza de sus destrezas suplantar identidades para adquirir tarjetas bancarias, líneas móviles y hacer uso de ellas ocasionando un daño económico, material y moral a las personas usurpadas, deviniendo de ello, incluso, que las personas agraviadas deben defender su nombre ante estas grandes empresas y encuentren una desatención, ineficiencia y desconocimiento al momento de dar a conocer el hecho del que son víctimas.

La transformación digital de la que se habla ya ocurre como instrumento de inmediatez de las entidades del sistema financiero hacia el cliente, pero, así como estas nuevas tecnologías y transformación digital es evolutiva, constantemente las normas y los organismos reguladores deben ir a la par con esta evolución.

Así como lo menciona, Villavicencio, donde se expresa las principales características que demuestran la vulnerabilidad en el mundo informático:

a) No se establecen jerarquías en la red por lo que no se puede establecer un control y dificulta la originalidad de la información que se vierte.
b) Con la evolución de los medios informáticos y la sociedad se acrecienta los usuarios con acceso a medios informáticos.

c) Los cibernautas al navegar lo hacen de forma anónima lo cual dificulta el reconocimiento y la persecución del delito a través de estos medios.
d) Existe una facilidad de uso de estos medios informáticos para alterar datos y destruir sistemas informáticos, por lo que dificulta su persecución. (2015, p.2).

Como lo menciona Vidal, una de las primeras regulaciones al respecto de los delitos informáticos o también llamado ciberdelitos, se encuentra en Estados Unidos con la aprobación de la Crime Control Act desde 1984 donde se empezó a juzgar a los primeros ciberdelincuentes, por ejemplo: el caso United States vs Robert Morris, quien sería el primer hacker encargado de propagar un virus (2018, p.3).

En otros países del primer mundo como España, en el año 1995 recién se empieza a regular los ciberdelitos incorporándolos en su Código Penal; sin embargo, estos no disponen de una Ley autónoma, solamente se encuentran sujetos a su Código Penal nacional. En este país, los medios informáticos son muy utilizados para diversas conductas financieras, ya sea compras, transferencias o adquisición de servicios; sin embargo, no poseen una norma que castigue la suplantación de identidad digital propiamente dicha. La suplantación de identidad es castigada con una pena privativa de libertad, pero establece condiciones como que sea permanente y que el perjuicio sea ocasionado con el uso del internet, es decir, evalúa el perjuicio que se ocasionó y no la comisión del delito por los medios que usó.

Nos menciona Hugo, que, en el Reino Unido, debido al hacking en el 1991, entró en vigor la “ley del abuso informático”, de acuerdo a esta ley, el éxito o el fracaso de los intentos de cambiar los de la computadora puede ser condenado hasta cinco años de prisión o una multa. Una parte de la ley prevé específicamente la modificación de datos no autorizada. Los virus se incluyen en esta categoría, las sanciones por liberar virus varían de un mes a cinco años, según el daño que causen (2014, p.75)

Debido a esto existe una imperante necesidad de investigar la protección de este delito, ya que las nuevas tecnologías exigen conocimiento amplios de informática, necesita gente experimentada y estudiada para la investigación de este delito porque el sujeto activo no es una persona que realizará este delito por medios

físicos sino que utilizará medios informáticos para su comisión, siendo una Ley nueva que integra tipificaciones nuevas el campo de la protección no debe estar muy desarrollado por lo que existiría mucha impunidad en la comisión de este delito.

Además, existe una problemática fija en el hecho de que el artículo 9 de la Ley de Delitos Informáticos, la cual tipifica el delito de suplantación de identidad desde que entró en vigor la Ley N° 30096 jamás fue modificada, ni por la Ley N° 30171 que es la única que ha modificado la Ley de Delitos Informáticos poniéndola acorde al Convenio de Budapest, siendo dato importante que el Perú no es parte de este Convenio. Siendo así, se trata de un artículo que necesita acogerse a la evolución de las tecnologías de información y del acceso de la sociedad a estas.

La presente investigación posee una justificación teórica porque integramos y nos basamos en la teoría del delito, la teoría de la tipicidad para legislar y estudiar los nuevos delitos informáticos y la teoría de la ubicuidad; justificación tecnológica ya que se enseña nuevos medios informáticos de los que se deben tomar conocimiento para no ser víctimas del delito de suplantación de identidad; una justificación social porque ayudará a la sociedad a tomar conocimiento y de esa forma brindar recomendaciones o tomar medidas de prevención en el uso de instrumentos a los que se tiene acceso cuando eres parte de un sector financiero y una justificación legal, debido a que existe una norma autónoma, Ley Nº 30096 y su modificatoria, Ley Nº 30171 que regula los delitos informáticos, conjuntamente con el Código Penal peruano y las normas y convenios internacionales que regulan la materia.

Sobre la base de esta realidad problemática desarrollada se plantea el problema general y los problemas específicos de la presente investigación. El problema general de la investigación es ¿De qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019? Los problemas específicos de la presente investigación son los siguientes: ¿De qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?, ¿De qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?, ¿De qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?

El objetivo general es determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019. Siendo los objetivos específicos los siguientes: Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019, determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019, determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

Muchas personas que son víctimas de este delito en el sistema financiero tienen que demostrar su verdad, su honor, su honestidad a estas grandes empresas como si no fuese suficiente el hecho de haber sido dañadas en gran magnitud, es por ello que el supuesto general de la presente investigación es: Los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019. Teniendo como supuestos específicos las siguientes: El vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019. El spyware incide en la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019, El spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019, El skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

II. MARCO TEÓRICO

Siguiendo la línea de investigación el delito de suplantación de identidad es indefectible integrar como antecedente de referencia la investigación realizada por la Oficina de las Naciones Unidas contra la droga y el delito de Viena denominada: Manual sobre los delitos relacionados a la identidad.

La investigación realizada plantea que en el marco de las naciones que se encuentran dentro de la Organización Mundial de Naciones Unidas, cuáles son las naciones que tipifican estos delitos relacionados a la identidad.

Donde muestra que será forzosa una actualización a la legislación, asimismo usando el derecho comparado trabajado en la investigación ya citada, cambiar las denominaciones de algunos delitos para poder incorporar otras conductas en la tipificación del delito. Por ejemplo, dicho Manual desarrolla sobre el hurto de identidad y lo relativo a este delito, sugiriendo soluciones de gestión de la identidad como medidas técnicas relacionadas con la gestión de la información de la identidad, y, por ejemplo, estrategias destinadas a minimizar el alcance de dicha información, la información necesaria para realizar transacciones de comercio electrónico puede afectar el riesgo de hurto de identidad (2013, pp.3-6).

Asimismo, contribuye a esta investigación en desarrollo la tesis elaborada por Celi y Diaz (2017) denominada: Políticas de seguridad de la información en función del comportamiento de los usuarios de tecnologías de la información en el sector microfinanciero de Lambayeque de la Universidad Nacional Pedro Ruiz Gallo.

Siendo su objetivo general evaluar los factores que influyen en el comportamiento de los usuarios de tecnologías de información en el sector microfinanciero de Lambayeque por lo que su muestra se basó en 24 entidades financieras de Lambayeque, seleccionando solo 8 y distribuyendo 365 cuestionarios. Finalmente, una de sus conclusiones:

Considera que para poder brindar mejores políticas de seguridad en el sector financiero se debe analizar el ambiente interno y externo de los trabajadores de este sector, estos ambientes influyen en las conductas de los trabajadores de este sector y es por ello que con la aproximación que tienen pueden ser supuestos de hecho para cometer el delito de suplantación de identidad, con la aproximación a la

información y las tecnologías del sector financiero; asimismo, en la tesis antes citada menciona que tomado ocho factores necesarios ayudarían a brindar mejores políticas de seguridad como: integración, compromiso, medidas de disuasión, tecnologías orientadas al control, motivación, entrenamiento, usabilidad de herramientas de seguridad, presión del tiempo, carga de trabajo y concienciación, siendo así estos factores que influirán a la conducta de los trabajadores del sector financiero, evaluando ello se podría evitar cometer el delito brindando eficientes políticas de seguridad.

Por otro lado, tenemos Balcazar (2017) en su tesis elaborada, también arriba las formas o medios informáticos en los que se pueda cometer el delito de suplantación de identidad, identificando como su objetivo general determinar qué medidas de seguridad deben incorporarse en la Resolución Nº 6513-2013-SBS, redactando en una de sus conclusiones lo siguiente:

Se establece que una de las medidas más importante a integran en la Resolución Nº 6513-2013-SBS es el uso del sistema biométrico porque así se evitaría conductas no reconocidas en la adquisición de tarjetas de uso financiero, por lo que se estaría brindando una protección al consumidor financiero, priorizando el reforzar las áreas de supervisión de entidades financieras o bancarias.

Asimismo, Paredes (2013), en su tesis elaborada también brinda un aporte importante sobre los sistemas informáticos que usan para cometer delitos, estableciendo como objetivo general demostrar que las conductas que emplean o se basan en sistemas informáticos se encuentran deficientes o inadecuadamente tipificadas, para ello utilizó como muestra 18 entrevistas a magistrados o abogados especialistas consignando así en una de sus conclusiones:

Coincide en que se debe modificar la regulación o en su defecto realizar una reforma integral de la norma donde se deberá integrar diversas conductas ilícitas, determinar los bienes jurídicos en afectación y que estas se deben tipificar como delitos de peligro.

Aportando a lo antes vertido en la conclusión de la tesis antes citada cabe mencionar que los delitos de peligro son aquellos delitos que pueden finalizar ocasionando un daño irreparable o no al bien jurídico, así como también existen

delitos de peligro en los que será necesario el uso de medios y que eso medios ya supongan un peligro para la afectación de algún bien jurídico.

Zea (2016) en su tesis denominada: Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala por la Universidad Rafael Landivar de Guatemala, en esta tesis internacional se brinda un aporte importante al presente proyecto de investigación siendo que también investiga el delito de suplantación de identidad, en su legislación nacional se le denomina robo de identidad mediante dispositivos electrónicos, teniendo como objetivo principal describir el fenómeno del robo de identidad en Guatemala a través de dispositivos electrónicos, brindando la siguiente conclusión:

Cuando existe concurso de delitos que derivan del robo de identidad que ocasionan meramente daños económicos, en juicio se consigue el resarcimiento económico del año que se ocasionó, siendo así que el imputado no logra efectuar alguna pena debido a la imputación del delito ya que el daño ocasionado ya se encuentra resarcido por lo que las víctimas de este delito pierden el interés en la búsqueda de la justicia con el fin de castigar el hecho en búsqueda de que no se vuelva a cometer por parte del imputado.

Merchán (2012) en su tesis elaborada, denominada: Reformas al Régimen Penal Ecuatoriano en cuanto al delito de suplantación de identidad de la Universidad de Loja de Ecuador. Aquí visualizamos que la denominación del delito es la misma que se establece en el artículo 9 de la Ley Nº 30096 “ley de delitos informáticos” regulada en el Perú, ofreciendo un colaborando con reformas que se pueden incorporar a la legislación peruana para mejorar la persecución del delito, teniendo como objetivo general realizar un estudio socio-jurídico y doctrinario con respecto al delito de suplantación de identidad, incorporando así las siguientes conclusiones:

Siendo la identidad un particularidad propia del individuo en la cual contiene aspectos como el nombre, nacionalidad, domicilio, filiación, entre otros datos personales que permite a la persona ser sujeto de derecho y tener derechos y obligaciones; asimismo aplicando la encuesta hecha a la muestra se tomó que casi el cien por ciento de las personas encuestadas manifiestan que este delito ocasiona un grave daño y que este no puede ser resarcido jamás debido que la persona agraviada ya queda expuesta.

Hunter (2009) en su tesis “Computer Crime and Identity theft” dado que esta tesis contribuye especificando las políticas de estado y medidas que utiliza el gobierno para combatir este tipo de crímenes estableciendo así en una de sus conclusiones:

Los problemas de robo de identidad es uno que requiere un enfoque holístico, donde los negocios, consumidores, organizaciones y gobiernos trabajan todos juntos para contrarrestar la amenaza de robo de identidad. En este estudio, en la actualidad no existe un documento integrado para planificar que describe una visión tan holística e integrada del problema. La investigación por lo tanto tiende para sugerir que se deben hacer esfuerzos concertados para lograr un enfoque más integral comprensión del contexto y el alcance del robo de identidad.

Los delitos informáticos se encuentran tipificados en el capítulo X del título V donde se tipifican los delitos contra el patrimonio; estos se encuentran tipificados cuatro artículos, siendo los siguientes:

Artículo Nº 207-A: Interferencia, acceso o copia ilícita contenida en base de datos.

Artículo Nº 207-B: Alteración, daño o destrucción de base de datos.

Artículo Nº 207-C: Circunstancias cualificantes agravantes.

Artículo Nº 207-D: Tráfico ilegal de datos.

Los artículos antes mencionados que se encontraban tipificados en el Código Penal de 1991 fueron derogados por la Ley Nº 30096 el 22 de octubre de 2013 en la que se incorporan nuevos delitos informático.

Sobre la Ley Nº 30096, Villavicencio sostiene al respecto:

> “(…) Esta Ley de Delitos Informáticos está conformada por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII)”. (2015, p.287)

Seguidamente se publica la Ley Nº 30171 la cual modificará la Ley de delitos informáticos adecuándola al Convenio de Budapest sobre la ciberdelincuencia,

integrando entre las conductas la posibilidad de cometer los delitos deliberadamente e ilegítimamente.

Ahora bien, la presente investigación realmente no trata en su totalidad los delitos informáticos, sino un solo delito informático llamado “Suplantación de identidad” el cual se encuentra tipificado en el artículo 9 de la Ley Nº 30096 en el que se expresa lo siguiente:

“El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años”.

Siendo que el sujeto activo no será cualquier persona, sino una persona con destrezas o habilidades en informática que podrá cometer el delito, el sujeto pasivo si se tratará de cualquier persona con un historial financiero, por la parte de la tipicidad subjetiva requiere de dolo, es decir, intención y voluntad de cometer el delito.

Para Villavicencio, identifica que se trata de un delito de resultado porque en un inicio te exige que se cometa la suplantación, pero eso es lo que presume la comisión del delito, pero no basta solo con ello, sino que exige que se cometa un prejuicio o daño a la persona natural o jurídica como resultado (2015, p.298).

Por ejemplo: cuando una persona suplantando una identidad mediante medios como telemarketing o páginas de internet obtiene tarjetas de crédito, líneas móviles, realiza compras por internet, etc.

La RAE define a la informática como un conjunto de informática de conocimiento científico y técnico que permita la información automáticamente con la ayuda de computadoras.

La informática es accesible en base a la evolución de la sociedad y de la informática y esto hace que las personas tengan acceso a un mundo globalizado donde es fácil conectar a personas de diferentes orígenes para un mismo fin tan solo usando la informática, es por ello que, es importante investigar su conexión con los delitos porque, así como la sociedad evoluciona, evoluciona la informática y con ambas evoluciones, también lo hace la delincuencia, en específico la ciberdelincuencia.

En el convenio de Budapest sobre la ciberdelincuencia en su artículo 1 define al sistema informático como cualquier dispositivo aislado o grupo de dispositivos conectados o relacionados entre sí, cuya función o función de cualquiera de sus elementos es el procesamiento automático de los datos de ejecución del programa. Por otro lado, para buscar una definición sobre los delitos informáticos se requiere muchas veces que esta conceptualización este en la normativa punitiva en este caso, sin embargo, la normativa peruana no establece en si una definición de delitos informáticos, solamente regula los diferentes delitos típicos existentes.

Por su parte, Tellez define a los delitos informáticos como ""actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijuridicas y culpables que tienen a las computadoras como instrumentos o fin" (concepto típico)" (2008, p.188).

En comentario a la definición de Tellez se puede identificar que utiliza dos métodos de conceptualización para definir a los delitos informáticos, una conceptualización atípica en la que se conoce como una conducta no normada y una conducta típica en la que sí está normada, en base a ello no se podría escoger que definición le va mejor porque ambas definen el delito informático, siendo que el delito es una conducta antijurídica, culpable y típica y que a su vez termina siendo una conducta ilícita, para conectarlo a la informática usa el término "computadora" como instrumento para la comisión de este delito; sin embargo, podemos manifestar que una computadora a estas alturas no es el único instrumento para cometer un delito informático, pero se entiende como un término que abarca toda la informática.

Es necesaria una distinción entre delitos informáticos y actividades ilícitas por medios informáticos, sobre ello Peñaloza, nos expresa que existe distinción, el último es en aplicación de las herramientas; por ejemplo, en la trata de personas, muchas de las personas traficadas son vendidas o adquiridas como si fuese mercancía. El departamento de Estados Unidos anunció el 3 de junio de 2005 a través de medios televisivos que las victimas de esta mafia eran entre 6 y 800.000 (principalmente niños), el mercado aplicable de la pornografía infantil es también uno de los más activos y de "trata de blancas" de mujeres jóvenes (especialmente mujeres de países subdesarrollados). Atraído por la promesa de una vida mejor, mas tarde forzada a la prostitución. El comercio de material radioactivo es otra

residencia en avanzada, las cuales hoy en día tienen a los medios informáticos y son característicos de la economía global (2010, p.366).

Sobre el sistema financiero y su conexión con los medios informáticos también son el objetivo de uso de estas tecnologías de la información y comunicación en actividades ilegales, que es uno de los sectores más afectados por esta mafia. Los narcotraficantes utilizan redes financieras y equipos de enseñanza avanzados para lavar dinero, también conocido como lavado de dinero o reciclado de activos o capital generalmente derivado de transacciones de drogas. De esta forma, una gran cantidad de "dinero caliente" circula libremente por el mundo sin ningún control o ley que pueda suprimirlos. La existencia de países con regulaciones menos estrictas en materia de regulación constituye sus propios paraísos fiscales, que pueden enviar grandes cantidades de dinero de actividades ilegales.

Por otro lado, Rico, define al delito informático citando a la doctrina española como actos que ponen en peligro o dañan la integridad, la confidencialidad o la disponibilidad de datos y sistemas informáticos sin complicar el hecho de que también pueden poner en riesgo o dañar bienes jurídicos protegidos por la legislación (2013, p.209).

Retornando a Tellez menciona que existen ciertas características para los delitos informáticos: conductas que solo pueden ser cometidas por cierto grupo de gente que necesariamente debe reunir ciertas habilidades que solo ellos pueden poseer en base a sus conocimientos, es decir que el sujeto activo no será cualquier persona, sino alguien con habilidades requeridas, que estas conductas se desarrollar en la inmediatez que tiene el sujeto activo en el desarrollo de sus funciones y con las herramientas que este posee, por ejemplo: Un ejecutivo de banca y negocios, son conductas planificadas que requirieron de una investigación para su comisión, es decir, no a cualquiera le robaras porque no sabrás si esta persona pertenece al sector financiero, más bien el sujeto activo tendrá acceso a cierta información que ayudará a develar a su víctima, el perjuicio que ocasiona la comisión del delito informático es en su mayoría un perjuicio económico, este tipo de conductas ilícitas se pueden cometer rápidamente con un solo clic, la falta de regulación sobre los delitos informáticos es muy ambigua o escasa, por lo que, existen muchos casos denunciados que duran mucho por su difícil investigación, la mayoría se cometen con dolo, los menores de edad suelen

ser muchas veces los sujetos activos y se pueden cometer de forma masiva porque no requiere de muchos instrumentos (2008, p.188).

Con respecto al delito de suplantación de identidad como ya lo manifestamos párrafos arriba se encuentra regulado en el artículo 9 de la Ley de delitos informáticos, reconociéndose así como un delito de resultado porque se exige que en uso de tecnología de información o comunicación suplanten la identidad de una persona natural o jurídica se cometa un perjuicio, este perjuicio puede ser económico o moral, pero en la presente investigación desarrollaremos el perjuicio económico que se ocasiona en la comisión de este delito. La RAE define suplantar como emplear en el uso de malas artes el sitio de alguien, en este caso podrían ser muchas características de ese alguien, ocasionándole un perjuicio.

Siendo un delito contra la fe pública, se puede encontrar en conflicto con ciertos delitos de falsedad genérica, si bien el delito manifiesta que el perjuicio debe económico y moral, sabemos que el derecho penal no puede perseguir un delito que atente a la moral, por lo que, solo debería ser un perjuicio económico.

Puelles, manifiesta, a diferencia nuestra, que el delito de suplantación de identidad solo debería sancionar “algún perjuicio” y no solo lo patrimonial y moral (2014, p.23).

Por su lado, Romero, para brindar una aproximación conceptual sobre la usurpación de identidad menciona que la identidad son aquellas características o particularidades que definen o diferencian a una persona de las demás (2019, p.849). Asimismo, estas características ayudaran al sujeto activo a identificar a su víctima.

Existe un conflicto entre llamar usurpación o suplantación de identidad, algunas normas optan por llamar usurpación, otras por llamar suplantación. Para ello, Vidal, menciona una diferenciación de conceptos y de esa manera podríamos identificar cual es el correcto termino para nuestra legislación, menciona que la suplantación de identidad en internet es aquella conducta por la cual una persona suplanta a otra, es decir, mediante actuaciones se hace pasar por una persona ajena a su entorno, apropiándose de derechos y facultades que posee la persona suplantada y hacer uso u ejercicio de ello, por otro lado, la usurpación de identidad en internet y esa se comete desde que el sujeto activo hace uso de los derechos

y facultades de la persona usurpada, actuando en nombre de esa, pero para beneficio propio (2018, p.5).
Sobre ello se identifica que la diferencia es mínima por lo que es muy difícil determinar si la norma seguirá llamándose suplantación de identidad o usurpación de identidad, existen legislación que la llaman hurto de identidad.

Por otro lado, los medios informáticos tienen su definición en sí mismo, a consideración propia se podría definir a los medios informáticos como aquellos instrumentos que se usan en búsqueda de información, la información puede ser de cualquier tipo. Según Hugo, el uso de computadoras, es decir, el uso de sistemas informáticos, tiene un impacto fundamental en el desarrollo social de cada país (directamente relacionado con el grado de desarrollo cultural y económico). Por lo tanto, la gente también dice que la lucha por el poder político y económico ha pasado del ámbito del control de una enorme energía al ámbito de la información (2014, p.70)

Para Mayer, la informática es un campo de conocimiento que presenta altas especificaciones y complejidad técnica, la cual se refleja en el uso de términos y códigos en específico, siendo así, constituyen un lenguaje encriptado que lo hace propio. Por otro lado, en el desarrollo los cálculos continúan padeciendo modificaciones en muy poco tiempo; Albacea, un legislador y juez del sistema procesal penal, cree necesario afrontar este campo con conocimiento multidisciplinario que comprende características básicas y busca adaptarse a él trabajando en base a una realidad cambiante (2016, p.160)

Lopez, manifiesta que los medios informáticos están establecidos en un software y articulados en una computadora, presentando así diversas características; su escritura alineal presenta una gran flexibilidad, altamente interactivo, auto aprendizaje, la persona desarrolla su conocimiento de manera grupal o individual (2006. p.28). Los medios informáticos tienen diferentes funciones, algunas son motivadoras, evaluadoras, instructivas, informativas, etc. Estas funciones ayudaran a su desarrollo y empleo.
En el universo de la informática existen muchos medios informáticos, pero antes de abarcar los medios informáticos de los que se hablará en esta investigación,

debemos mencionar que los medios informáticos pertenecen al universo de la tecnología de la información y comunicación (TIC) donde se desarrollan un gran contenido de medios informáticos, sobre ello, Rivera, manifiesta que los medios informáticos carecen de corporalidad, es lo que hace difícil la investigación en la persecución del delito; sin embargo el autor manifiesta que estos si deben tener corporeidad, porque si bien se determinó que la electricidad no tiene cuerpo lo que hace fácil su inexistencia, siempre deja huella (2008, p.307). Esto hace que de alguna forma en la persecución del delito de suplantación de identidad siempre se encontrará la huella que dejo el sujeto activo en el uso de los medios informáticos para su identificación.

En esta investigación hablamos solo de tres medios informáticos, ellos navegan dentro del universo de la tecnología de información y comunicación, escogimos a estos medios informáticos por su alta incidencia en la comisión de los delitos informáticos.

Según Yeboah & Mateko en su artículo Phishing, Smishing y Vishing: An assesment of threats against mobile devices, definen al vishing como un mecanismo dentro de la tecnología de la información y comunicación que se comete usando una voices notes o línea telefónica basándose en habilidades de la ingeniería social para recaudar información delicada, como lo es la información financiera de la persona, para engañarla y así hacer uso de su identidad (2014, p.300). En uso de este medio informático, las personas con conocimientos sobre ingeniería social realizan llamadas a distintas personas, en la que solicitan información delicada, el sujeto pasivo que probablemente confía o se encuentra necesitado brinda esta información sin saber que al otro lado de la línea se está cometiendo un fraude telefónico, siendo que el sujeto activo ha adoptado esta modalidad para obtener cuentas financieras, las contraseñas y otros datos del usuario.

El spyware es un malware y tal como indica su nombre se trata de un programa malicioso usado para recaudar información que se extrae desde una computadora, usando una computadora, valga la redundancia, transfiriendo esta información a un lugar externo y por lugar, me refiero a un sitio dentro del universo de la informática, sin el asentimiento y desconocimiento del propietario de dicha información. En palabras más entendibles, se trata de aquel programa que sin

conocimiento podemos descargar o ingresar brindando nuestros datos personales que ayudaran a que el sujeto activo en uso de la ingeniería social transfiera estos datos y conduzcan a la comisión del delito de suplantación de identidad.

El skimming es un método de hurto de información muy utilizado y que se encuentra unido al delito de clonación de tarjetas, puesto que se trata del hurto de la información de tarjetas de crédito o débito utilizado para producir un perjuicio económico, es decir, es el uso fraudulento que se da a estas tarjetas que evidentemente no pertenecen al sujeto activo, pero que en nombre del propietario de dichas tarjetas realiza transacciones como compras, transferencias o gastos.

Cabe mencionar que para este último medio informático y a los demás no se necesita principalmente la presencia física del sujeto activo, sino de sus conocimientos, este aspecto, como lo describen los conocedores de ingeniería informática.

Por su parte, Hugo manifiesta que en los países latinoamericanos carecen de legislación que específicamente regule los delitos informáticos, en Argentina no podemos encontrar una clasificación de delitos informáticos, solo se protegen base de datos o softwares, en Chile siendo el primer país de Sudamérica que tipifica con sanción los delitos informáticos mediante una ley (2014. p.7)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El Consejo Nacional de Ciencia y Tecnología e Innovación Tecnológica (CONCYTEC) en la Ley Nº 30806, menciona que la investigación básica adquiere un conocimiento más completo a través de aspectos fundamentales de hechos de observación o de la relación que existe entre ellos (2018, p.7). La presente investigación desarrolla este tipo y tiene como propósito adquirir y recopilar información para construir una base de conocimiento, que se pueda agregar a la información ya existente.

La presente investigación es cualitativa y está dirigida a la comprensión de los fenómenos sociales y jurídicos, siendo cualitativa por su utilidad y desarrollo jurídico-doctrinario, en el cual el argumento del orden legal es crucial para crear nuevos conceptos que aporten una renovación en la legislatura penal sobre los delitos informáticos, en específico del delito de suplantación de identidad.

Esta investigación está orientada a nutrir el entendimiento y raciocinio de los futuros investigadores, con el fin de desarrollar mejoras para nuestra legislatura en la materia penal, incluso ayudando a la doctrina adquirida por los nuevos investigadores, de esta forma exterminar la impunidad sobre conductas no tipificadas o no castigadas por la legislatura penal.

Por su lado, Hernández, Fernández & Baptista, sobre el enfoque cualitativo menciona que “utiliza la recolección y análisis de datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación” (2014, p.7).

Según el diseño, la presente investigación es interpretativo basado en la teoría fundamentada porque busca, en la recolección de los datos que se emplearon, crear nuevas teorías, brindar recomendaciones y ampliar el conocimiento de los futuros investigadores en esta materia respaldándonos de las entrevistas que se realizaran en este campo.

3.2. Categorías, subcategorías y matriz de categorización apriorística.

Tabla 1

Categorías	Definición conceptual	Sub categorías
Delito de suplantación de identidad	Es aquel delito en el que una persona con habilidades o destrezas informáticas suplanta la identidad de una persona natural o jurídica ocasionándole un perjuicio económico o moral.	• Regulación expresa • Suplantación • Identidad
Medios informáticos	Son aquellos instrumentos, medios, mecanismos que se encuentran en un ordenador y que son usados para desarrollar programas, hardware, servidores, entre otros.	• Vishing • Spyware • Skimming

Fuente: Elaboración propia.

3.3. Escenario de estudio

En referencia a lo citado párrafos arriba y correlativamente con la naturaleza de la presente investigación, esta no posee población ni muestra por lo que los datos a analizar resultan del aporte de personas especialistas y destacadas en la materia, al respecto se tendrá a 2 abogados penalistas, 2 especialistas o ingenieros informáticos.

Participantes

Tabla 2

Nº	PARTICIPANTES	APELLIDOS Y NOMBRE	GRADO	CARGO	FUNCIÓN
1	Abogado	Tello Meneses Caroline	Magister	Secretaria de la Primera Sala Penal para Reos en Cárcel	Supervisar a los asistentes judiciales y llevar audiencias

2	Abogado	Felix Eduardo Dorregaray	Titulado	Abogado penalista independiente y conciliador	Litiga y resuelve conciliaciones
3	Ingeniero de Sistemas	Carlos Escobar Cornejo	Titulado	Gerente general de KRUMA	Desarrollo, seguridad e implementación de plataformas informáticas
4	Ingeniero de Sistemas	Percy Aquino Cruz	Titulado	Responsable de seguridad de servidores informáticos	Se encarga de la seguridad de las redes informáticas

Fuente: Elaboración propia.

3.4. Técnicas e instrumentos de recolección de datos

En el marco del desarrollo del presente proyecto se usarán técnicas e instrumentos propios de investigación cualitativa, debido a ello se consideran los siguientes aspectos:

Entrevistas: Al respecto Kerlinger menciona que se utiliza la entrevista personal para adquirir una mejor información, construyendo y elaborando de forma cuidadosa un cuestionario, esto como instrumento la recaudar la información por medio de la entrevista personal, siendo esta una situación interpersonal donde personas denominadas entrevistador y entrevistado resuelven preguntas pertinentes y diseñadas para responder el problema de la investigación. (2002, p.631). En la presente investigación la guía de entrevista está integrada por 12 items o preguntas

Análisis de documentos: Esta técnica es usada para adquirir teorías, conceptos, definiciones y antecedentes teniendo como fuentes internacionales o nacionales con el fin de nutrir la investigación, obteniendo estos datos de forma física o digital. La cual está elaborado por una matriz que responderá los objetivos.

Tabla 3

Nº	EXPERTOS	APELLIDOS Y NOMBRE	GRADO	CARGO	% (PORCENTAJE)
1	**METODOLÓGICO**	Rosas Job Prieto Chavez	Doctor	Coord. De investigación de la Escuela Profesional de Derecho de la Universidad Cesar Vallejo	90%
2	**ESPECIALISTA**	Fernando Tomas Cañari Flores	Abogado	Docente de la Universidad Cesar Vallejo	95%

Fuente: Elaboración propia.

3.5. Procedimiento

La presente investigación se desarrolla integrando teorías, antecedentes, normas, artículos, asimismo con la creación de una guía de entrevista en base a un instrumento validado.

3.6. Rigor científico

Correspondiendo al diseño, tipo y métodos de recolección de datos de la presente investigación, se busca certificar que los resultados que se obtengan de la presente investigación sean confiables y validos con el fin de determinar que o cuán importante es la tipificación del delito de suplantación de identidad y los medios informáticos.

Ahora bien, para recolectar estos instrumentos de datos estos deben tener ciertas características imperantes para su ejecución: la confiabilidad y la validez.

Según Kerlinger, la confiabilidad “es la falta de distorsión o precisión de un instrumento de medición” (2002, p.583). Es decir que, si el instrumento de recolección de datos es preciso u oportuno para la investigación, la confiabilidad será buena y fácil de demostrar.

Kerlinger, también nos menciona con respecto a la validez que para estudiarla es necesario tener la conceptualización, naturaleza y significado de las variables, de no ser así será imposible su estudio (2002, p. 603)

3.7. Método de análisis de la información

En la presente investigación utilizamos como métodos de análisis, el método jurídico debido a que es una investigación basada en normas, doctrina y jurisprudencia, método de inductivo porque desmembraremos y analizaremos las normas y los documentos recolectados; método hermenéutico por la interpretación que se le da a las teorías y por las definiciones obtenidas y un método sistemático porque el contenido del presente proyecto es un acopio de distintas informaciones sobre la materia.

3.8. Aspectos éticos

En cuantos al aspecto ético de la presente investigación, la información que se recaudó para el desarrollo de sus distintas partes se hace de investigaciones científicas nacionales e internacionales relacionadas al título o a la materia de esta investigación, por lo que, se verificó que se tratase de fuentes confiables que serán citadas de acuerdo a las normas de Derecho de Autor, la Ley de Propiedad Intelectual (Decreto Legislativo Nº 822), derechos de autoría y de acuerdo a la norma de cita y referencia de la séptima edición. Siendo que este trabajo es de autonomía propia y que cumple con todas las normas brindadas para su desarrollo siguiendo los principios éticos.

IV. RESULTADOS Y DISCUSIÓN

Mediante el uso de herramientas utilizadas para la recopilación de información, se describe los resultados obtenidos en este estudio, métodos que han sido verificados por expertos en la materia y en el método.

Por otro lado, cabe mencionar que el resultado es la parte más importante de la investigación, debido a que refrenda el propósito de una investigación científica, teniendo en cuenta que se basa en el sustento, prueba, explicación, argumento y análisis de todos los resultados en cada entrevista realizada, siendo los mismos indicadores que las preguntas planteadas han sido formuladas en base al conocimiento y dominio del marco teórico.

Siendo así, se pasará a desarrollar y a profundizar la información obtenida de las entrevistas realizadas en el presente trabajo de investigación, dichas entrevistas se ejecutaron en el desarrollo del trabajo durante los meses de octubre, noviembre y diciembre del presente año, la información adquirida sirve para ostentar los supuestos jurídicos del presente trabajo de investigación, partiendo por el objetivo general compuesto por 3 preguntas, así como los objetivos específicos dando un total de 12 de preguntas, según se manifiesta a continuación:

Objetivo general: Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

Sobre la primera pregunta planteada a este objetivo, el ingeniero informático Escobar, C. (2020) manifiesta conocer sobre el delito de suplantación de identidad y los medios informáticos al igual que el técnico Aquino, P. (2020) y el abogado Dorregaray, F. (2020). Escobar, C. (2020) al igual que Aquino, P. (2020) conocían al delito de suplantación de identidad no como un delito, más bien en un sentido más común, siendo ambos ingenieros de sistemas, mencionaron conocer más sobre los medios informáticos. Por otro lado, el abogado Dorregaray, F. (2020) conocía sobre la regulación de este delito dentro de la Ley de Delitos Informáticos, pero manifestó no conocer mucho sobre los medios informáticos, manifestando que solo conocía los celulares, computadoras y aplicaciones de pago bancarias. Por su lado, la abogada Tello, C. (2020) refiere su propia definición sobre el delito de suplantación de identidad consistente en simular ser otra persona obteniendo un

beneficio de ello, refiere sobre los medios informáticos utilizados en los delitos que se ejecuta en un entorno digital con el uso de internet causando un daño.

Sobre la pregunta dos de este objetivo, Escobar, C. (2020) manifestó no conocer sobre el delito de suplantación de identidad en tanto no podría opinar sobre la modificación de su regulación, por su lado, Aquino, P. (2020) considera que deberían existir penas más severas y tratándose de un delito informático este debe ir evolucionando día a día con las nuevas tecnologías. Por otro lado, Dorregaray, F. (2020) manifestó que la regulación del delito de suplantación debería recibir una pena más fuerte e incluir agravantes en su regulación, puesto que en la comisión de dicho delito se pueden ocasionar daños muchas veces irreversibles. Tello, C (2020) considera también que se debe modificar la forma de regulación del delito en la Ley.

En base a la pregunta tres, Escobar, C. (2020) menciona que no se deberían regular los medios informáticos, lo que se debe hacer es educar a las personas sobre estos medios y no caigan como víctimas en estos delitos, en contrario, Aquino, P. (2020) menciona que, si se deberían regular, se debería castigar a personas mal intencionadas que abusan de dichas herramientas tecnológicas para cometer este delito. Por su lado, Dorregaray, F. (2020) al igual que Aquino, aporta que también se debe regular los medios informáticos, puesto que "existen medios más peligrosos que simplemente crear un perfil falso en Facebook". Tello, C. (2020) considera que debe ser regulado los medios informáticos como artículos suscritos a la Ley.

Objetivo específico 1: Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

Respecto a la pregunta uno, Escobar, C. (2020) manifiesta que, si tuvo una experiencia con el uso del vishing por ciberdelincuentes, mencionando que una vez lo llamaron suplantando a un familiar, queriendo sacar información sobre este familiar; sin embargo, ya conocía sobre esta modalidad y colgó inmediatamente. Por su lado, Aquino, P. (2020) menciona que, si lo llamaron de una empresa y con el simple hecho de responder "aceptó" la suscripción a una empresa que se dedica a crear ringtones, pagando, sin poder recuperar ese dinero. Asimismo, sobre su experiencia con el vishing, Dorregaray, F. (2020) nos manifestó que no conocía al

vishing, pero con la explicación de la entrevistadora, se percató que había sido víctima de esta modalidad de suplantar la identidad, siendo que una vez lo llamaron de una entidad bancaria diciéndole que identificaron movimientos sospechosos en su tarjeta, solicitándole datos como su número y el CVV de la tarjeta, notando el abogado la insistencia de la persona que lo llamó inmediatamente sospechó y colgó la llamada sin brindar esta información. Tello, C. (2020) no ha padecido experiencia alguna al respecto de esta pregunta.

En base a la pregunta dos, Escobar, C. (2020) mencionó que el vishing favorece a que el delito de suplantación de identidad se cometa con más facilidad, Aquino, P. (2020) manifiesta que es un tipo de fraude electrónico que usan los ciberdelincuentes para robar datos personales de las personas suplantando identidades de una empresa bancaria; Dorregaray, F. (2020) nos manifiesta que se trata de una modalidad muy peligrosa de identificar, es decir, que es difícil identificar si estamos siendo víctimas de un ciberdelincuente o si es cierto porque se suplanta la identidad de una entidad bancaria sin ningún tipo de tapujos. Tello, C. (2020) responde manifestando que se trata de una simulación o suplantación de entidades bancarias para hacer creer al usuario que se ingresa a una página que esta siendo guiado por la entidad financiera suplantada y así realizar las actividades que se deriven.

Escobar, C. (2020) refiere que el vishing debería regularse, siendo no muy conocedor de temas legales, pero sí de sistemas e informática por lo cual el uso de esta tecnología es usado para realizar delitos, por lo cual se debería castigar. Asimismo, Aquino, P. (2020) menciona que con el desarrollo tecnológico aparecen nuevas formas de estafas o engaños, por lo tanto, debería ser regulado. Por su lado, Dorregaray, F. (2020) refiere que se debe regular, siendo una conducta ilegal y como tal debe ser sancionada, Tello, C. (2020) manifiesta que no se encuentra regulado en el sistema legal, pero que si debería ser regulado a fin de evitar vacíos legales y que estos ciberdelincuentes burlen la norma.

Objetivo específico 2: Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

Sobre haber experimentado o ser victima de este medio informático, el abogado Dorregaray, F. (2020) refiere que no tenia conocimiento de la existencia de este

virus, a diferencia de la abogada Tello, C. (2020) y el ingeniero Escobar, C. (2020) brindando en sus respuestas que si aprecian conocer la existencia de este virus, incluso la abogada ha recibido correos electrónicos que contenían este virus, por su lado el ingeniero refiere conocer programas que se utilizan para la ejecución de este virus.

Dorregaray, F. (2020) no posee conocimiento de como favorece el spyware la ejecución del delito de suplantación de identidad, por su lado, Tello, C. (2020) expresa que se trata de un dispositivo electrónico que ingresa a la información personal que es recabada para la comisión de delitos por parte de estos ciberdelincuentes. Escobar, C. (2020) el spyware se ejecuta de la misma forma que el vishing y se usa para obtener información personal, mas detallado, Aquino, P. (2020) menciona que se trata de un software que se instala en una computadora con la cual se extrae información personal.

Todos los participantes coinciden en el que el spyware debe estar regulado; sin embargo, Dorregaray, F. (2020) expresa que se debería considerar como un agravante al igual que Aquino, P. (2020) es incisivo en que debería existir una ley autónoma que regule el uso de los medios informáticos.

Objetivo específico 2: Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

Los participantes Dorregaray, F. (2020) y Aquino, P. (2020) refieren haber tenido una experiencia muy penosa sobre el medio informático del skimming, el técnico fue víctima de ello al realizar un viaje a Estados Unidos, pero que la entidad bancaria pudo bloquear la tarjeta a tiempo, al igual que el abogado, quien fue víctima cuando acudió a un centro comercial y al realizar sus pagos identificó que se estaba realizando el skimming a su tarjeta bancaria, a diferencia de los participantes Escobar, C (2020) y Tello, C. (2020) quienes no tuvieron experiencia alguna.

El favorecimiento del skimming al delito de suplantación de identidad para Aquino, P. (2020) es mediante el escaneo de estas tarjetas bancarias en donde también obteniendo los datos personales pueden usar las tarjetas suplantando la identidad mediante el umbral cibernético para la comisión del delito. Escobar, C (2020) y Tello, C. (2020) coinciden en que favorece en la ejecución del delito de suplantación

de identidad, por su lado, Dorregaray, F. (2020) menciona que existe una mayor afectación al derecho de la identidad para la tramitación de la respectiva denuncia en la entidad bancaria, puesto que solicitan muchos requisitos para ello.

Tello, C. (2020) coincide en que este medio informático y en general la Ley de Delitos Informáticos debe estar en constante cambio por la naturaleza y esencia de la Ley, asimismo, Dorregaray, Aquino y Escobar acuerdan en sus respuestas que debe consignarse una regulación específica obligatoria.

Acotando un poco a la discusión y resultados de la aplicabilidad de la ficha de entrevista, responde a que todos estos especialistas a pesar de conocer la materia ya sea en el ámbito penal como el delito que se desarrolla o en el ámbito informático como los medios informáticos que se desarrollan, también tuvieron la condición de agraviado. Según Rodriguez Caro citado por Vidal, E. (2018) esto inicia generalmente cuando el cliente financiero percibe un correo, llamada, virus, algún mecanismo informático que tiene como finalidad inducir al usuario a una red maliciosa en la que suplantando a la entidad bancaria se obtiene la información personal de usuario afectado (p.13). Es decir, se puede reconocer dos sujetos o, mejor dicho, dos tipos de agraviados, porque las personas jurídicas, tal como lo expresa el articulo 9 de la Ley de Delitos informáticos, pueden ser agraviados

V. CONCLUSIONES

Por un lado se concluye que el delito de suplantación de identidad se encuentra incluso en cuanto a su regulación debido a que no presenta modificatoria alguna, siendo un delito muy ejecutado en los últimos años, siendo que en nuestro país existe un incertidumbre jurídica sobre la regulación de los medios informáticos en la ejecución del delito de suplantación de identidad, identificando también en la respuestas de los participantes de la investigación que existe un importante favorecimiento para su realización.

El vishing siendo un medio tecnológico usado para obtener información personal directa del agraviado por usos de mecanismos tecnológicos que suplantan al personal de una entidad bancaria favorece la comisión del delito de suplantación de identidad.

El spyware respectivamente se trata de un software malicioso que es ingresado al computador personal del agraviado y que mediante habilidades cibernéticas es usado para extraer información delicada para suplantar la identidad de una persona y generarle un perjuicio moral y económico.

El skimming es otro medio informático que favorece la comisión del delito de suplantación de identidad usando habilidades más físicas que cibernéticas para el escaneo de tarjetas bancarias en el que al igual que los otros medios informáticos anteriormente mencionados se obtiene información delicada que luego es usado usurpando la identidad del agraviado para generar un perjuicio directamente económico.

VI. RECOMENDACIONES

Es de necesidad inmediata una actualización total a la Ley N° 30096, Ley de Delitos Informáticos, la naturaleza de esta ley y el aumento del uso de las tecnologías de la información y la comunicación ameritan una modificatoria y regulación exhaustiva a esta Ley.

Respectivamente recomendamos que se modifique la regulación del articulo 9 que integra el delito de suplantación de identidad, puesto que este delito no fue integrado en la última modificatoria.

También exhortamos a que se regulen los medios informáticos desarrollados en esta investigación, en base a nuestros hallazgos teóricos y lo referido por nuestros participantes, los medios informáticos deben ser regulados específicamente en la Ley de Delitos Informáticos o tener una Ley autónoma que regule su uso.

En la actualidad el sistema financiero evoluciona constantemente, puesto que, al obtener mucha clientela deben brindar mayores facilidades para el uso del sistema bancario lo que integra la constante ejecución de las tecnologías de la información y comunicación por lo cual se encontraran nuevos problemas, específicamente, vacíos legales, que no regulan ciertas conductas delictivas.

REFERENCIAS

Acurio Del Pino, S. (s.f.). Delitos informáticos: generalidades. Recuperado de http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Informe%c3%a1ticos.%20generalidades.pdf

Arocena, G. (2012). La regulación de los delitos informáticos en el Código Penal Argentino. Introducción a la Ley nacional Nº 26388. Boletín Mexicano de Derecho Comparado,135, 945-988. [Fecha de consulta 08 de mayo de 2020]. https://www.redalyc.org/pdf/427/42724584002.pdf

Balcazar, W. Y. (2017). *Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito*. [Tesis de bachiller, Universidad Privada Antenor Orrego]. Repositorio institucional UPAO. http://repositorio.upao.edu.pe/handle/upaorep/3314

Carvajal, C., Bayona, D.& Ortiz, Z. (2013). Extensión de taxonomía y tratamiento de valores faltantes sobre un repositorio de incidentes de seguridad informática. Revista Ingeniería, 18(1), 24-49. [Fecha de consulta 19 de mayo de 2020]. https://www.redalyc.org/articulo.oa?id=498850176003

Celi, E. K. & Diaz, R. J. (2017). *Políticas de seguridad de la información en función del comportamiento de los usuarios de tecnologías de la información en el sector microfinanciero de Lambayeque.* [Tesis de doctorado, Universidad Nacional Pedro Ruiz Gallo]. Repositorio institucional UNPRG. http://repositoro.unprg.edu.pe/handle/UNPRG/1365

Congreso de la Republica del Perú (2018, 5 de julio). Ley Nº 30806, Ley que modifica la Ley del Consejo Nacional de Ciencia y Tecnología e Innovación Tecnológica. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-diversos-articulos-de-la-ley-28303-ley-mar-ley-n-30806-1666491-1/

Congreso de la Republica del Perú (2013, 27 de setiembre). Ley Nº 30096, Ley de Delitos Informáticos. https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Congreso de la Republica del Perú (2014, 10 de marzo). Ley Nº 30171, Ley que modifica la Ley de Delitos Informáticos.

https://cdn.www.gob.pe/uploads/document/file/200326/197055_Ley30171.pdf20180926-32492-1l0lzim.pdf

Consejo de Europa- (2001, 23 de noviembre). Convenio de Budapest. Convenio sobre la ciberdelincuencia. Serie de tratados europeos Nº 185.

Faraldo, P. (2010). Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. Revista de Derecho Penal y Criminología, 3(10), 73-134. [Fecha de consulta 23 de abril de 2020]. Disponible en http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned%3ArevistaDerechoPenalyCriminologia-2010-3-5030&dsID=Documento.pdf&hc_location=ufi

Hernandez, R., Fernandez, C. & Baptista, L. (2014). Metodología de la investigación. (6ta ed.). McGraww-Hill; México.

Hernández, D. A. (2019). *La suplantación de identidad cibernética en el Ecuador.* [tesis de maestría, Universidad Externado de Colombia]. Repositorio institucional UEC.https://bdigital.uexternado.edu.co/bitstream/001/1822/1/GAAA-spa-2019-La_suplantacion_de_identidad_cibernetica_en_el_Ecuador

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution, 4(1), 1-12. [Fecha de consulta 01 de mayo de 2020]. https://academicjournals.org/article/article1379859409_Hedayati.pdf

Hugo, S. (2014). Tipificación de los delitos informáticos patrimoniales en la nueva ley de delitos informáticos N° 30096. Derecho y Ciencia Política, 1(1), 69-80 [Fecha de consulta 01 de mayo de 2020]. https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/view/11870

Kerlinger, F. & Howard, L. (2008). *Investigación del Comportamiento.* 4ta ed. (L. Pineda & I. Mora, ed. Trad.). McGraw-Hill; México.

Leenes, R.(2006). Identity theft, identity fraud and/or identity – related crime. DUD, 9, 553-556. https://www.researchgate.net/publication/257703479_Identity_theft_identity_fraud_andor_identityrelated_crime?enrichId=rgreq7ec6536411aeb0a35fab4dfff8014173XXX&enrichSource=Y292ZXJQYWdlOzI1NzcwMzQ3OTtBUzo5ODY4NjgwMTU0NzI3MEAxNDAwNTQwMTc1Njkz&el=1_x_2&_esc=publicationCoverPdf

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico penal de los delitos informáticos. Revista Ius et Praxis, 24(1), 159-206. [Fecha de consulta 22 de mayo de 2020]. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S071800122018000100159

Merchán, A. P. (2012). *Reformas al régimen penal ecuatoriano en cuanto al delito de suplantación de identidad*. [Tesis de grado no publicada, Universidad Nacional de Loja]. https://nanopdf.com/download/merchan-sarmiento-anibal-patricio_pdf

Montoya, F. A. (2018). *Regulación expresa del delito informático de clonación de tarjetas – Sede DIVINDAT, 2017*. [Tesis de grado, Universidad Cesar Vallejo]. Repositorio institucional URL. http://repositorio.ucv.edu.pe/handle/20.500.12692/39776?locale-attribute=en

Oficina de las Naciones Unidas contra la Droga y el Delito (2013). Manual sobre los delitos relacionados con la identidad. Naciones Unidad; Nueva York.

Paredes, J. M. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010*. [tesis de maestría, Universidad Nacional Mayor de San Marcos]. Repositorio institucional UNMSM.http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/10314/Paredes_pj.pdf?sequence=1&isAllowed=y

Pecoy, M. (2011). Delito en el comercio electrónico. Revista Prisma Jurídico, 10(1), 209-224. [Fecha de consulta 08 de mayo de 2020]. ISSN: 1677-4760. Disponible en: http://www.redalyc.org/articulo.oa?id=93420939012

Peñaloza, M.C., Morillo, M. C.(2010). El sector servicios y los delitos informáticos. Revista Vision Gerencial, 2, 358-370. [Fecha de consulta 08 de mayo de 2020]. https://www.redalyc.org/articulo.oa?id=465545889014

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Revista Latinoamericana de Seguridad, 20, 80-93. [Fecha de consulta 08 de mayo de 2020]. https://www.redalyc.org/articulo.oa?id=552656641007

Puelles, R. (2014). Luces y sombra en la lucha contra la delincuencia informática en el Perú. Revista Hiperderecho. [Fecha de consulta 08 de mayo de 2020].

https://hiperderecho.org/wpcontent/uploads/2014/07/01_delitos_informaticos_elias.pdf

Rico, M. (2013). Los desafíos del Derecho Penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. Revista del Instituto de Ciencias Jurídicas de Puebla, 11(31), 207-222. [Fecha de consulta 01 de mayo de 2020]. ISSN: 1870-2147. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S18702147201300010 0011

Rivera, R. (2008). Los medios informáticos: Tratamiento procesal. Dikaion, 22(17), 297-324. [Fecha de consulta 19 de mayo de 2020]. https://www.redalyc.org/comocitar.oa?id=72011607012

Rivero, L. K. (2017). *Delitos informáticos y la evidencia digital en el proceso penal peruano en el 2017*. [Tesis de grado, Universidad Cesar Vallejo]. Repositorio institucional URL. http://repositorio.ucv.edu.pe/handle/20.500.12692/23302

Romero, R. (2019). Las conductas vinculadas a la suplantación de identidad por medios telemáticos: Una propuesta de acción legislativa. UNAM. 849-863. [Fecha de consulta 01 de mayo de 2020]. http://ru.juridicas.unam.mx/xmlui/handle/123456789/31540

Tellez, J. (2008). *Derecho informático* (4ta ed.). McGraw Hill; México.

Vidal, E. (2018). *La falta de regulación frente a la suplantación y usurpación de identidad en internet.* [Tesis de grado, Universidad de Islas Baleares]. Repositorio institucional URL https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal_Torres_Elionor.pdf?sequence=1&isAllowed=y

Villavicencio Terreros, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. Recuperado a partir de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Yeboah, E. & Mateko, P. (2014). Phishing, Smishing and Vishing: an assesment of threats against Mobile devices. *Journal of Emerging Trends in Computing and Information Sciences,* 5(4), 297-307. Recuperado de http://www.cisjournal.org

Zea, A. M. (2016). *Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala*. [Tesis de grado, Universidad Rafael Landívar]. Repositorio institucional URL. http://recursosbiblio.url.edu.gt/tesiseortiz/2016/07/03/Zea-Arely.pdf

Zegarra, D. (2018). *Introducción al derecho de las telecomunicaciones.* (1era. ed.) Fondo editorial PUCP. Lima.

ANEXOS

MATRIZ DE CONSISTENCIA

TÍTULO: EL DELITO DE SUPLANTACIÓN DE IDENTIDAD Y MEDIOS INFORMÁTICOS EN EL SECTOR FINANCIERO DE LIMA, 2019.

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, PROCESAL PENAL, SISTEMA DE PENAS, CAUSAS Y FORMAS DEL FENÓMENO CRIMINAL.

PROBLEMAS	OBJETIVOS	SUPUESTO	CATEGORIZACIÓN	DISEÑO DEL ESTUDIO
Problema general: ¿De qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?	**Objetivo general:** Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.	**Supuesto general:** Los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.	1.Delito de suplantación de identidad **Subcategorización:** 1.1: Regulación expresa 1.2: Suplantación 1.3: Identidad 2. Medios informáticos **Subcategorización:** 2.1: Vishing 2.2: Spyware 2.3: Skimming	Tipo: Básica Nivel: Cualitativa Diseño: Teoría fundamentada Muestra: 2 Abogados especialistas penales y 2 especialistas informáticos. Técnicas de recolección: Guía de entrevista.
Problemas específicos: ¿De qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?	**Objetivos específicos:** Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.	**Supuestos específicos:** El vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.		

¿De qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?	Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.	El spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.		
¿De qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019?	Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.	El skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.		

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Rosas Job, Prieto Chávez
1.2. Cargo e institución donde labora: Coord. De Investigación de la EP Derecho de la Universidad César Vallejo
1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista
1.4. Autora de Instrumento: Aldecoa Jimenez, Milagros del Rosario

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.											X		
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.											X		
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.											X		
4. ORGANIZACIÓN	Existe una organización lógica.											X		
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales											X		
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.											X		
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.											X		
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos											X		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.											X		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											X		

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación — ------

IV. PROMEDIO DE VALORACIÓN :

90%

Lima, 27 de junio del 2020

Dr. Rosas Job Prieto Chávez
Abogado CAS Nº 2486
Administrador

FIRMA DEL EXPERTO INFORMANTE
DNI No 41651398. Telf.:922011064

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: CAÑARI FLORES FERNANDO TOMAS
1.2. Cargo e institución donde labora: UNIVERSIDAD CESAR VALLEJO - JPC
1.3. Nombre del instrumento motivo de evaluación: GUÍA DE ENTREVISTA
1.4. Autor(A) de Instrumento: ALDECOA JIMENEZ MILAGROS DEL ROSARIO

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuanta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorias.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación — --------

IV. PROMEDIO DE VALORACIÓN : 95%

Lima, 30 de Junio del 2020

Telf.: 913386932

FICHA DE ENTREVISTA DIRIGIDO A LOS PARTICIPANTES DEL PROYECTO DE INVESTIGACIÓN

Título: El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.

Entrevistado (a):

Cargo / profesión / grado académico:

Institución o Empresa:

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

1.- ¿Sabe Ud. que es el delito de suplantación de identidad y que son los medios informáticos?

2.- Considera ud., basándose en su criterio, que se deba modificar la regulación expresa del delito de suplantación de identidad.

3.- Considera ud., basándose en su criterio, que se deba regular el uso de medio informáticos para evitar la comisión del delito de suplantación de identidad.

Objetivo específico 1:

Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?

5.- ¿Sabe ud. de qué manera favorece el vishing la comisión del delito de suplantación de identidad?

6.- ¿Consideraría ud. regular el vishing dentro de nuestra legislación?

Objetivo específico 2:

Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

7.- ¿A tenido ud. experiencia alguna referente a la figura del spyware en el delito de suplantación de identidad?

8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?

9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?

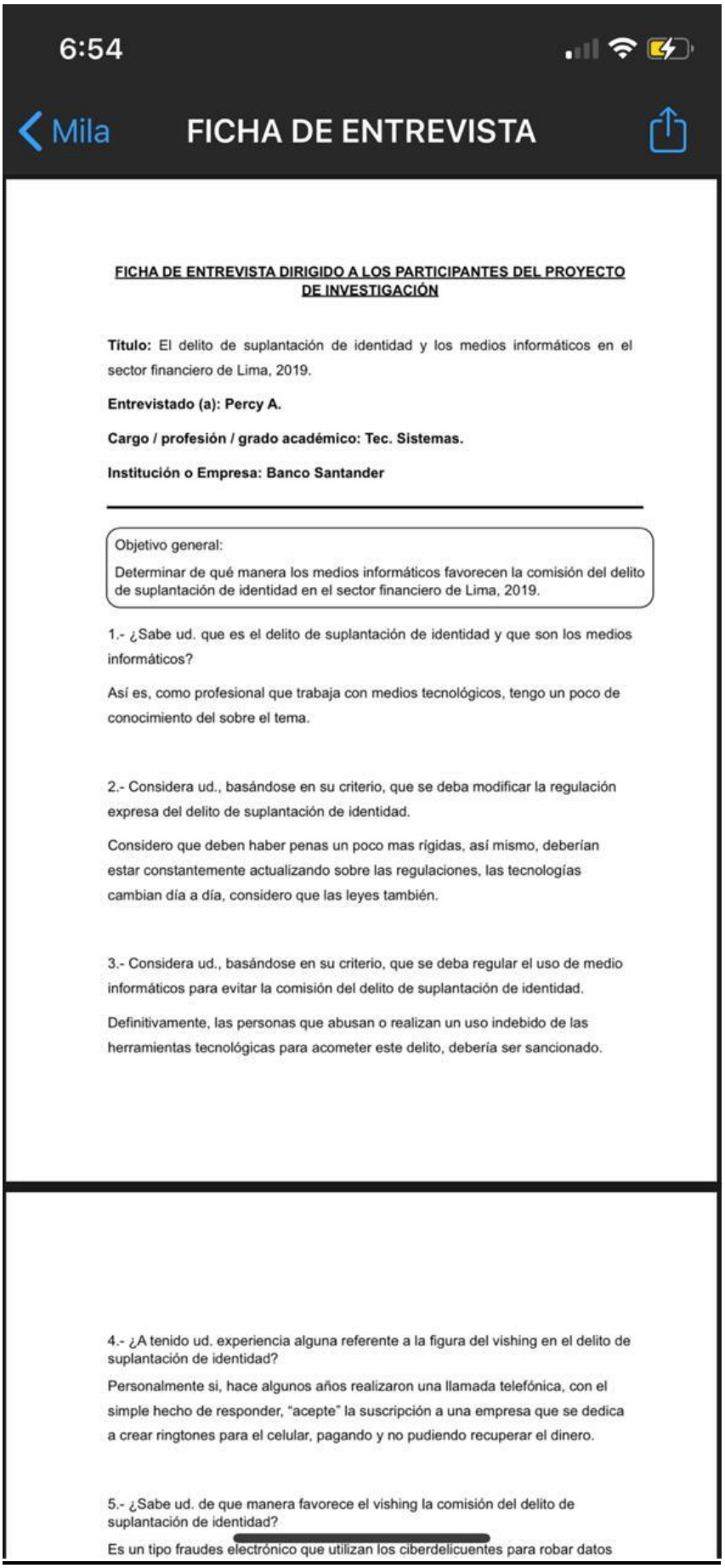
Objetivo específico 3:

Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?

11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?

12.- ¿Consideraría ud. regular el skimming dentro de nuestra legislación?



FICHA DE ENTREVISTA DIRIGIDO A LOS PARTICIPANTES DEL PROYECTO DE INVESTIGACIÓN

Título: El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.

Entrevistado (a): Percy A.

Cargo / profesión / grado académico: Tec. Sistemas.

Institución o Empresa: Banco Santander

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

1.- ¿Sabe ud. que es el delito de suplantación de identidad y que son los medios informáticos?

Así es, como profesional que trabaja con medios tecnológicos, tengo un poco de conocimiento del sobre el tema.

2.- Considera ud., basándose en su criterio, que se deba modificar la regulación expresa del delito de suplantación de identidad.

Considero que deben haber penas un poco mas rígidas, así mismo, deberían estar constantemente actualizando sobre las regulaciones, las tecnologías cambian día a día, considero que las leyes también.

3.- Considera ud., basándose en su criterio, que se deba regular el uso de medio informáticos para evitar la comisión del delito de suplantación de identidad.

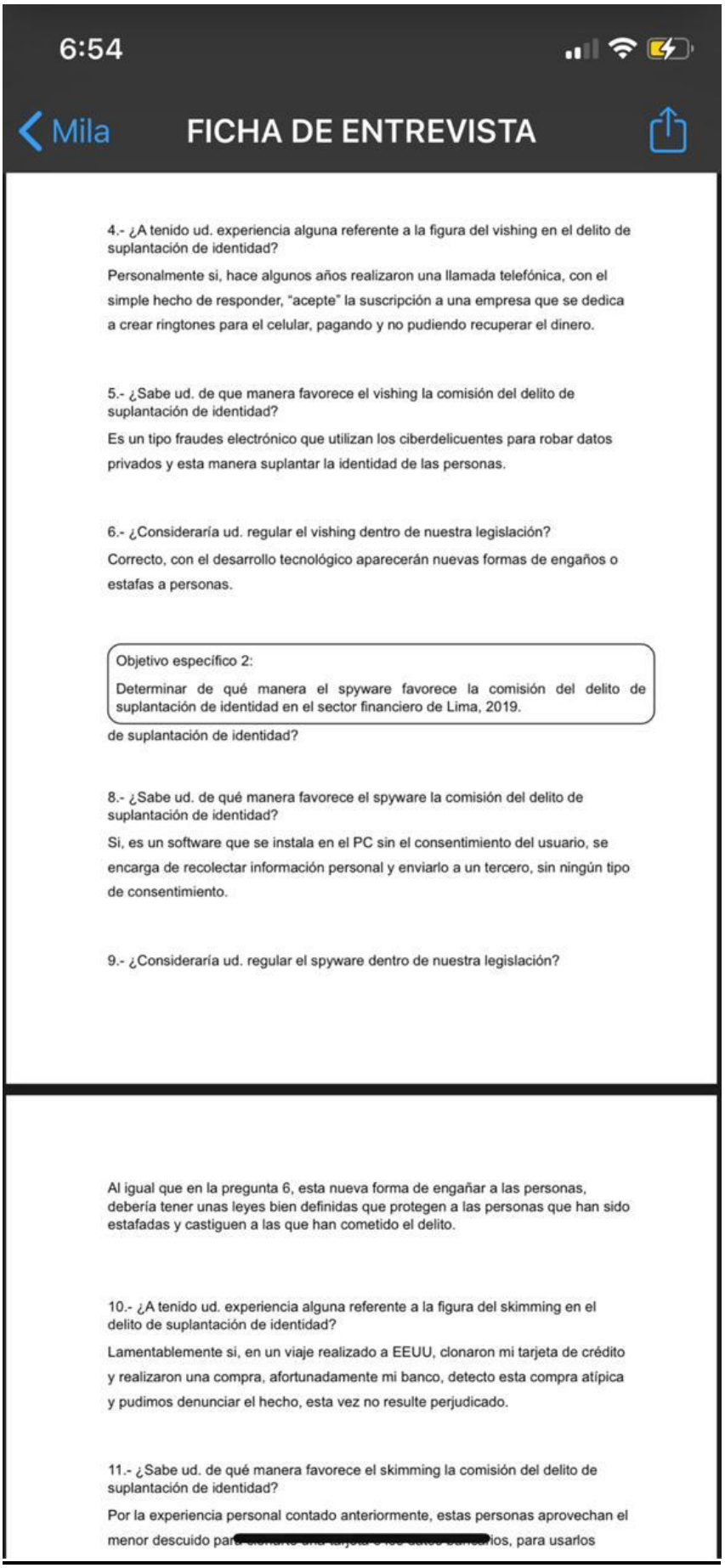
Definitivamente, las personas que abusan o realizan un uso indebido de las herramientas tecnológicas para acometer este delito, debería ser sancionado.

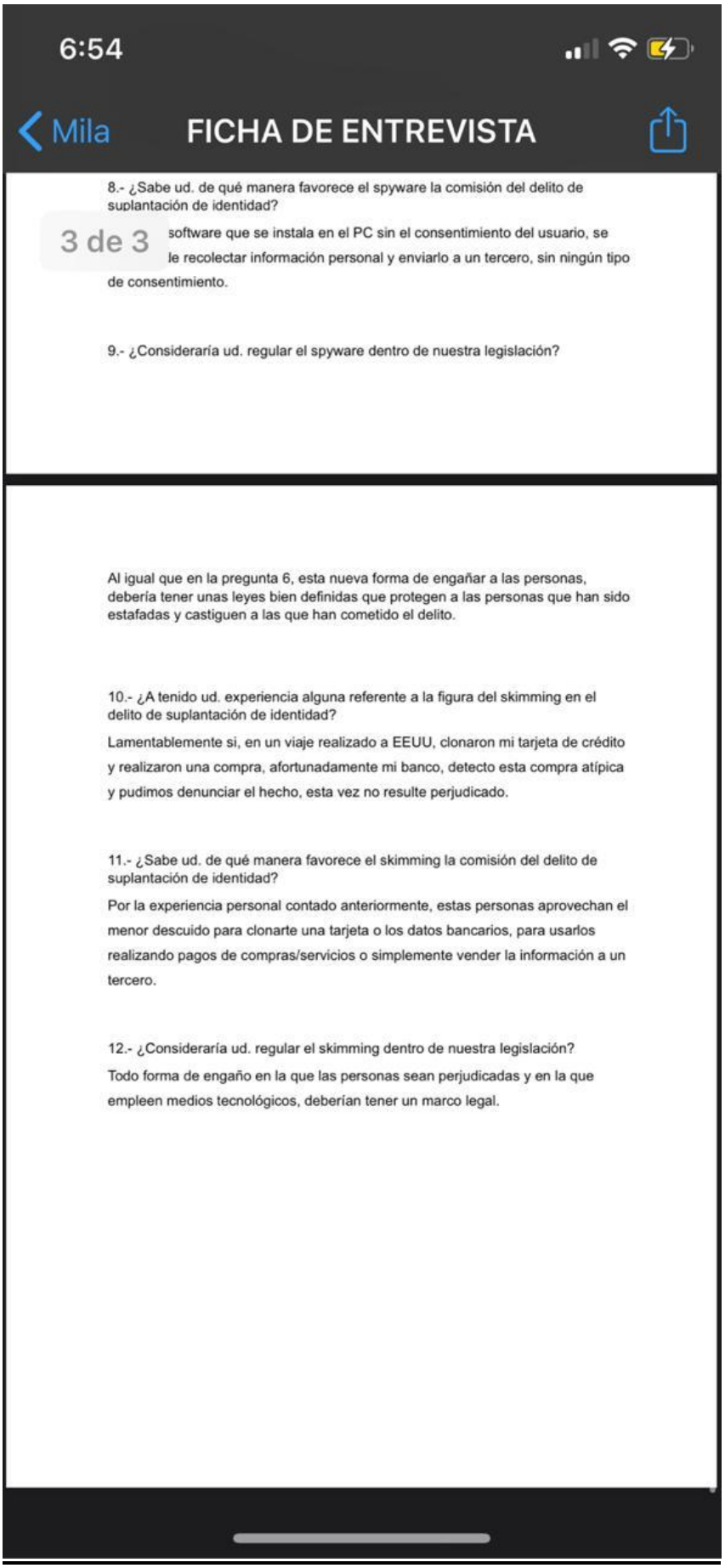
4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?

Personalmente si, hace algunos años realizaron una llamada telefónica, con el simple hecho de responder, "acepte" la suscripción a una empresa que se dedica a crear ringtones para el celular, pagando y no pudiendo recuperar el dinero.

5.- ¿Sabe ud. de que manera favorece el vishing la comisión del delito de suplantación de identidad?

Es un tipo fraudes electrónico que utilizan los ciberdelicuentes para robar datos


6:54
Mila
FICHA DE ENTREVISTA
4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?
Personalmente si, hace algunos años realizaron una llamada telefónica, con el simple hecho de responder, "acepte" la suscripción a una empresa que se dedica a crear ringtones para el celular, pagando y no pudiendo recuperar el dinero.
5.- ¿Sabe ud. de que manera favorece el vishing la comisión del delito de suplantación de identidad?
Es un tipo fraudes electrónico que utilizan los ciberdelicuentes para robar datos privados y esta manera suplantar la identidad de las personas.
6.- ¿Consideraría ud. regular el vishing dentro de nuestra legislación?
Correcto, con el desarrollo tecnológico aparecerán nuevas formas de engaños o estafas a personas.
Objetivo específico 2:
Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.
de suplantación de identidad?
8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?
Si, es un software que se instala en el PC sin el consentimiento del usuario, se encarga de recolectar información personal y enviarlo a un tercero, sin ningún tipo de consentimiento.
9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?
Al igual que en la pregunta 6, esta nueva forma de engañar a las personas, debería tener unas leyes bien definidas que protegen a las personas que han sido estafadas y castiguen a las que han cometido el delito.
10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?
Lamentablemente si, en un viaje realizado a EEUU, clonaron mi tarjeta de crédito y realizaron una compra, afortunadamente mi banco, detecto esta compra atípica y pudimos denunciar el hecho, esta vez no resulte perjudicado.
11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?
Por la experiencia personal contado anteriormente, estas personas aprovechan el menor descuido par
ios, para usarlos


6:54
Mila
FICHA DE ENTREVISTA
8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?
3 de 3
software que se instala en el PC sin el consentimiento del usuario, se le recolectar información personal y enviarlo a un tercero, sin ningún tipo de consentimiento.
9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?
Al igual que en la pregunta 6, esta nueva forma de engañar a las personas, debería tener unas leyes bien definidas que protegen a las personas que han sido estafadas y castiguen a las que han cometido el delito.
10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?
Lamentablemente si, en un viaje realizado a EEUU, clonaron mi tarjeta de crédito y realizaron una compra, afortunadamente mi banco, detecto esta compra atípica y pudimos denunciar el hecho, esta vez no resulte perjudicado.
11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?
Por la experiencia personal contado anteriormente, estas personas aprovechan el menor descuido para clonarte una tarjeta o los datos bancarios, para usarlos realizando pagos de compras/servicios o simplemente vender la información a un tercero.
12.- ¿Consideraría ud. regular el skimming dentro de nuestra legislación?
Todo forma de engaño en la que las personas sean perjudicadas y en la que empleen medios tecnológicos, deberían tener un marco legal.

FICHA DE ENTREVISTA DIRIGIDO A LOS PARTICIPANTES DEL DESARROLLO DE INVESTIGACIÓN

Título: El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.

Entrevistado (a): Carlos Eduardo Escobar Cornejo

Cargo / profesión / grado académico: Ingeniero de Sistemas

Institución o Empresa: Kruma

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

1.- ¿Sabe ud. que es el delito de suplantación de identidad y que son los medios informáticos?

Si se. Sobrentiendo que se trata de un delito en el que una persona se puede hacer pasar por otra ocasionándole un daño. Sobre los medios informáticos o tecnologías de la información se trata de medios por el cual una persona tiene conexión con el mundo informático y con redes que conectan el mundo.

2.- Considera ud., basándose en su criterio, que se deba modificar la regulación expresa del delito de suplantación de identidad.

No conozco el detalle de lo que dice la ley de suplantación de identidad

3.- Considera ud., basándose en su criterio, que se deba regular el uso de medio informáticos para evitar la comisión del delito de suplantación de identidad.

Considero que no se debe regular el uso de medios informáticos, sino, educar a las personas para que puedan saber y evitar caer en este tipo de delitos

Objetivo específico 1:

Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?

Si, una vez me llamaron diciéndome que un familiar estaba en la comisaria, sin decirme el nombre del familiar y queriendo obtener esta información. Felizmente, ya había conocido de esta modalidad de delito y corte la llamada

5.- ¿Sabe ud. de qué manera favorece el vishing la comisión del delito de suplantación de identidad?

Imagino que a través del vishing logran conseguir información valiosa que luego puede permitir que se cometa el delito con mayor facilidad

6.- ¿Consideraría ud. regular el vishing dentro de nuestra legislación?

Si, debería regularse y castigarse, entiendo que al respecto la regulación es general, no soy muy conocedor de leyes, porque mi campo son los sistemas y la informática y entiendo que el vishing es un medio informático que puede ser utilizado para realizar delitos, por lo cual se debería castigar.

Objetivo específico 2:

Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

7.- ¿A tenido ud. experiencia alguna referente a la figura del spyware en el delito de suplantación de identidad?

Si, conozco algunos programas que sirven para eso

8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?

De igual forma que el vishing, obtiene información importante de la persona, sin que esta lo sepa

9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?

De todas maneras, me parece que existen medios informáticos muy comunes, los cuales necesitarían de una regulación especial para sancionar esos actos.

Objetivo específico 3:

Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?

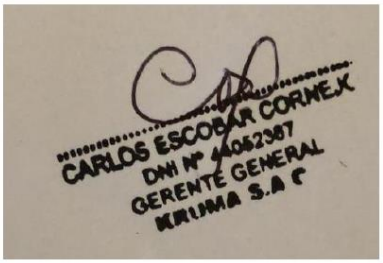
No he tenido ninguna experiencia

11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?

Igual que los delitos anteriores, favorece a través de la obtención de información importante y delicada de las personas, sin la autorización previa

12.- ¿Consideraría ud. regular el skimming dentro de nuestra legislación?

De todas maneras, al igual que los demás medios informáticos considero que son mecanismos muy peligrosos.



FICHA DE ENTREVISTA DIRIGIDO A LOS PARTICIPANTES DEL PROYECTO DE INVESTIGACIÓN

Título: El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.

Entrevistado (a): Felix Eduardo Dorregaray Garcia

Cargo / profesión / grado académico: Abogado y Conciliador

Institución o Empresa: Superintendencia Nacional de Salud

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

1.- ¿Sabe ud. que es el delito de suplantación de identidad y que son los medios informáticos?

Se trata de un delito informático según lo regulado en su ley autónoma en el articulo 9, en donde una persona suplantando la identidad de otra, ya sea persona natural o jurídica causa un perjuicio económico o moral será sancionado con pena privativa de la libertad. Sobre los medios informáticos no conozco mucho, solo aquellos medios que usamos habitualmente como celular, computadora o aplicaciones bancarias, imagino que a ello se refieren.

2.- Considera ud., basándose en su criterio, que se deba modificar la regulación expresa del delito de suplantación de identidad.

Si, porque me parece que tiene una pena muy endeble para el perjuicio que se puede ocasionar suplantando la identidad de alguien, también el hecho de que no lo hace cualquier persona porque esa persona lo hace usando sus habilidades en computación, o sea siempre existirá una voluntad de hacer daño, siendo un delito doloso, debería modificarse la pena e integrar agravantes en cuanto a los medios informáticos que se usen.

3.- Considera ud., basándose en su criterio, que se deba regular el uso de medio informáticos para evitar la comisión del delito de suplantación de identidad.

Supongo que se refiere a que se deban regular los medios informáticos para que no los usen de forma mal intencionada, si se refiere a eso, pues si, me parece que existen medios mas peligrosos que simplemente crear un perfil falso en Facebook.

Objetivo específico 1:

Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?

No tengo mucho conocimiento sobre los medios informáticos en especial, pero la entrevistadora me indico de que trataba cada uno de ellos y cuando me lo explicó dije: pero si a mi me ha pasado esto y a mi entorno también. Una vez, me llamaron de una entidad bancaria diciéndome que habían identificado un movimiento malicioso en mi cuenta bancaria, me pidieron mis datos personales como el número de mi tarjeta y el número detrás de la tarjeta, al inicio no sospeche, pero al hacer tantas preguntas y siendo muy insistente el hombre que me llamó colgué el teléfono, luego llame a mi entidad bancaria para saber si todo estaba bien y me indicaron que no realizan ese tipo de llamadas, solo bloquean la tarjeta.

5.- ¿Sabe ud. de qué manera favorece el vishing la comisión del delito de suplantación de identidad?

Bueno como comentaba en la pregunta anterior, pues ya denotamos que favorece bastante, me parece que es un medio muy peligroso, sobre todo porque es difícil identificar si es cierto o se trata de un ciberdelincuente, se suplanta la identidad de una entidad bancaria sin ningún tipo de tapujo, también me han enviado mensajes raros solicitando mis datos, es increíble.

6.- ¿Consideraría ud. regular el vishing dentro de nuestra legislación?

Así como lo pregunta, supongo que se refiere a regular especialmente este medio informático como una agravante del delito de suplantación de identidad, pues

considero que si, como un hombre de leyes, la norma regula la conducta del agente que es ilegal, esto es ilegal, por lo tanto, debe ser regulado.

Objetivo específico 2:

Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

7.- ¿A tenido ud. experiencia alguna referente a la figura del spyware en el delito de suplantación de identidad?

No la he tenido, no conozco sobre este medio, pero me informó la entrevistadora que es un virus malicioso que roba datos sensibles de la computadora que uno usa.

8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?

Sabiendo lo que es, no creo saber como lo favorece.

9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?

De todas maneras, debe ser un agravante, para crear estos virus se necesita de mucho conocimiento y sobre todo que el ciberdelincuente puede obtener información hasta de todo un gobierno y causar un gran daño.

Objetivo específico 3:

Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?

Por supuesto, una vez asistí a un centro comercial, tuve que realizar el pago de un producto con una de mis tarjetas, me pareció raro el POS que usó el cajero porque nunca antes lo había visto, posterior a ello, la entidad bancaria de donde provenía mi tarjeta me envió un correo electrónico cifrado en el que mencionaban que habían intentado realizar compras en otros centros comerciales de incluso provincia con mi tarjeta, me solicitaron identificarme, me preguntaron hasta donde

había nacido, también me mostraron cámaras de seguridad de ciertas tiendas y pudieron visualizar que no había sido yo, me dieron una nueva tarjeta.

11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?

Bueno con lo que me paso, tuve que dar hasta el máximo detalle sobre mi identidad para que el banco supiera que se trataba del titular de la tarjeta y no de los ciberdelincuentes; sin embargo, he tenido experiencia de amigos, que a pesar de haber respaldado su identidad sufrieron un gran perjuicio económico y el banco no les supo reconocer, hoy por hoy se encuentran inmersos en un proceso judicial porque la Policía tampoco ha podido atrapar al o los delincuentes.

12.- ¿Consideraría ud. regular el skimming dentro de nuestra legislación?

Por supuesto que sí, he leído sobre los delitos informáticos y los delitos tipificados hablar de los medios informáticos en su generalidad, quien desarrolla este trabajo ha tocado medios informáticos muy delicados y me parece que al menos de 10 personas a 8 le ha pasado que han suplantado su persona usando alguno de estos medios, deberían tener mas sanción o tomarlos como agravantes.

FICHA DE ENTREVISTA DIRIGIDO A LOS PARTICIPANTES DEL PROYECTO DE INVESTIGACIÓN

Título: El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.

Entrevistado (a): CAROLINE MELISSA TELLO MENESES

Cargo / profesión / grado académico: SECRETARIA DE SALA / ABOGADO / EGRESADA DE MAESTRIA EN DERECHO PROCESAL

Institución o Empresa: PODER JUDICIAL

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

1.- ¿Sabe ud. que es el delito de suplantación de identidad y que son los medios informáticos?

El delito de suplantación de identidad, o también llamado de usurpación, consiste en el accionar que despliega una persona teniendo como fin el apropiarse de la identidad de otra persona para hacerse pasar por esta y obtener beneficios, es decir, consiste en simular ser otra persona.

Los delitos informáticos son actividades ilícitas que se realizan en el entorno digital utilizando como medio el uso de internet, burlando el sistema de seguridad y que tienen como fin provocar daños o impedir el uso de sistemas informáticos.

2.- Considera ud., basándose en su criterio, que se deba modificar la regulación expresa del delito de suplantación de identidad.

Considero que sí se debe modificar la forma como está regulado este delito en el código penal peruano.

3.- Considera ud., basándose en su criterio, que se deba regular el uso de medio informáticos para evitar la comisión del delito de suplantación de identidad.

Sí debe ser regulado el uso de los medios informáticos.

Objetivo específico 1:

Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

4.- ¿A tenido ud. experiencia alguna referente a la figura del vishing en el delito de suplantación de identidad?

No he tenido ninguna experiencia.

5.- ¿Sabe ud. de qué manera favorece el vishing la comisión del delito de suplantación de identidad?

El vishing trata de simular la voz de los sistemas de audios de las entidades financieras, para hacer creer al usuario de éstos, que se ingresa a una página o que está siendo guiado por la entidad financiera y así realizar actividades financieras.

6.- ¿Consideraría ud. regular el vishing dentro de nuestra legislación?

El vishing como tal, no se encuentra regulado en nuestro sistema legal, sin embargo sí considero que debe ser regulado, con la finalidad de no dejar vacíos legales que den paso a la comisión de estos delitos.

Objetivo específico 2:

Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

7.- ¿A tenido ud. experiencia alguna referente a la figura del spyware en el delito de suplantación de identidad?

He recibido varios correos electrónicos en el que solicitan que registre datos para acceder a páginas a páginas web de entidades financieras, sin embargo, conocedora de este tipo de delitos no he aceptado acceder a ninguna de ellas.

8.- ¿Sabe ud. de qué manera favorece el spyware la comisión del delito de suplantación de identidad?

El spyware infecta un dispositivo electrónico accediendo a información personal, información que luego es enviada a los ciberdelincuentes, facilitando así la comisión de actos ilícitos.

9.- ¿Consideraría ud. regular el spyware dentro de nuestra legislación?

Sí debería estar regulado.

Objetivo específico 3:

Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

10.- ¿A tenido ud. experiencia alguna referente a la figura del skimming en el delito de suplantación de identidad?

No.

11.- ¿Sabe ud. de qué manera favorece el skimming la comisión del delito de suplantación de identidad?

Por medio del skimming se copia la banda de seguridad de las tarjetas de crédito o débito, para su posterior uso fraudulento, por lo que sí favorece la comisión de este delito.

12.- ¿Consideraría ud. regular el skimming dentro de nuestra legislación?

Sí debería estar regulado como tal en nuestro ordenamiento jurídico. Respecto de los delitos informáticos la legislación debería estar en constante cambio y regulación, porque este es un delito que cada día va cambiando su forma operativa, por lo que derecho debe entrar a regular todas estas figuras, y con esto no dejar vacíos legales, que permitan la comisión impune de estos delitos.

GUIA DE ANÁLISIS DOCUMENTAL

Objetivo general:

Determinar de qué manera los medios informáticos favorecen la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

"ANÁLISIS DE INFORME"

Delitos Informáticos

DESCRIPCIÓN DE LA FUENTE	IDENTIFICACIÓN DEL OBJETO DE ANÁLISIS
Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. Recuperado a partir de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630	Articulo 9°. Suplantación de identidad El que mediante tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años (Villavicencio, p.297) Bajo esta premisa podemos observar que se trata de un delito de resultado en el que sugiere que se ocasione un prejuicio para su comisión.

Objetivo especifico1:

Determinar de qué manera el vishing favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

DESCRIPCIÓN DE LA FUENTE	IDENTIFICACIÓN DEL OBJETO DE ANÁLISIS
Yeboah, E. & Mateko, P. (2014). Phishing, Smishing and Vishing: an assesment of threats against Mobile devices. *Journal of Emerging Trends in Computing and Information Sciences,* 5(4), 297-307. Recuperado de http://www.cisjournal.org	Definen al vishing como un mecanismo dentro de la tecnología de la información y comunicación que se comete usando una voices notes o línea telefónica basándose en habilidades de la ingeniería social para recaudar información delicada, como lo es la información financiera de la persona, para engañarla y así hacer uso de su identidad (2014, p.300) El vishing (medio informático que utilizamos en la presente investigación) trata de recaudar a través de correos electrónicos u otros medios informáticos con el fin de recaudar la información personal y financiera de la víctima a fin de suplantar su identidad ante la entidad bancaria y generarle un perjuicio económico ya sea desfalcando sus cuentas.

Objetivo específico 2:

Determinar de qué manera el spyware favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

DESCRIPCIÓN DE LA FUENTE	IDENTIFICACIÓN DEL OBJETO DE ANÁLISIS
Stafford, T. & Urbaczewski, A. (2004). Spyware: The Ghost in the machine. *Comunications of the Association for Information Systems.* 14, 291-306. Recuperado de http://www.researchgate.net/publication/220892580	Spyware es el nombre dado a la clase de software que se instala subrepticiamente en la computadora y monitorea la actividad de un usuario e informa a un tercero al respecto de esa actividad o la base de datos contenida en el ordenador del usuario. The Federal Trade Commission, la cual probablemente es la autoridad más potente para controlar el uso de spyware, lo define como software que ayuda a reunir información a otra entidad sin el consentimiento del usuario. Podemos identificar el spyware es un virus malicioso que se instala, ya sea por medios de cookies o la apertura de páginas web no seguras, para recaudar información personal del usuario que domina el ordenador con el fin de extraer dicha información y brindarla a un tercero para generar un perjuicio.

Objetivo específico 3:

Determinar de qué manera el skimming favorece la comisión del delito de suplantación de identidad en el sector financiero de Lima, 2019.

DESCRIPCIÓN DE LA FUENTE	IDENTIFICACIÓN DEL OBJETO DE ANÁLISIS
Mauritius Bankers Association Limited (s.f) (2016). Card Fraud and skimming. Consultado el 6 de octubre de 2020 Recuperado de http://www.mba.mu/pdf/2016/Card-Fraud-and-Skimming-EnglishV.pdf	El skimming es un tipo de fraude informático en el que la información de la cuenta de la persona se adquiere o se registra ilegalmente mediante una técnica de lector de tarjetas o insertado de un lector de chips. Los dispositivos de desnatado o skimmers son lectores que colocados en la parte superior de un POS o ATM generan la réplica de una tarjeta de crédito, haciendo difícil la identificación de estas personas malintencionadas, debido a que colocan sofisticados desnatados dentro de la terminal en sí mismos. (2016, p.1) Podemos identificar que el skimming es una forma de fraude electrónico que mediante sofisticados mecanismos de lectura de tarjetas pueden hurtar la información de una tarjeta de crédito o débito haciendo una igual para posteriormente actuar en nombre del titular de dicha tarjeta y cometer un perjuicio económico.

UNIVERSIDAD CÉSAR VALLEJO

Lima, 20 de noviembre de 2020

DIRECTOR DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ
Vicente Tiburcio Orbezo

Atención:
Coronel Orlando Mendieta
Jefe de la División de Investigación de Delitos de Alta Tecnología

Presente. -

ASUNTO: Facilidades para la aplicación de instrumento de investigación

Tengo el honor de dirigirme a usted, para expresarle mi cordial saludo, a nombre de la Escuela de Derecho, sede Ate, de la Universidad Cesar Vallejo, seguidamente informarle que como parte del desarrollo de tesis de la estudiante, **Aldecoa Jimenez Milagros del Rosario** con DNI N° 71405994, teléfono: 925962623 y correo electrónico: maldecoaj@gmail.com, titulado ***"El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019"***, es necesario la autorización de su representada, a fin de que la indicada estudiante pueda aplicar su instrumento de investigación en su prestigiosa división.

Por lo cual solicito se le brinde todas las facilidades, para la aplicación de su instrumento de investigación.

Agradeciendo por anticipado su amable atención a lo solicitado, me despido de usted expresándole mis deseos de salud y bienes para usted y su familia en estas épocas difíciles.

Atentamente,

MILAGROS ALDECOA JIMENEZ
DNI N° 71405994

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL PNP
SECRETARÍA GENERAL
20 NOV. 2020
Recibí: 1135 Folios: Firma:

UNIVERSIDAD CÉSAR VALLEJO

Lima, 24 de noviembre de 2020

DIRECTOR DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ
Vicente Tiburcio Orbezo

Atención:
Coronel Orlando Mendieta
Jefe de la División de Investigación de Delitos de Alta Tecnología

Presente. -

ASUNTO: Facilidades para la aplicación de instrumento de investigación

Tengo el honor de dirigirme a usted, para expresarle mi cordial saludo, a nombre de la Escuela de Derecho, sede Ate, de la Universidad Cesar Vallejo, seguidamente informarle que como parte del desarrollo de tesis de la estudiante, **Aldecoa Jimenez Milagros del Rosario** con DNI N° 71405994, teléfono: 925962623 y correo electrónico: maldecoaj@gmail.com, titulado ***"El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019"***, es necesario la autorización de su representada, a fin de que la indicada estudiante pueda aplicar su instrumento de investigación en su prestigiosa división.

Por lo cual solicito se le brinde todas las facilidades, para la aplicación de su instrumento de investigación.

Agradeciendo por anticipado su amable atención a lo solicitado, me despido de usted expresándole mis deseos de salud y bienes para usted y su familia en estas épocas difíciles.

Atentamente,

Coordinador de Investigación EP de Derecho – UCV Sede Ate
Dr. Job Prieto Chávez

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL PNP
SECRETARÍA GENERAL
02 DIC. 2020
15:23

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, ALDECOA JIMENEZ MILAGROS DEL ROSARIO estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "EL DELITO DE SUPLANTACIÓN DE IDENTIDAD Y LOS MEDIOS INFORMÁTICOS EN EL SISTEMA FINANCIERO DE LIMA, 2019.", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
ALDECOA JIMENEZ MILAGROS DEL ROSARIO **DNI:** 71405994 **ORCID** 0000-0002-8067-857X	Firmado digitalmente por: MALDECOAJ el 24-12-2020 13:15:42

Código documento Trilce: INV - 0193922

INVESTIGA UCV