# FACULTAD DE DERECHO Y HUMANIDADES

## ESCUELA PROFESIONAL DE DERECHO

Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**
**Abogado**


**AUTORES:**

Burga Carrero, Kleyder Maycot (orcid.org/0000-0003-2550-243x)

Morales Padilla, Gerardo Alexis (orcid.org/ 0000-0001-8143-4078)

**ASESOR:**

Dr. Santisteban Llontop, Pedro Pablo (orcid: 0000-0003-0998-0538)


**LÍNEA DE INVESTIGACIÓN:**

Derecho Penal, Procesal Penal, Sistema de Penas, Causa y Formas del Fenómeno Criminal.

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Fortalecimiento de la democracia, liderazgo y ciudadanía

**LIMA - PERÚ**

**2023**

**Dedicatoria**

A nuestros padres, familiares, que fueron el ancla del barco de nuestro futuro.

A todos aquellos que confiaron en nosotros desde el principio.

**Agradecimiento**

Agradecemos muy profundamente a nuestro asesor de tesis por su dedicación y paciencia, ya que, sin sus palabras y correcciones precisadas no hubiéramos podido llegar a esta instancia tan anhelada.

## Índice de contenidos

Pág.

**Índice de tablas** **Pág.**

## Índice de gráficos y figuras Pág.

**RESUMEN**

La presente tesis tiene como objetivo general analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático, del mismo modo, determinar de qué manera se utiliza el smishing y phishing para la comisión del delito de fraude informático; nuestro tipo de investigación es básica, con nivel descriptivo y en el enfoque de investigación es cualitativa.

Para la obtención de los datos, se utilizó revistas indexadas, tesis y jurisprudencia de relevancia nacional como internacional especializada en materia penal y administrativa; además de otras fuentes de información que se relacionan con la presente tesis. Como resultado de la fuente documental concluimos los fraudes informáticos no solamente se expanden por los servicios financieros, sino por diferentes medios perjudicando a los ciudadanos de manera general, esto debido a que, los medios informáticos pueden conectarse por diferentes plataformas, como redes sociales, correos, aplicativos instalados en el celular, entre otros más. Es importante acotar que la pandemia por la COVID-19 no ha sido impedimento para la realización de los fraudes informáticos en sus diferentes modalidades más conocidas como el phishing y smishing.

**Palabras Clave:** Uso de los datos personales, nuevas modalidades, fraude informático, acceso a cuentas bancarias.

**ABSTRACT**

The general objective of this thesis is to analyze how personal data is used in the new forms of computer fraud, in the same way, to determine how smishing and phishing are used to commit the crime of computer fraud; our type of research is basic, with a descriptive level and the research approach is qualitative.

To obtain the data, indexed journals, theses and jurisprudence of national and international relevance specialized in criminal and administrative matters were obtained; in addition to other sources of information that are related to this thesis. As a result of the documentary source, we conclude that computer fraud is not only expanded by financial services, but by different means, harming citizens in general, this is because computer media can be connected through different platforms, such as social networks, emails, etc. , applications installed on the cell phone, among others. It is important to comment that the COVID-19 pandemic has not been an impediment to carrying out computer fraud in its different, best-known modalities such as phishing and smishing.

**Keywords:** Use of personal data, new modalities, computer fraud, access to bank accounts.

**I. INTRODUCCIÓN. - A fin de apersonarnos adecuadamente al tema,** debemos enfatizar la relevancia e influencia a **nivel internacional** de los delitos relacionados al fraude informático, pues al tratarse de un delito que se materializa mediante el internet puede ser empleado en diferentes países como Ecuador, Colombia, Chile y Venezuela, asimismo, países europeos como España y finalmente, países norteamericanos como Estados Unidos. Sin embargo, la coyuntura reciente de la pandemia por la COVID-19 en la que nos encontrábamos, no fue impedimento para la comisión de estos delitos cibernéticos, esto es, de manera específica a la realización del smishing y phishing como una modalidad de estafa cibernética vulnerando valiosos datos personales de muchos usuarios que resguardan su dinero en cuentas bancarias.

Por su parte, a **nivel nacional** es necesario hacer énfasis que tampoco se consiguió salvaguardar los derechos de los consumidores en relación a las modalidades delictivas del smishing y phishing, toda vez que, los ciberdelincuentes lograron vulnerar las medidas de seguridad de las entidades financieras haciendo uso indebido de los datos personales produciendo la sustracción de efectivo de las cuentas bancarias de los consumidores, es de hacer hincapié que durante la entrada del Estado de Emergencia el incremento del delito cibernético investigado.

Por otro lado, teniendo esa perspectiva, la Sala Especializada en Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual extrayendo el criterio nacional, resolvió en última instancia administrativa diferentes conflictos entre los consumidores y las entidades financieras relacionados a las nuevas modalidades de fraudes informáticos, smishing y phishing, pues los mismos han vulnerado los mecanismos de seguridad transgrediendo los datos sensibles de los usuarios.

Por lo narrado, en los párrafos previos y de acuerdo a los lineamientos constituidos para la presente tesis, expresamos como ***problema general***, la posterior interrogante: ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?; en ese sentido, exponemos como ***problema específico N°1***, ¿De qué manera se utiliza el smishing para la

comisión del delito de fraude informático?; y del misma forma, se planteó como ***problema específico N°2***, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

En tal sentido, se planteó como ***objetivo general*** lo siguiente: Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático; además, expresamos como ***objetivo específico N°1***, Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático; también, se abordó como ***objetivo específico N°2***, Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Subsiguientemente, es menester realizar la acreditación de la tesis; teniendo como ***justificación teórica*** en función a las categorías plasmadas en nuestra matriz de categorización apriorística, es que buscamos contribuir en base al análisis de la infracción normativa del uso de los datos personales en las nuevas modalidades de fraude informático, con teorías emergentes, las cuales coadyuvaron al correcto análisis del principio de inmediación con teorías nacientes. Ahora bien, como ***justificación práctica***, nuestra tesis determinó que el uso de los datos personales en las nuevas modalidades de fraude informático, como es el phishing y smishing; es transgredido en la realización de los hechos delictivos cometidos bajo las nuevas modalidades de fraude informático, teniendo como referencia el artículo 8º de la Ley N° 30096, Ley de Delitos Informáticos; la cual establece que “el que premeditado e indebidamente procura para sí o para un tercero una ganancia ilícito en perjuicio de tercero mediante la introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier intromisión o manejo en el funcionamiento de un sistema informático”. Finalmente, en alusión a la ***justificación metodológica***, utilizando dos instrumentos para el desarrollo de este trabajo; los cuales fueron: la guía de entrevista y la ficha de análisis documental, obteniendo la validación de experimentados profesionales que consolidaron nuestro trabajo.

En esa línea, como ***contribución*** lo que buscamos con esta investigación, es analizar el uso de los datos personales en las nuevas modalidades de fraude

informático, específicamente en las denominadas “smishing y phishing”; debido a que estas figuras deberían de contener un definición clara respecto del uso de los datos personales en las nuevas modalidades de fraude informático, debido a que en nuestra doctrina y jurisprudencia actual, no sé advierte definición precisa con referencia a estas nuevas figuras delictivas.

Asimismo, la ***relevancia*** del estudio radicó en que, es imprescindible determinar la causa del uso de los datos personales en las nuevas modalidades de fraude informático, especialmente cuando se realiza las investigaciones de los hechos, pues es donde el ministerio público declara inadmisible las denuncias relacionadas al smishing y phishing, por no encontrar responsables de las estafas cibernéticas. Para finalizar, se planteó como **supuesto general**, los datos personales fueron empleados para la comisión de delitos cibernético se ejecuta, a fin de obtener un lucro patrimonial tomando en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. Los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. En ese sentido, las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático., formulamos como ***supuesto específico N°1***, el smishing se utilizó como una nueva modalidad de fraude informático, en razón de que, se emplearon datos personales facilitados por las tecnologías de información y comunicación. Dado que, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Esta modalidad va orientada exclusivamente a obtener de la víctima información confidencial, mediante enlaces, para luego pasar a un segundo momento y utilizar estos datos, como ***supuesto específico N°2***, la manera más recurrente que se puede advertir, la identificación del phishing como modalidad para la comisión de este hecho delictivo, dado que, el phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos

manipulados y que tiende a buscar las necesidades de las víctimas. En la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias.

**II. MARCO TEÓRICO. -** En este apartado nos planteamos sustentar los **trabajos previos**, es decir los antecedentes de recopilación importancia, provenientes de tesis nacionales e internacionales; de la misma manera, artículos de revistas indexadas en el contexto nacional e internacional, ello con el motivo de responder nuestros objetivos propuestos en nuestra tesis. En cuanto a los **antecedentes internacionales**, un interesante aportes es de Rodríguez (2018) que expresa respecto a los **datos personales:** "el incremento de la clasificación de fraudes informáticos en redes sociales vulneran los datos personales en Ecuador, asimismo, se puede afirmar que los usuarios tienen un gran desconocimiento de los fraudes informáticos siendo los más alarmantes, el smishing y phishing" (p. 61), siendo que, en nuestra opinión las plataformas sociales es el acceso para compartir muchos datos sensibles que originan un gran problema si llegan a manos de ciberdelincuentes, motivo por el cual, nuestra tesis se direcciona en analizar las infracciones normativas que ocasiona el fraude informático.

Continuando con los aportes académicos, en palabras de Peñarete (2020) manifiesta sobre los **datos sensibles:** "Se debe considerar la información privada del usuario, siendo la manifestación de una parte de su interior a otro usuario, bajo una conexión de confianza y compromiso, la cual no debe ser distribuida con otras personas sin la real autorización del propio interesado (p. 53). Por lo expuesto, podemos corroborar que los datos sensibles es información delicada que no puede ser compartida a terceras personas, debido que la obtención de los mismos puede conducir a la realización de un fraude informático como es el smishing y phishing.

Por otro lado, citamos a López (2018) determinando que, la **recolección de datos** se puede materializar mediante las redes sociales, siendo que es un medio donde se prolifera conductas ilícitas centradas, principalmente, en delitos patrimoniales, ocasionando que la cifra de perjudicados sea muy cuantiosa, existiendo, además, importantes inconvenientes en su investigación (p. 5). Por ende, en nuestra opinión, consideramos que las redes sociales es una más, de las tantas maneras para cometer un fraude informático, debido que, existen

nuevas modalidades como es el smishing y phishing que mediante un mensaje o página web buscan cometer un acto defraudatorio.

Siguiendo lo antes referido, Vinelli (2021) señala que, el **fraude informático:** "es una forma de estafa. De la misma manera, se debe delimitar terminantemente el crimen de fraude informático con el delito de hurto, toda vez que no existe un bien material objeto de extracción, sino un tratamiento informático doloso que ocasiona una transferencia bancaria (p. 10). Complementando con nuestra idea, no nos encontramos de acuerdo por lo arribado con el autor, debido que el fraude informático no debe relacionarse con el delito de estafa, ya que, para su comisión delictiva implican diferentes supuestos, como, por ejemplo, la utilización del internet para cometer el delito.

Finalmente, tenemos a Rueda (2021) señalando que el **phishing** como delito informático es practicado hacia los usuarios de correo electrónico y redes sociales, debido a que, los ciberdelincuentes usan formas sutiles de engañar a personas con poco conocimiento en actividades digitales, logrando así la extracción de información y claves bancarias (p. 3), asimismo, tenemos García (2021) precisando que el **smishing** ha resultado una de las variantes más preocupantes de la seguridad cibernética, ya que, es más fácil el bloqueo del phishing con computadoras que el smishing debido a que resulta más fácil tener acceso recto a una página con el vínculo (p. 22). Es de menester señalar que, la única manera de protegernos de las nuevas modalidades de fraude informático es con el apoyo colectivo de todas las autoridades competentes del país, aunado a ello, consideramos importante imponer una ley que regule obligatoriamente a las páginas web y mensajes de texto con la finalidad de prevenir el smishing y phishing.

Ahora bien, en cuanto a los **antecedentes nacionales**, citando a Custodia (2021) centrándose en estudiar las actuales modalidades delictivas de **fraude informático**, que se deben de ajustar expresamente en la ley especial, incorporándose en el artículo 8 de la Ley N° 30096. En ese sentido, la conclusión que destaca su investigación está orientada a que la Ley Especial de Delitos Informáticos está constituido por artículos amparando ciertas circunstancias del

crimen informático, que en su totalidad no regulan las nuevas modalidades que actualmente surgen; teniéndose en cuenta que la norma está vigente desde el año 2013, habiendo pasado años de estar obsoleto, pese a que con el avance de la ciencia el cibercriminal ha creado nuevas maneras de menoscabo pecuniario a sus damnificados, evidenciándose que existe una escasa normativa penal sobre los delitos cibernéticos en contraste a otras legislaciones como la de Colombia que es pionero en la aplicación de ilícitos informáticos. (p. 46)

Barboza, Ataucusi y Celiz (2021) todos ellos; llegaron a la conclusión que, el malware ha adquirido una rapidez de crecimiento demasiado rápido ofreciendo a la comunidad hacker la facilitación para que puedan establecer nuevos atentados. A pesar de la lucha constante y la mejora es humanamente inviable que se elabore una resolución para algunos códigos se propagan en cuestión de minutos, siendo la solución para este tipo de advertencias, al menos un primer frente de protección, sino que deben aplicarse medidas de seguridad mediante las actuaciones que se llevan a cabo en el computador. De esta manera, cada vez que se intente realizar un ataque al sistema de la computadora, como es el caso de las aplicaciones para pharming, sea reconocido el ataque y frenado, así como el repertorio que lo ha realizado. (p. 35)

En palabras de Mengoa (2021) el autor concluye que, en el Perú se castiga el acceso ilícito a un procedimiento informático, pero no hay un régimen real del delito de fraude informático, pudiendo decirse que es necesario de un actor sin el cual no se podría materializar el delito. El sistema actual penal peruano está comprendido de dificultades para prevenir, contrarrestar y sancionar los fraudes cibernéticos, pues la identificación física de la persona que cometió el delito, la falta de patrimonio de la persona natural para reparar los daños que no han sido solucionados de manera jurídica en el país. (p. 55)

Ahora bien, en alusión a las conductas delictivas no reguladas en el ordenamiento jurídico peruano Hidalgo y Solano (2021) concluyen que, es necesaria que los legisladores del Congreso de la República creen un tipo penal específico, regulando correctamente los delitos cibernéticos como el phishing y pharming, estableciendo una conducta típica, el bien jurídico protegido, así como

una pena en relación a la magnitud del daño causado a los bienes jurídicos y probablemente en materia civil, los daños y perjuicios. (p. 119)

Asimismo, Sosa (2022) concluye que las modalidades del **phishing y smishing** es un atentado informático porque cumple con los requisitos de ser un comportamiento que se aprovecha del uso ilícito de tecnología para el acceso de datos informáticos privados y usarlos en afectación al daño patrimonial de los sujetos pasivos del delito. El delito de fraude informático a través de las modalidades “phishing y smishing” no se encuentra expresamente regulado en la Ley N° 30096 a pesar de contar con delito nuclear, el crimen contra la propiedad en la modalidad de fraude informático. Uno de los análisis que se pudo realizar es la existencia de disposiciones generales en cuanto al delito de suplantación de identidad dejando de lado la verdad material, que aunque parecidos como el phishing y pharming, que actualmente no gozan de normativa legal adecuada. (p. 65)

Continuando con el desarrollo del marco teórico, en este apartado abordaremos lo concerniente a la **fundamentación teórica** en relación a las categorías, así como también a las sub categorías. Ahora bien, en cuanto a la **primera categoría**, esto es, **El uso de los datos personales**, el autor Ducuara (2018) apunta que los datos personales acumulados por los servicios de internet, logran identificar que el servicio que mayor información administra es Google seguidamente por Facebook, Microsoft, Twitter entre otros. (p. 55). Lo descrito por el autor se relaciona justamente con nuestra **subcategoría N°1,** es decir los **datos sensibles**, siendo que los datos sensibles constituyen información confidencial de los usuarios como el acceso a sus cuentas bancarias. Por otro lado, Remolina, (2013) citado en Galvis et al., (2019). [...] El derecho a la defensa de datos personales no se reduce a los datos relacionados con la intimidad de las personas. No debe confundirse el primero con el derecho a la privacidad de las personas. La protección de datos personales comprende cualquier índole de esta indagación (privada, sensible, semi privada y pública. (p. 65)

En lo concerniente a la **subcategoría N°2, recolección de datos**, Gómez (2018) los datos personales están asociados a herramientas tecnológicas, ya que, tradicionalmente están relacionados a documentos físicos, pero si se

considera al uso de las tecnologías de la información como un detonante para que se pusiera atención, la recolección de datos personales serían más seguras. Es así que, la importancia de la tecnología en la recolección de datos sigue siendo un tema por descubrir, debido a que la tecnología va transformándose cada día. Por su parte, Martínez (2018) citando a Ramírez (2019) plasmó los orígenes del denominado derecho a recolección de datos; siendo utilizada en la Ley del Censo del Tribunal Alemán como en otros instrumentos nacionales e internacionales que fueron tomados como referentes y por ello se ha considerado como un nuevo derecho, siendo así, autónomo e independiente al derecho a la intimidad. (p. 41)

Siguiendo ese orden de ideas, en lo que respecta a la **segunda categoría**, denominada, **fraude informático**, Miro y Contreras (2022) hacen referencia de que, “el fraude informático no exige o requiere la existencia de engaño, sino que, “el fraude informático tiene en su estructura diversas modalidades que implican una sustracción y/o manipulación a favor del ciberdelincuente. Es decir; el sistema de fraude es efectivo a través de las TICs, pues en ese momento no existe ningún engaño, empero, si es que existen interacciones a través de las TICs, es decir, Facebook, Instagram, Grindr, etc., no siempre pertenecen a la figura del fraude cibernético, sino que, se consuma como estafa por medio de las TICs. En ese entorno, guarda relación con nuestra **subcategoría N°1**, toda vez que, el **smishing** es una modalidad nueva de fraude cibernético que consiste en el engaño mediante tráfico ilegal de datos personales, una obtenidos estos serán usados ilícitamente sustrayendo su patrimonio. Por su parte, Miro y Contreras (2022) refieren sobre el **smishing,** “consiste en utilizar los mensajes de texto en telefonía celular, los cuales enmascaran en el contenido del mensaje de texto direcciones de instituciones”. (p. 346)

Ante ello, Rosero (2021) sostiene que la mejor prevención es estar preparados, lo que se logra mediante la capacitación constante a los usuarios, las herramientas físicas y lógicas que deben de existir en cada institución, además de planes de contingencia [...] (p. 17). En base a lo mencionado la prevención es importante en cualquier situación que pueda generar una consecuencia patrimonial.

Dentro de esta óptica y en lo que apunta a la **subcategoría N°2**, **phishing** refiere García (2018) lo define como una modalidad de fraude informático para obtener información confidencial siendo que la entidad financiera corresponde extender distintas acciones para prevenir la hurto de los datos personales de contenido económico del ordenador, como por ejemplo dar aviso inmediato que no se facilite información sensible en respuesta a correos electrónicos ni tampoco utilizar enlaces integrados en un email o acceder a páginas fraudulentas de terceros, advirtiendo a las oleadas de phishing y sobre todo implementar instrumentos que bloqueen las transferencias cuando puedan existir indicios de que las mismas puedan haberse realizado de forma fraudulenta. En caso contrario, los bancos a la luz de la Ley 16-2009 de servicios de pago exponen a que se les exija una obligatoriedad civil cuasi-objetiva y deban de reintegrar el importe del traspaso fraudulento al usuario de los servicios de pago.

Continuando, haremos referencia al **primer enfoque conceptual** de la presente tesis, esto es, **fraude informático**, que consiste en un delito contra el patrimonio en las cuentas bancarias de los consumidores, debido a que los ciberdelincuentes hacen creer que las páginas ingresadas por los usuarios son seguras colocando sus datos personales, compartiendo en tiempo real información sensible para la comisión del delito, además, el fraude informático puede realizarse desde cualquier parte del país, incluso fuera del territorio nacional. Aunado a ello, el fraude informático no suele ser detectada en tiempo real, por lo que, hace más complicado la detección, no obstante, a ello, algunas entidades financieras cuentan con sistemas de seguridad que logran su detención en base al comportamiento habitual o patrón de consumo del usuario, para ello, la entidad bancaria debe de tener una base de datos de movimientos del consumidor, de lo contrario, no podrá detectarse y la estafa cibernética podrá ser cometida. Cabe precisar que existen diferentes modalidades de estafas cibernéticas siendo las más usuales la del phishing y smishing.

Asimismo, nuestro **segundo enfoque conceptual**, se refiere a la recolección de datos el cual es relevante para complementar la primera categoría de la presente tesis; dado que, siempre se recolectan datos sensibles como, por ejemplo, documentos de identidad, cuentas financieras, correos electrónicos,

entre otros, siendo las cuentas bancarias las más sensibles, puesto que, las medidas de seguridad que contratan las entidades financieras son fáciles de engañar.

Finalmente, como **tercer enfoque conceptual**, es menester que contextualicemos a la **vishing;** ya que, si bien no se encuentra dentro de nuestras subcategorías, pero forma parte de la clasificación de la segunda categoría de nuestra tesis. Ello se debe llamadas fraudulentas electrónicas que con astucia se hacen pasar por operadoras de entidades financieras para proponernos un aumento de línea de crédito, préstamo financiero, anulación de tarjeta de crédito entre otras más con la finalidad crear credibilidad para que el usuario pueda compartir sus datos personales cometiendo la estafa cibernética extrayendo dinero de sus cuentas bancarias, es de precisar que las llamadas son tan reales que los ciberdelincuentes logran cometer el acto ilícito.

**III. METODOLOGÍA.-** Respecto al presente capítulo, cabe advertir que el sustento de la metodología de investigación empleada para el desarrollo del proyecto tesis; por tal motivo, este trabajo tiene un enfoque hacia la **investigación científica cualitativa**, lo que permitirá a través de las respuestas obtenidas por los especialistas y documentos recabados, servirán para proceder a verificar los supuestos y de esa manera llegar a nuestros obtenidos, **respecto del enfoque cualitativo**, según afirma Piza, N., at el (2019) da cuenta como enfoques transversales a, "la observación, los grupos focales y la entrevista, con una síntesis de sus ventajas y limitaciones según los criterios de diferentes autores". (p. 9)

En ese sentido, desde el punto de vista de Piza, N., at el (2019) desde el análisis del enfoque cualitativo, se tiene que definir y resaltar la importancia de este tipo de enfoque, que es relevante para resaltar los contrastes que permiten crear teorías y así exponer dudas para ser resueltas, sobre una determinada teoría, asimismo, propusimos supuestos que dieron respuesta al problema planteado, posterior a un análisis exhaustivo de datos de la información que se ha recopilado. (p. 9)

Asimismo, es importante precisar que, existen dos tipos de enfoques: enfoque cuantitativo y enfoque cualitativo; tal y como refiere, Galeano (2020) al advertir que presuntamente existe una visible distinción entre el uno y el otro; tal que, cuando se refiere al enfoque cuantitativo, precisa que, emplea un estudio basado en la aplicabilidad de la estadística, a diferencia del cualitativo, dado el tipo de enfoque va centrado a los argumentos, posturas y determinados pensamientos de índole inferencial (p. 13)

En tanto; Lio (2020) precisa que, el enfoque cualitativo va a ser el procedimiento mediante el cual a partir de una base de interpretación que se da a causa del efecto generado por las múltiples aplicaciones y metodologías contemporáneas; advirtiendo primero respecto de la fenomenología, teoría fundamentada; etc. las cuales tienen como objetivo de estudio a los problemas reflejados en la sociedad.

## 3.1. Diseño y tipo de investigación

En el mismo orden de ideas, debemos dejar señalando que la presente tesis estará conformado a través de una investigación básica, en concordancia con el enfoque cualitativo que se viene desarrollando, lo cual, en palabras de Alvares, 2020 “Investigación va orientada a conseguir un mayor conocimiento en una línea sistemática, con el objetivo de contribuir en conocimiento de la realidad”. (p. 03)

Seguido de la **teoría fundamentada** la cual afirma Arias et al, (2021) “es preciso destacar, como metodología, precisando su tres grandes aspectos; el primero, lo podemos definir como la descripción, misma que, se realiza sobre objetos, personas, escenas, acontecimientos, acciones, emociones, estados de ánimas y aspiraciones que son objeto de estudio. Dando cuenta sobre el propósito, el público y el observador […] El segundo es el ordenamiento conceptual; relatos etnográficos, etapas o pasos, tipo de actores o acciones […] Lo anterior estaría contribuyendo respecto de la teorización (es el objeto último de la teoría fundamentada). (p. 70)

Consecuentemente en últimos términos, la presente tesis se estableció un nivel **descriptivo**, lo cual, en palabras de Carrasco afirma Condori (2020) la investigación descriptiva busca, “Conocer, identificar, describir las características de fenómeno social”. (p. 4)

## 3.2. Categorías, Subcategorías y matriz de categorización

Para poder llevar a cabo la presente investigación es debemos advertir que, las categorías en el enfoque cualitativo vienen a ser la figura principal, debido a que, a partir de ello se funda las bases de la presente tesis, la misma que, va a permitir analizar y determinar resultados determinados y determinantes, por medio de los cuales vamos a encontrar las conclusiones más coherentes abocadas al fin supremo de nuestra investigación.

En tanto, con respecto a las categorías uno y dos, así como, las subcategorías que se plantearon en la presente investigación señalamos lo siguiente: La **primera categoría** es el uso de los datos personales. Como

subcategorías: datos sensibles y recolección de datos. La **segunda categoría** es fraude informático. Como subcategorías: smishing y phishing.

### 3.3. Escenario de estudio

Al advertir respecto del entorno de estudio, este puede ser tratado como el área determinada donde se llevará a cabo la investigación, así como, la recolección de los datos propiciados por los participantes; en ese contexto, se puede sostener que, ese va a ser el escenario donde se aplicarán los instrumentos validados y diseñados por los respectivos expertos. Entonces, cabe hacer mención, que la ficha de entrevista, como propio instrumento que se ha empleado en este trabajo, sea aplicada a las personas que se encuentren capacitadas para contextualizar el problema de nuestra tesis; en ese sentido, el escenario de estudio abarcó la totalidad del territorio peruano, lo cual en esencia sería el departamento de Lima como zona focalizada, en donde se obtuvo información de profesionales en derecho y software especializados en delitos y fraudes cibernéticos, así como de ingenieros especialistas en sistemas, finalmente se ha considerado la documentación recolectada con objeto de estudio acerca del smishing en nuestra legislación actual.

### 3.4. Participantes

De manera correlativa a los anteriores párrafos, llegados a este punto cabe subrayar a nuestros participantes de los cuales se detallará la categoría de las personas intervinientes en las respuestas de nuestra ficha de entrevista. Como hemos señalado, serán abogados especializados en el ámbito de fraudes cibernéticos penal e ingenieros de sistemas especialistas en informática y temas financieros.

**Tabla N°1 -** Cuadro de participantes de estudio

| DESCRIPCIÓN | DATOS DEL PARTICIPANTE |
|---|---|
| **FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA** | Dr. Juan Humberto Flores Cáceres<br>Dra. Martha Elena Munayco Medina |

| | |
|---|---|
| | Dra. Karina Raisa Quispe Ali<br>Dra. Ingrid Vallejos Ramos<br>Dra. Tania Bobadilla Centurión |
| **FISCAL ESPECIALIZADO EN CRIMEN ORGANIZADO** | Dr. José Miguel Cuya Berrocal |
| **INGENIEROS DE SISTEMAS ESPECIALIZADOS EN TECNOLOGÍAS DE LA INFORMACIÓN.** | Ing. Mauro Zevallos Morales<br>Ing. Irving Lyonel Solsol Vilca |
| **ABOGADA ESPECIALIZADOS EN DERECHO PENAL** | Dra. Meri Liliana Padilla Virhuez |

***Fuente:*** *Elaboración propia*

### 3.5. Técnicas e instrumentos de recolección de datos

Para describir el presente criterio, debemos explicar la forma por medio de los cuales serán nuestros métodos en instrumentos de investigación para recoger la información requerida, la cual en adelante deberá ser analizada, contrastada y así mismo discutida. De tal forma que, la información recabada nos va a ayudar a dar una solución probable a nuestra problemática planteada. Para finalizar, la presente tesis tendrá como técnica de recolección de datos a la entrevista, asimismo, el análisis de fuente documental. Así mismo afirma Hernández et al (2020) "[…] respecto de las técnicas para la recolección de datos han comprendido, procedimientos y actividades que permiten a los investigadores en general la obtención de información necesaria para dar respuesta asertiva respecto de su problema de investigación". (pp. 51-53)

**LA ENTREVISTA:** En referencia a este punto cabe señalar que, la entrevista es una de las técnicas actualmente más importante dentro de una investigación de carácter cualitativo debido a que permite la recolección de datos de manera directa de una determinada población o muestra. Por lo cual refuerza Torres et al (2019) Actualmente es importante reconocer el gran aporte a las investigaciones que tiene la entrevista. Permite tener un acercamiento con el

entrevistado para obtener su propio criterio. Fundamentalmente por medio de este instrumento el entrevistado aporta aspectos pertinentes a la solución de nuestro problema general. (p. 13)

**FICHA DE ENTREVISTA:** Es de considerar como el instrumento ineludible por el cual vamos a aplicar la técnica como tal, por lo que se considera como la parte técnica de la misma. Por lo cual, señala Useche et al (2019) “La ficha de la entrevista confirma una orientación precisa al momento de diseñar la investigación, es un refuerzo para que el investigador o entrevistador enfoque su tiempo en recabar información objetiva respecto del tema al que, se ha indagado y no dilatar en aspectos no relevantes al caso”. (p. 39)

**Fuentes de documentos:** Debemos entender que la misma es un trabajo de desarrollo de capacidades, por lo cual se le va a brindar a una determinada interrelación entre la documentación original y la información obtenida. Por lo que, Valencia (2018) “se identifica investigaciones anteriores a través de la revisión documental (…) La revisión documental permite que se pueda configurar y finalizar la investigación”. (p. 23)

**Ficha de Análisis de Fuente de Documentos:** En esa línea, así como hemos venido desarrollando respecto de la entrevista, las técnicas que se van a emplear en la tesis tienen carácter referencial por lo que, las mismas se deberán de aplicar mediante instrumentos a la realidad propia. Por lo cual, corresponde al análisis de fuente documental, que, a través de determinadas resoluciones, jurisprudencia, doctrina y su misma investigación científica, relacionándose con las categorías planteadas en la presente tesis.

### 3.6. Procedimiento

A través de lo que se ha venido realizando, comprendiendo una exhaustiva búsqueda de información documental, a fin de poder identificar y determinar la problemática de la investigación, y de esa manera formular los problemas de estudio. Elaborando y estructurando de modo tal, nuestras justificaciones, nuestro objetivo general, nuestros objetivos específicos. Respecto de los instrumentos que se ha ocupado, se ha tenido a bien considerar la ficha de entrevista aplicada a nuestros expertos, y, la guía de análisis de documentos.

Finalmente, se respetó el rigor científico, los aspectos éticos, para poder obtener nuestros resultados, conclusiones y recomendaciones.

Debemos tener en cuenta el que en este proceso, vamos a verificar la información obtenida a través de técnicas, las cuales se cruzaran datos para determinar nuestros objetivos planteados, por lo que finalmente vamos obtener nuestras propias conclusiones, las mismas que van a corresponder al problema planteado. En tanto, se va a analizar acerca de:

**Tabla N°2 –** De las categorías y subcategorías

| **CATEGORÍA 1** | |
|---|---|
| USO DE DATOS PERSONALES | |
| **SUB CATEGORÍAS 1 Y 2** | |
| DATOS SENSIBLES | RECOLECCION DE DATOS |
| **CATEGORÍA 2** | |
| FRAUDE INFORMÁTICO | |
| **SUB CATEGORÍAS 1 Y 2** | |
| SMISHING | PHISHING |

***Fuente:*** *Elaboración propia*

### 3.7. Rigor científico

Con respecto al rigor científico tenemos que entender que, la calidad que corresponde a la investigación, así como la fidelidad debe ser de alta rigurosidad, así como lo señala, Guillen, C., at el (2021) “cualidad humana, de los procesos de investigación, cuyos discursos de orden científico presentan una gran exactitud y una lógica inflexible”. (P. 48)

En el mismo orden de ideas, podemos entender que el rigor de la tesis se ha evidenciado a través de los participantes y a quienes se han tenido considerados en la entrevista, por el medio de la cual se ha comprobado la calidad y estándar profesional de cada entrevistado, evidenciando de ese modo sus capacidades en dar respuesta a la investigación. Mismo que, evitará que se

entienda, que los entrevistados no conocen de la temática abordada, por ello deben ser aptos para dar información valiosa, que destaque, y que, al finalizar la investigación se haya logrado lo propuesto como investigación.

Para finalizar, con lo que respecta al rigor científico que se va a tener sobre la ficha de análisis de fuente documental, se debe realizar el destilado correspondiente del análisis documental. Teniendo ese objetivo, es que el documento debe ser obtenido con arraigos genéricos. Como segundo punto, es la identificación de dicho material documental.

**Tabla N°3 -** Validación de instrumentos

| **DESCRIPCION DEL CUADRO DE LA VALIDACION DE NUESTRA GUIA DE ENTREVISTA** | | |
|---|---|---|
| **DATOS DE LOS EXPERTOS** | **CARGOS QUE EJERCEN** | **PORCENTAJE** |
| **Munayco Medina, Martha Elena** | Fiscal Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia | 95% |
| **Padilla Virhuez, Meri Liliana** | Abogada Penalista del Estudio Jurídico – Padilla Abogados & Consultores | 95% |
| **Marchinares Ramos, Lidia** | Docente de la Universidad Cesar Vallejo - Metodología | 95% |
| **Cuya Berrocal, José Miguel** | Fiscal Provincial del Tercer Despacho de Crimen Organizado | 95% |
| **PROMEDIO EN TOTAL** | | 95% |

***Fuente:*** *Elaboración propia*

### 3.8. Método de análisis de información

**Al enfatizar sobre la triangulación** debemos precisar que, respecto a la triangularización ha sido necesario aplicar métodos que han sido correctos para comprender la información recabada. Pues, la misma, consta de material documental que requiere de un riguroso análisis. En tanto, todo lo anterior debe de tener como base principal la teoría fundamentada; asimismo, se utilizó un método específico (método sistemático). Consta de las entrevistas, las cuales han sido resueltas por los participantes a través de los instrumentos planteados; seguido de hermenéutico; debido a que se recogió la opinión técnica bajo criterio diverso de los entrevistados, lo que reforzó nuestra investigación teniendo, en la misma línea fue analítico, ya que, cada participante a través de su vasto conocimiento jurídico y técnico, nos han permitido analizar el uso de los datos personales en las nuevas modalidades de fraude informático.

| | |
|---|---|
| **Metodo de analisis de recoleccion de datos** | Sistemático |
| | Hermenéutico |
| | Analítico |
| | Comparativo |
| | Inductivo |

***Figura N° 1 -*** *Métodos de Análisis*

### 3.9. Aspectos Éticos

La investigación respecto de los aspectos éticos de la investigación, haciendo referencia a la presente temática, misma que lleva como enfoque cualitativo, respetando los derechos de Autor, misma normativa se comprende

en el manual de referencias American Psycological Association (APA), el cual apunta a utilizar conocimientos preconcervados, para que de ese nodo se pueda obtener conocimientos, sociales, políticos, etc. Asimismo, se ha comprendido el cumplimiento respecto de lo preestablecido por la Resolución de Vicerrectorado de Investigación N°062-2023-VI-UCV actualizada a fecha 16 de marzo del 2023, Ayudando de ese modo a dar solución o resolviendo los objetivos planteados y no se de una perpetua violación de la moral, saliendo a relucir los valores e intrínsecos principios humanos.

## IV. RESULTADOS Y DISCUSIÓN

Respecto del presente capítulo, se podrá plasmar y analizar lo referente a la información recopilada a través de los instrumentos utilizados para recolectar los datos de la presente tesis, es decir, el de la ficha de entrevista, así como la ficha de análisis documental elaborado acorde a nuestra investigación.

Asimismo, en alusión a nuestro **objetivo general** propuesto “Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático”.

### Resultados obtenidos por parte de nuestros expertos entrevistados

De lo advertido en nuestra **primera pregunta** de la ficha de entrevista; esto es: “Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático? Ellos respondieron lo siguiente:

Flores (2023), Munayco (2023), Quispe (2023) y Vallejos (2023), señalaron que los datos personales en las nuevas modalidades de fraude informático se emplean en el perfilamiento de las potenciales víctimas a fin de poder ejecutar desde una suplantación de identidad, debiendo de tomar en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima.

De igual modo, Padilla (2023), Cuya (2023), Bobadilla (2023) y Solsol (2023) sostienen que, los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. Una vez obtenida, esta será usada para fines delictivos como es el delito de phishing.

No obstante, Zevallos (2023) refiere que, los datos personales se tienen que verificar con el propósito de validar la identidad de una persona natural o jurídica ante una plataforma tecnológica con el fin de obtener un lucro económico y/o la obtención de información.

Con respecto a nuestra **segunda pregunta** la ficha de entrevista; esto es: "En su opinión, ¿todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

Flores (2023), Munayco (2023), Quispe (2023) y Vallejos (2023), indicaron que todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático, debido a que, en estos tiempos, se confunde muchos los delitos informáticos, con los delitos computaciones; que están relacionados a todos los eventos en la que el agente tiene como herramienta de trabajo una computadora, un teléfono o cualquier herramienta tecnológica y de una u otra forma el agente realiza actuaciones en contra de los intereses de la empresa lo cual bien puede ser una estafa, apropiación ilícita, fraude en la administración de personas jurídicas, etc.

Por su parte, Solsol (2023) y Zevallos (2023) contemplan que, los ciberdelincuentes en muchos ataques informáticos tienen propósitos de afectar el funcionamiento de redes de comunicaciones y/o sistemas informáticos, terminan obteniendo información sensible y que posteriormente cometiendo fraudes de personas jurídicas o personas naturales, si bien es cierto que el bien jurídico protegido en los delitos de fraude informático es el "patrimonio", este debe cumplir con los elementos constitutivos: sujeto activo genérico, sujeto pasivo genérico; que el sujeto activo implemente una conducta "engañosa" que "induzca al error" a la víctima; orientado a la obtención de un beneficio económico (ánimo de lucrar).

De la misma manera, Padilla (2023) y Cuya (2023) apuntan que, el medio de realización de los delitos es mediante plataformas digitales, buscando afectar el patrimonio que es la única finalidad de los ciberdelincuentes.

Por otro lado, Bobadilla (2023) señala que, el fraude es un concepto engañoso, que no tiene solución con el resultado típico, pero no todas las conductas delictivas deben de constituir el delito del fraude cibernético.

Asimismo, de lo referido a nuestra **tercera pregunta** de la ficha de entrevista; esto es: "desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo? Los entrevistados expusieron lo siguiente:

Flores (2023), Munayco (2023), Quispe (2023), anotan que el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las TICs como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada. Por lo que, en nuestra vida cotidiana, se dan situaciones en las que se induce a error al sujeto pasivo, así por ejemplo si Juan haciéndose pasar como trabajador de una entidad bancaria realiza llamada a María comunicándome que debe realizar el cambio de su tarjeta por una nueva en la cual se amplía su línea de crédito, para lo cual un funcionario de PROSEGUR se constituirá a su inmueble a recoger la tarjeta llevando además documentos a firmar, María quien en ese momento requería de dinero procede a entregar su tarjeta y luego del cual recibe una llamada del banco en el sentido que desde su cuenta, se habían realizados transferencias de dinero, otra modalidad es cuando la persona accede a una página clonada en la cual consigna información personal y bancaria.

Según, Bobadilla (2023) y Zevallos (2023) destacan que, se puede consumar el fraude informático al inducir a error, en cuyo caso se hace más compleja la obtención de evidencia digital que contiene la atribución de los actos ilícitos mediante la obtención de datos sensibles de una forma ilegítima.

A diferencia de Padilla (2023) quien rechaza esta postura; puesto que, considera necesario que el fraude informático se tiene que configurar mediante la tecnología, ya que, sin los datos personales de la víctima, no podría cometer su perjuicio patrimonial.

**Análisis e interpretación de las categorías apriorísticas y emergentes**

**Respecto del objeto general:**

| |
|---|
| Analizar el uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022. |

En merito a nuestra **categoría emergente** encontrada en nuestros resultados, generados a partir de nuestro objetivo general, en referencia a las respuestas obtenidas por parte de los entrevistados, se advierte que, para poder obtener determinados datos para ejecutar o consumar un delito, se entiende que, a razón de las respuestas obtenidas, la categoría emergente sería el **"perfilamiento de víctima".** Pues, tenemos que enfatizar en que este tipo de delito no está dirigido hacia un solo perfil de personas, dado que, estas deben poseer dinero en entidades bancarias o mantener a su nombre, cuentas corrientes, tarjetas de crédito, etc.

Siendo así, y en alusión a nuestro **objetivo específico N°1** "Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático".

**Resultados obtenidos de nuestra ficha de análisis de fuente documental**

En relación a nuestro objetivo general focalizamos dos (2) fuentes documentales; de los cuales extrajimos lo que se hace mención y se muestra a continuación:

En primer lugar, el **Recurso de Nulidad N° 743-2018**, prevé que, para ingresar al sistema informático se utiliza información confidencial proporcionada por malos elemento de las entidades que tiene bajo su tutela datos personales de los usuarios de sus funciones (usuario y contraseña) para ingresar al sistema informático con la finalidad de modificar ingresando datos falsos para lograr que los administrados tengan un duplicado de licencia, pero bajo una categoría que no les correspondía.

Seguidamente, la **Resolución Final N° 0001-2023/INDECOPI-CCHT** advierte que, se ha demostrado respecto de que los proveedores son responsables por la calidad e idoneidad de los productos y prestar los servicios al consumidor en las condiciones entregar los productos y prestar los servicios al consumidor bajo los criterios y condiciones previstos por ambas partes con la voluntad propia del consumidor, así como la del proveedor.

**Resultados obtenidos por parte de nuestros expertos entrevistados**

Con respecto a nuestra **cuarta pregunta** de la ficha de entrevista; esto es: “PREMISA: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa. En ese orden, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?” ellos han respondido lo siguiente:

Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Cuya (2023), Padilla (2023), Zevallos (2023) y Bobadilla (2023) indicaron que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Por ello, si hay un procesamiento de datos y transacciones bancarias pero ilícito, correspondiendo

evaluar en qué circunstancia o situación nos encontremos, en todo caso la manera de procesar datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos.

A su vez, Solsol (2023) declara que, el smishing se limita a que el agraciado o víctima sea redirigido a un sistema de información (página web, entre otros), la misma que pueda ser un sistema clonado o falso para que posteriormente los ciberdelincuentes con la información recolectada ejecutar sus actividades delictivas.

En el mismo orden, con relación a la **quinta pregunta** de la ficha de entrevista; esto es: “por otro lado, ¿considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

Flores (2023), Munayco (2023) y Vallejos (2023), exponen que en cierta forma si hay un procesamiento de datos y transacciones bancarias pero ilícito, corresponde también evaluar en qué circunstancia o situación nos encontremos, en todo caso la manera de procesar estos datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Ante esto, se podría decir que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje.

En ilación con esto, Quispe (2023), Cuya (2023) y Padilla (2023) atisban que, el smishing consiste en pedir a los clientes que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje.

Acorde a lo planteado, con relación a la **sexta pregunta** de la ficha de entrevista; esto es "según su percepción sobre esta temática, ¿cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Quispe (2023), Cuya (2023), Padilla (2023) y Flores (2023) exponen que el Estado, las entidades bancarias y las empresas de telecomunicaciones en acción conjunta deberían brindar, realizar y motivar campañas de sensibilización e información concreta, sencilla y accesible para todos los usuarios, de manera que pueda ser de fácil acceso y compresión respecto al uso y restricción de sus datos personales; asimismo, uniformizar e individualizar de manera correcta sus canales de comunicación, acceso y atención al cliente de manera que frente a mensajes, correos electrónicos y otras modalidades, se encuentren informados de no brindar sus datos personales y finalmente implementar un instrumento o protocolo de adecuada identificación de los usuarios. De igual modo, la solución para esta modalidad de fraude informático del smishing, es la educación y prevención financiera en relación a los mensajes de texto fraudulentos, esta tarea debe ser realizada por las mismas entidades financieras y las autoridades estatales.

Mientras que Vallejos (2023), Zevallos (2023) adoptan una postura más bilateral sobre esta interrogante; consistente en desconfiar de los remitentes desconocidos, no facilitando la información que pide el mensaje de texto, sobre todo si se trata de datos personales o bancos, no abriendo los enlaces que adjuntan y bloqueando el número telefónico en caso de no reconocer el origen

(también llamado como SPAM). Asimismo, resulta importante trabajar con herramientas tecnológicas de seguridad cibernética y su difusión, concientizando a las personas a no confiar en ese tipo de información recibida.

**Respecto a nuestro objetivo específico N°1:**

| |
|---|
| Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático. |

Respecto de la **categoría emergente** identificada en los resultados correspondientes al **objetivo específico N°1**, en referencia a lo aportado por parte de nuestros especialistas, se ha señalado que, para generar u obtener datos se realizan a través del smishing, este a su vez, utiliza "**hipervínculos incluidos"** mismos que van a generar la conexión entre los datos obtenidos y la información bancaria de las cuentas de la víctima.

Permitiendo de esta forma explicar el modo o de qué manera se utiliza el smishing para la comisión de los delitos informáticos en la modalidad de fraude informático.

**Resultados recopilados en nuestra ficha de análisis de fuente documental**

En relación a nuestro **objetivo específico N°1** focalizamos dos (2) fuentes documentales; que se muestran a continuación:

En suma, el **Proyecto de Ley N° 398/2021-CR**, prevé que los **fraudes informáticos** no solamente se expanden por los servicios financieros, sino por diferentes medios perjudicando a los ciudadanos de manera general, esto debido a que, los medios informáticos pueden conectarse por diferentes plataformas, como redes sociales, correos, aplicativos instalados en el celular, entre otros más. Es importante acotar que la pandemia por la COVID-19 no ha sido impedimento para la realización de los fraudes informáticos en sus diferentes modalidades más conocidas como el phishing y smishing.

Es así que, por las razones expuestas en los párrafos que anteceden, y en sintaxis con lo estipulado en el **Artículo Científico "seguridad por capas frenar ataques de smishing,** se busca prevenir el ataque del smishing mediante la educación en sus diferentes niveles (inicial, primaria y secundaria), asimismo, a nivel empresarial, los proveedores de tarjetas de crédito o débito, deben de encargarse de la capacitación constante de su personal, con la finalidad mejorar la instrucción a los usuarios financieros disminuyendo el número de las posibles víctimas del ataque de smishing, finalmente, otra capa de solución a esta modalidad del fraude informático es la instalación de antivirus efectivos desde que se compra el equipo móvil, en otras palabras que el operador telefónico cumpla con instalar predeterminadamente en sus funciones del móvil el aplicativo antismishing.

**Resultados obtenidos por parte de nuestros expertos entrevistados**

Siguiendo el orden de nuestras preguntas, la **séptima pregunta** planteada en la ficha de entrevista; esto es: "desde su experiencia, ¿de qué manera se utiliza el phishing para la comisión del delito de fraude informático? Los entrevistados plantearon lo siguiente:

Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) explayaron que la materialización del phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. Por ende, consideran común esta estafa y comercializando los datos personales de muchos usuarios.

En adición a esto, se tiene lo estipulado por Cuya (2023) y Padilla (2023) al mencionar que, el phishing de manera similar que el smishing, se materializa mediante un medio electrónico. En el caso del phishing es un correo electrónico - de los casos más comunes que he tomado información – el emisor del phishing se hace pasar por una entidad financiera enviando publicidad o alguna información referente a su cuenta bancaria de la víctima, es aquí, cuando el

consumidor cae en el anzuelo compartiendo sus datos personales sensibles y logrando darles un beneficio a los ciberdelincuentes.

Dentro del planteamiento en nuestra **octava pregunta** de la ficha de entrevista; esto es: “de acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing? Los entrevistados plantearon lo siguiente:

Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) coinciden que, en la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. No obstante, algunos autores expresan su progreso mediante el equipo de fiscales y peritos informáticos para indagar y articular de forma correcta la investigación de estos delitos.

Por otro lado, se tiene las posturas de Padilla (2023) y Cuya (2023) quienes denotan que, el Ministerio Publico no cuenta con instrumentos o programas tecnológicos para erradicar las modalidades de fraude informático. Considerando que el Ministerio Publico debería tener apoyo de otras autoridades como el INDECOPI o la División de Delitos Informáticos de la Policía Nacional del Perú. Este último, si cuenta con los instrumentos tecnológicos para combatir estos delitos cibernéticos.

En última instancia a virtud de nuestra **novena pregunta** de la guía de entrevista; esto es: “desde su expertise, ¿qué alternativas de solución plantearía a fin de que, se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) examinan que, para evitar este tipo de situaciones, los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o

virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos.

De igual manera, Padilla (2023) y Cuya (2023) decretan que, la alternativa de solución, para erradicar el phishing es la creación de programas que puedan detectar correos falsos que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que el programa de mensajería instantánea consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace. De la misma forma que el smishing, las entidades financieras y otras autoridades públicas deben capacitar a la ciudadanía para evitar ser víctima de estos fraudes informativos.

**Respecto al objetivo específico N° 2:**

| |
|---|
| Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático. |

En tanto, respecto de la **categoría emergente** identificada en los resultados obtenidos, respecto al **objetivo específico N°2,** en las referenciales respuestas parte de nuestros entrevistados, examinan que, para evitar este tipo de situaciones referidas al uso de los datos personales en las nuevas modalidades de fraude informático, específicamente a través del phishing, mencionan que, los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos.

Esto supone que, nuestra categoría emergente a partir de la expertise de los entrevistados seria “cultura informática”. Esto permite explicar mejor el reducir los índices de delitos informáticos consumados a través de esta modalidad.

**Resultados obtenidos de nuestra ficha de análisis de fuente documental**

En relación con nuestro **objetivo específico N°2** ubicamos dos (2) fuentes documentales; que se muestran a continuación:

En resumidas palabras, en atención a nuestro referido objetivo y concordantemente con lo expuesto en la citada **Sentencia P.A.M.** de 12 de marzo de 2018 refiere que, la comisión del delito de **fraude informático**, **por medio de phishing** usualmente se realiza a través del que ordena algún pedido online no es el titular de la cuenta) es un riesgo a cargo del banco. Asimismo, la **Sentencia A.P. Burgos** de 03 de marzo del 2016, sostiene que, el fraude informático a través del phishing no requiere una estructura propia de esta modalidad, por eso es que, cuando se cometa este tipo de fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que la información que se podría obtener nos podría indicar como se ha realizado el **phishing.**

A manera de conclusión, se puede indicar que el **Boletín Semanal - SBS Informa N° 26 de la SBS,** prevé que, en este proyecto se busca brindar mayores mecanismos de protección en las etapas de contratación, uso y cancelación de dichas tarjetas; así como fortalecer las medidas de seguridad de las operaciones y productos financieros vinculados a las mismas. Asimismo, mediante el precitado Boletín Semanal, se analizó estadísticamente el crecimiento de los pagos a través de los medios electrónicos habiendo crecido las transacciones monetarias, lo que incrementó las modalidades de fraude informático, sin embargo, esta medida no ha reducido los fraudes informáticos como es el phishing.

## DISCUSIÓN

En la misma línea de ideas, pasando a desarrollar este ítem, y en aplicación del método de triangulación, se analizaron los datos e información recogida a través de nuestra ficha de entrevistas; asimismo, tuvimos en consideración a los aportes recolectados en la ficha de análisis de documentos; mismas que, han podido contribuir para la base de la presente investigación, así como los antecedentes recolectados, nacionales e internacionales, los cuales se planteó en nuestro marco teórico.

En ese sentido, y teniendo en consideración a nuestro objetivo general, procedemos a mostrar la siguiente tabla:

**Tabla N°4 – De la discusión del objetivo general**

| Objetivo General |
| --- |
| Analizar cómo se emplean los datos personales en las nuevas modalidades de Fraude Informático. |
| **Supuesto General** |
| Los datos personales fueron empleados para la comisión de delitos cibernético se ejecuta, a fin de obtener un lucro patrimonial tomando en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. Los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. En ese sentido, las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático. |

***Fuente:*** *Elaboración propia*

Al proceder al desarrollo de esta partitura, debemos precisar nuestra **primera pregunta;** Flores (2023), Munayco (2023), Quispe (2023) y Vallejos (2023), han llegado a concluir que, los datos personales en las nuevas modalidades de fraude informático se emplean bajo el perfilamiento de las potenciales víctimas, a fin de ejecutar desde una suplantación de identidad, debiendo de tomar en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima, recayendo hasta en un concurso real de delitos; así como, Fraude informático, subsecuente de Suplantación de identidad, acceso ilícito, estafa y fraude, etc.

Aunado a ello, Padilla (2023), Cuya (2023), Bobadilla (2023) y Solsol (2023) han concordado en lo siguiente, los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante

de los usuarios. Una vez obtenida, esta será usada para fines delictivos como es el delito de phishing.

Respecto de Zevallos (2023) concluye que, los datos personales se tienen que verificar con el propósito de validar la identidad de una persona natural o jurídica ante una plataforma tecnológica, con el fin de obtener un lucro económico y/o la obtención de información.

Siguiendo el orden de nuestra discusión, advirtiendo respecto de la **segunda pregunta**; Flores (2023), Munayco (2023), Quispe (2023) y Vallejos (2023), han explicado que, todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático, debido a que, en estos tiempos, se confunde muchos los delitos informáticos, con los delitos computaciones; que están relacionados a todos los eventos en la que el agente tiene como herramienta de trabajo una computadora, un teléfono o cualquier herramienta tecnológica y de una u otra forma el agente realiza actuaciones en contra de los intereses de la empresa lo cual bien puede ser una estafa, apropiación ilícita, fraude en la administración de personas jurídicas, etc.

Por su parte, Solsol (2023) y Zevallos (2023) explican que, los ciberdelincuentes en muchos ataques informáticos tienen propósitos de afectar el funcionamiento de redes de comunicaciones y/o sistemas informáticos, terminan obteniendo información sensible y que posteriormente cometiendo fraudes de personas jurídicas o personas naturales, si bien es cierto que el bien jurídico protegido en los delitos de fraude informático es el “patrimonio”, este debe cumplir con los elementos constitutivos: sujeto activo genérico, sujeto pasivo genérico; que el sujeto activo implemente una conducta “engañosa” que “induzca al error” a la víctima; orientado a la obtención de un beneficio económico (ánimo de lucrar).

En la misma línea, Padilla (2023) y Cuya (2023) apuntan que, el medio de realización de los delitos es mediante plataformas digitales, buscando afectar el patrimonio que es la única finalidad de los ciberdelincuentes.

Por otro lado, Bobadilla (2023) ha inferido que, el fraude es un concepto engañoso, que no tiene solución con el resultado típico, pero no todas las conductas delictivas deben de constituir el delito del fraude cibernético.

Ahora bien, de lo que respecta a nuestra **tercera pregunta**, teniendo en consideración que, al analizar si debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo, a lo que; Flores (2023), Munayco (2023), Quispe (2023), anotan que el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las TICs como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada. Por lo que, en nuestra vida cotidiana, se dan situaciones en las que se induce a error al sujeto pasivo, así por ejemplo si Juan haciéndose pasar como trabajador de una entidad bancaria realiza llamada a María comunicándome que debe realizar el cambio de su tarjeta por una nueva en la cual se amplía su línea de crédito, para lo cual un funcionario de PROSEGUR se constituirá a su inmueble a recoger la tarjeta llevando además documentos a firmar, María quien en ese momento requería de dinero procede a entregar su tarjeta y luego del cual recibe una llamada del banco en el sentido que desde su cuenta, se habían realizados transferencias de dinero, otra modalidad es cuando la persona accede a una página clonada en la cual consigna información personal y bancaria.

Según, Bobadilla (2023) y Zevallos (2023) destacan que, se puede consumar el fraude informático al inducir a error, en cuyo caso se hace más compleja la obtención de evidencia digital que contiene la atribución de los actos ilícitos mediante la obtención de datos sensibles de una forma ilegítima.

A diferencia de Padilla (2023) quien rechaza esta postura; puesto que, considera necesario que el fraude informático se tiene que configurar mediante

la tecnología, ya que, sin los datos personales de la víctima, no podría cometer su perjuicio patrimonial.

De lo antes mencionado, hemos tenido concordancias con los entrevistados, en el sentido de que, al analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático, llegamos a la conclusión que, Los datos personales en las nuevas modalidades de fraude informático se emplean en el perfilamiento de las potenciales víctimas, a fin de poder ejecutar desde una suplantación de identidad, debiendo de tomar en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. Asimismo, los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. En ese sentido, las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático, debido a que, en estos tiempos, se confunde muchos los delitos informáticos, con los delitos computaciones; que están relacionados a todos los eventos en la que el agente tiene como herramienta de trabajo una computadora, un teléfono o cualquier herramienta tecnológica y de una u otra forma el agente realiza actuaciones en contra de los intereses de la empresa lo cual bien puede ser una estafa. Finalmente, el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las TICs como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada. Por lo que, en nuestra vida cotidiana, se dan situaciones en las que se induce a error al sujeto pasivo, así por ejemplo si Juan haciéndose pasar como trabajador de una entidad bancaria realiza llamada a María comunicándome que debe realizar el cambio de su tarjeta por una nueva en la cual se amplía su línea de crédito, para lo cual un funcionario de PROSEGUR se constituirá a su inmueble a recoger la tarjeta llevando además documentos a firmar, María quien en ese momento requería de dinero procede a entregar su tarjeta y luego del cual recibe una llamada del banco en el sentido que desde su cuenta, se habían realizados transferencias

de dinero, otra modalidad es cuando la persona accede a una página clonada en la cual consigna información personal y bancaria. De igual manera, nuestras **fichas de análisis de documentos,** con referencia al **objetivo general,** posiciona lo referido por los entrevistados que adoptaron en su mayoría un enfoque directo de postura sobre el uso de los datos personales en las nuevas modalidades de fraude informático; en conexión a lo resuelto en el **Recurso de Nulidad N° 743-2018,** prevé que, para ingresar al sistema informático se utiliza información confidencial proporcionada por malos elemento de las entidades que tiene bajo su tutela datos personales de los usuarios de sus funciones (usuario y contraseña) para ingresar al sistema informático con la finalidad de modificar ingresando datos falsos para lograr que los administrados tengan un duplicado de licencia, pero bajo una categoría que no les correspondía. Dentro del mismo orden de ideas, se tiene lo advertido por la **Resolución Final N° 0001-2023/INDECOPI-CCHT** advierte que, se ha demostrado respecto de que los proveedores son responsables por la calidad e idoneidad de los productos y prestar los servicios al consumidor en las condiciones entregar los productos y prestar los servicios al consumidor bajo los criterios y condiciones previstos por ambas partes con la voluntad propia del consumidor, así como la del proveedor.

En ese orden, complementando a lo señalado por nuestras fuentes de documentos y reforzando cada postura de nuestros especialistas, podemos sostener como hallazgo de nuestro marco teórico lo Rodríguez (2018) que expresa respecto a los **datos personales:** “el incremento de la clasificación de fraudes informáticos en redes sociales vulneran los datos personales en Ecuador, asimismo, se puede afirmar que los usuarios tienen un gran desconocimiento de los fraudes informáticos siendo los más alarmantes, el smishing y phishing” (p. 61), Teniendo como punto central nuestra ponderación, tanto, de las fichas de entrevistas, así como las fichas de documentos, asimismo, el hallazgo de nuestro marco teórico, cada uno dirigido al **objetivo general** de la presente tesis, hemos podido consumar que, mediante el uso de los datos personales de los sujetos pasivos o víctimas han sido empleados para la comisión de delitos cibernéticos afectando al patrimonio en la modalidad de fraude informático. No obstante, desde nuestra óptica, estamos convencidos de que, si las entidades bancarias o las autoridades competentes para preservar los

datos personales a buen recaudo, no se presentaría la cantidad insostenible de casos respecto de este delito.

Para finalizar, debemos precisar que se ha comprobado el **supuesto general** planteado, es decir que, Los datos personales fueron empleados para la comisión de delitos cibernéticos afectando al patrimonio en las modalidades del delito de fraude informático.

**Gráfico N°1 – Introducción de datos**


***Fuente:*** *Elaboración propia*

**Tabla N°5 – De la discusión del objetivo específico N°1**

| Objetivo Específico N°1 |
|---|
| Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático. |
| Supuesto General |
| El smishing se utilizó como una nueva modalidad de fraude informático, en razón de que, se emplearon datos personales facilitados por las tecnologías de información y comunicación. Dado que, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Esta modalidad va orientada exclusivamente a obtener de la |

| |
|---|
| víctima información confidencial, mediante enlaces, para luego pasar a un segundo momento y utilizar estos datos. |

***Fuente:*** *Elaboración propia*

En relación con nuestra **cuarta pregunta;** Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Cuya (2023), Padilla (2023), Zevallos (2023) y Bobadilla (2023) indicaron que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Por ello, si hay un procesamiento de datos y transacciones bancarias pero ilícito, correspondiendo evaluar en qué circunstancia o situación nos encontremos, en todo caso la manera de procesar datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos.

A su vez, Solsol (2023) declara que, el smishing se limita a que el agraciado o víctima sea redirigido a un sistema de información (página web, entre otros), la misma que pueda ser un sistema clonado o falso para que posteriormente los ciberdelincuentes con la información recolectada ejecutar sus actividades delictivas.

En referencia a la **quinta pregunta;** a la **quinta pregunta** de la ficha de entrevista; esto es: “por otro lado, ¿considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

Flores (2023), Munayco (2023) y Vallejos (2023), exponen que en cierta forma si hay un procesamiento de datos y transacciones bancarias pero ilícito, corresponde también evaluar en qué circunstancia o situación nos encontremos, en todo caso la manera de procesar estos datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Ante esto, se podría decir que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje.

En ilación con esto, Quispe (2023), Cuya (2023) y Padilla (2023) atisban que, el smishing consiste en pedir a los clientes que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje.

En el mismo sentido, tenemos la **sexta pregunta;** en la que Quispe (2023), Cuya (2023), Padilla (2023) y Flores (2023) exponen que el Estado, las entidades bancarias y las empresas de telecomunicaciones en acción conjunta deberían brindar, realizar y motivar campañas de sensibilización e información concreta, sencilla y accesible para todos los usuarios, de manera que pueda ser de fácil acceso y compresión respecto al uso y restricción de sus datos personales; asimismo, uniformizar e individualizar de manera correcta sus

canales de comunicación, acceso y atención al cliente de manera que frente a mensajes, correos electrónicos y otras modalidades, se encuentren informados de no brindar sus datos personales y finalmente implementar un instrumento o protocolo de adecuada identificación de los usuarios. De igual modo, la solución para esta modalidad de fraude informático del smishing, es la educación y prevención financiera en relación a los mensajes de texto fraudulentos, esta tarea debe ser realizada por las mismas entidades financieras y las autoridades estatales.

Mientras que Vallejos (2023), Zevallos (2023) adoptan una postura más bilateral sobre esta interrogante; consistente en desconfiar de los remitentes desconocidos, no facilitando la información que pide el mensaje de texto, sobre todo si se trata de datos personales o bancos, no abriendo los enlaces que adjuntan y bloqueando el número telefónico en caso de no reconocer el origen (también llamado como SPAM). Asimismo, resulta importante trabajar con herramientas tecnológicas de seguridad cibernética y su difusión, concientizando a las personas a no confiar en ese tipo de información recibida.

En esa misma línea, nos encontramos de acuerdo en el hecho que, que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Muchas veces, el smishing se limita a que el agraciado o víctima sea redirigido a un sistema de información (página web, entre otros), la misma que pueda ser un sistema clonado o falso para que posteriormente los ciberdelincuentes con la información recolectada ejecutar sus actividades delictivas. En tanto, el smishing va orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Ante esto, se podría decir que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un

enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios, en nuestra **ficha de análisis de documentos** del **objetivo específico N° 1,** hemos considerado pertinente, presenta el contenido del **Proyecto de Ley N° 398/2021- CR,** el cual prevé que los **fraudes informáticos** no solamente se expanden por los servicios financieros, sino por diferentes medios perjudicando a los ciudadanos de manera general, esto debido a que, los medios informáticos pueden conectarse por diferentes plataformas, como redes sociales, correos, aplicativos instalados en el celular, entre otros más. Es importante acotar que la pandemia por la COVID-19 no ha sido impedimento para la realización de los **fraudes informáticos** en sus diferentes modalidades más conocidas como el phishing y **smishing**. También hemos visto a bien considerar lo enfatizado en el **Artículo Científico "seguridad por capas frenar ataques de smishing**, se busca prevenir el ataque del smishing mediante la educación en sus diferentes niveles (inicial, primaria y secundaria), asimismo, a nivel empresarial, los proveedores de tarjetas de crédito o débito, deben de encargarse de la capacitación constante de su personal, con la finalidad mejorar la instrucción a los usuarios financieros disminuyendo el número de las posibles víctimas del ataque de smishing, finalmente, otra capa de solución a esta modalidad del fraude informático es la instalación de antivirus efectivos desde que se compra el equipo móvil, en otras palabras que el operador telefónico cumpla con instalar predeterminadamente en sus funciones del móvil el aplicativo antismishing.

En resumen, para acotar a los párrafos precedentes, y manteniendo la postura de nuestros entrevistados, debemos puntualizar nuestro mejor hallazgo del marco teórico, a lo que, Sosa (2022) concluye que las modalidades del **phishing y smishing** es un atentado informático porque cumple con los requisitos de ser un comportamiento que se aprovecha del uso ilícito de tecnología para el acceso de datos informáticos privados y usarlos en afectación al daño patrimonial de los sujetos pasivos del delito. El delito de fraude informático a través de las modalidades "phishing y smishing" no se encuentra expresamente regulado en la Ley N° 30096 a pesar de contar con delito nuclear, el crimen contra la propiedad en la modalidad de fraude informático. Uno de los

análisis que se pudo realizar es la existencia de disposiciones generales en cuanto al delito de suplantación de identidad dejando de lado la verdad material, que, aunque parecidos como el phishing y smishing, que actualmente no gozan de normativa legal adecuada. (p. 65)

En síntesis, a lo que refiere el **objetivo específico N° 1, los entrevistado mencionan que,** en cierta forma si hay un procesamiento de datos y transacciones bancarias pero ilícito, corresponde también evaluar en que circunstancia o situación nos encontremos, en todo caso la manera de procesar estos datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Ante esto, se podría decir que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje.

En tanto, se corroboro el **Supuesto Específico N° 1,** a lo que podemos referir que, el smishing se habría sutilizado como una alternativa o modalidad de fraude informático, en razón de que, se emplearon datos personales facilitados por las tecnologías de la información y comunicación (TICs).

**Tabla N°6 – De la discusión del objetivo específico N°2**

| Objetivo Específico Nº2 |
|---|
| Identificar de que manera se utiliza el phishing para la comisión del delito de fraude informático. |
| Supuesto General |
| La manera más recurrente que se puede advertir, la identificación del phishing como modalidad para la comisión de este hecho delictivo, dado que, el |

| |
|---|
| phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. En la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. |

***Fuente:*** *Elaboración propia*

En relación con **séptima pregunta;** estos son, Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) explayaron que la materialización del phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. Por ende, consideran común esta estafa y comercializando los datos personales de muchos usuarios.

En adición a esto, se tiene lo estipulado por Cuya (2023) y Padilla (2023) al mencionar que, el phishing de manera similar que el smishing, se materializa mediante un medio electrónico. En el caso del phishing es un correo electrónico - de los casos más comunes que he tomado información – el emisor del phishing se hace pasar por una entidad financiera enviando publicidad o alguna información referente a su cuenta bancaria de la víctima, es aquí, cuando el consumidor cae en el anzuelo compartiendo sus datos personales sensibles y logrando darles un beneficio a los ciberdelincuentes.

Por otro lado, en la **octava pregunta;** Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) coinciden que, en la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. No obstante, algunos autores expresan su progreso mediante el equipo de fiscales y peritos informáticos para indagar y articular de forma correcta la investigación de estos delitos.

Por otro lado, se tiene las posturas de Padilla (2023) y Cuya (2023) quienes denotan que, el Ministerio Publico no cuenta con instrumentos o programas tecnológicos para erradicar las modalidades de fraude informático. Considerando que el Ministerio Publico debería tener apoyo de otras autoridades como el INDECOPI o la División de Delitos Informáticos de la Policía Nacional del Perú. Este último, si cuenta con los instrumentos tecnológicos para combatir estos delitos cibernéticos.

En tanto, respecto de la **novena pregunta;** Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) examinan que para evitar este tipo de situaciones, los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos.

De igual manera, Padilla (2023) y Cuya (2023) decretan que, la alternativa de solución, para erradicar el phishing es la creación de programas que puedan detectar correos falsos que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que el programa de mensajería instantánea consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace. De la misma forma que el smishing, las entidades financieras y otras autoridades públicas deben capacitar a la ciudadanía para evitar ser víctima de estos fraudes informativos.

Para finalizar, es menester afirmar nuestra conformidad con lo referido por los especialistas; debido a que, La materialización del phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. En la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. No obstante, algunos autores expresan su

progreso mediante el equipo de fiscales y peritos informáticos para indagar y articular de forma correcta la investigación de estos delitos. Los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos. La alternativa de solución, para erradicar el phishing es la creación de programas que puedan detectar correos falsos que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que el programa de mensajería instantánea consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace. De la misma forma que el smishing, las entidades financieras y otras autoridades públicas deben capacitar a la ciudadanía para evitar ser víctima de estos fraudes informáticos. Aunado a ello, nuestra **ficha de análisis de documentos** del **objetivo específico N° 2,** recalca, la **SENTENCIA P.A.M.** de 12 de marzo de 2018 refiere que, la comisión del delito de **fraude informáticos, por medio de phishing** usualmente se realiza a través del que ordena algún pedido online no es el titular de la cuenta) es un riesgo a cargo del banco. Asimismo, la **Sentencia A.P. Burgos** de 03 de marzo del 2016**,** sostiene que, el fraude informático a través del phishing no requiere una estructura propia de esta modalidad, por eso es que, cuando se cometa este tipo de fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que la información que se podría obtener nos podría indicar como se ha realizado el phishing.

Posteriormente, para realzar lo antes referido, es pertinente, útil y conducente, presentar nuestro hallazgo del **objetivo específico N°2**; por lo que, usualmente se realiza a través del que ordena algún pedido online no es el titular de la cuenta) es un riesgo a cargo del banco. Asimismo, la **Sentencia A.P. Burgos** de 03 de marzo del 2016**,** sostiene que, el fraude informático a través del phishing no requiere una estructura propia de esta modalidad, por eso es que, cuando se cometa este tipo de fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que

la información que se podría obtener nos podría indicar como se ha realizado el phishing.

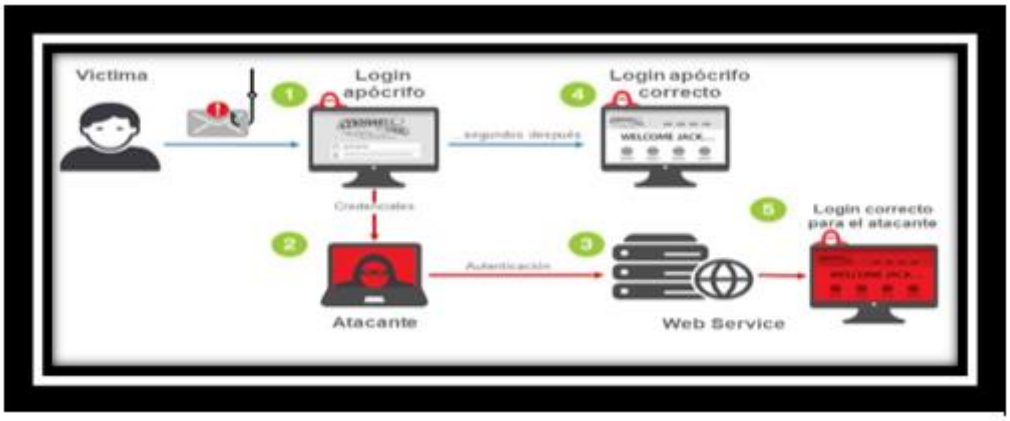
Ahora bien, allanándonos a lo indicado previamente, es necesario exponer nuestro hallazgo referido al **objetivo específico N°2**; respecto de la tesis de García (2018) lo define como una modalidad de fraude informático para obtener información confidencial siendo que la entidad financiera corresponde extender distintas acciones para prevenir la hurto de los datos personales de contenido económico del ordenador, como por ejemplo dar aviso inmediato que no se facilite información sensible en respuesta a correos electrónicos ni tampoco utilizar enlaces integrados en un email o acceder a páginas fraudulentas de terceros, advirtiendo a las oleadas de phishing y sobre todo implementar instrumentos que bloqueen las transferencias cuando puedan existir indicios de que las mismas puedan haberse realizado de forma fraudulenta.

Finalmente, debemos advertir respecto de los dispuesto en el **objetivo específico N°2** de la presente tesis, en síntesis, para prever o reducir la ejecución de estas modalidades de phishing en el fraude informático, los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos.

Por otro lado, corroboramos el **supuesto especifico N°2,** es decir que, El phishing permitió la captación de datos personales para la comisión del delito informático obteniendo datos, para la configuración del delito contra el patrimonio en la modalidad de fraude informático.

Para finalizar y enfocados en nuestro **objetivo específico N°2**, se plantea el siguiente gráfico.

**Figura N° 2 –** *Gráfico que enseña la manera de utilización del phishing para la comisión del delito de fraude informático.*




***Fuente:*** *Computer security.*

## V. CONCLUSIONES

**Primera. –** Respecto al análisis respecto de, el uso de los datos personales en las nuevas modalidades de fraude informático, se emplean en el perfilamiento de las potenciales víctimas, a fin de poder ejecutar desde una suplantación de identidad, debiendo de tomar en de antemano considerando que, una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las tecnologías de información y comunicación, como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada. En la mayoría casos sobre fraude informático, para ingresar al sistema informático se utiliza información confidencial proporcionada por malos elementos de las entidades. El incremento del uso constante de las redes sociales y las tecnologías de la información y comunicación, vulneran los datos personales.

**Segunda. –** Se determinó que, los ciberdelincuentes obtienen información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, si hay un procesamiento de datos y transacciones bancarias pero ilícito, correspondiendo evaluar en qué circunstancia o situación nos encontremos, en todo caso la manera de procesar datos seria cuando la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o clonada y al ingresar información personal o confidencial esta información es procesada, pero también hay smishing orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Asimismo, el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de, un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios. Va orientado exclusivamente a obtener de las víctimas información confidencial de usuarios, perjudicando a los ciudadanos de

manera general, esto debido a que, los medios informáticos pueden conectarse por diferentes plataformas, como redes sociales, correos, aplicativos instaladas en el celular, entre otros más. Es un atentado informático porque cumple con los requisitos de ser un comportamiento que se aprovecha del uso ilícito de tecnología para el acceso de datos informáticos privados y usarlos en afectación al daño patrimonial de los sujetos pasivos del delito.

**Tercera. –** Se ha identificado que el phishing es la creación de programas que puedan detectar correos falsos, que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que, el programa de mensajería instantánea consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace. La materialización del phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. La comisión del delito de fraude informáticos, por medio de phishing usualmente se realiza a través del que ordena algún pedido online no es el titular de la cuenta. El fraude informático a través del phishing no requiere una estructura propia de esta modalidad, por eso es que, cuando se cometa este tipo de fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que la información que se podría obtener nos podría indicar como se ha realizado el phishing.

## VI. RECOMENDACIONES

**Primera. –** Al ministro del Ministerio de Justicia y Derechos Humanos, que disponga la implementación de una Comisión en Delitos Cibernéticos y Datos Personales, la cual tendrá como objetivo principal, la lucha contra la obtención fraudulenta de los datos personales, de manera que los ciberdelincuentes tendrán una barrera adicional al momento de emplear y manipular los datos personales de sus víctimas. Estas barreras de protección deben ser inquebrantables y aplicadas para todo tipo de transacción financiera o bancaria. No obstante, desde nuestra óptica, estamos convencidos de que, si las entidades bancarias o las autoridades competentes para preservar los datos personales a buen recaudo, no se presentaría la cantidad insostenible de casos respecto de este delito.

**Segunda. –** Establecer un protocolo de seguridad, así como, la educación y prevención financiera en relación a los mensajes de texto fraudulentos, esta tarea debe ser realizada por las mismas entidades financieras, las autoridades estatales, las universidades, los colegios públicos y privados. Por otra parte, es necesario tener en cuenta que el smishing es un fraude informático que se materializa mediante los mensajes de texto, por lo que, recomendamos, que las empresas de telecomunicaciones deben de incluir un sistema de protección de datos personales en todos sus dispositivos telefónicos.

**Tercera. –** Implementar instrumentos o programas tecnológicos al Ministerio Publico, debido a que, no cuentan con sistemas altamente especializados para la lucha y erradicación de las nuevas modalidades de fraude informático dentro del territorio nacional. De igual manera, el phishing al ser una modalidad de fraude informático recurrente en nuestra sociedad, lo ideal es que las autoridades del estado incentiven constantemente la correcta cultura informática preventiva en todos los usuarios a nivel nacional.

## REFERENCIAS


Álvarez, A. (2020). Clasificación de las investigaciones. Universidad de Lima, Facultad de Ciencias Empresariales y Económicas, Carrera de Negocios Internacionales. URL: https://hdl.handle.net/20.500.12724/10818

Arias, J.L. Covinos, M. (2021), Diseño y metodología de la investigación. Ed. Enfoques Consulting EIRL DOI: https://doi.org/10.24142/rvc.n22a3

Alcivar, C, Blanc, G y Calderón, J. (2018) Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Benussi, C. (2020) Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes. http://dx.doi.org/10.5354/0719-2584.2020.56660

Bernal, M. (2019) Protocolo para la prevención de ataques de phishing. Revista ReDTiS. Vol. 3 Núm. 3. Recuperado de: URL: https://www.redtis.org/index.php/Redtis/article/view/34

Condori, P. (2020) Niveles de Investigación. Curso Taller. Recuperado de: URL: https://www.aacademica.org/cporfirio/17

Cornejo, M (2018) Principios de Seguridad Informática en Sistemas de Información. Recuperado de: URL: https://repository.uaeh.edu.mx/revistas/index.php/xikua/article/view/1309/4474

De la Rosa, P. (2021) Lack of security of the personal Information in Educational Digital Applications. Revista Iberoamericana para la Investigación y el Desarrollo Educativo (RIDE). (English Edition DOI: https: doi.org/10.23913/ride.v12i23.980

Fuentes, K (2021) Modificación de la ley N° 30096 para incorporar los delitos de phishing, vishing y carding como delitos penalizados con prisión, para

reducir la ciberdelincuencia, Lima 2019. https://hdl.handle.net/20.500.12802/8345

García, D. E., (2018) Phishing a crime of computer fraud. Comment on SAP Valencia 37/2017 of January 25 (REC, 2402/2016). (English Edition). Rev. Boliv. de Derecho, ISSN: 2070-8157 Num. 25 Recuperado de: www.scielo.org.bo/scielo.php?pid=S207081572018000100025&script=sci_abstract&tlng=pt

García, R. (2021). Definición del término Smishing. Recuperado de: URL: https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/

Gómez, L (2018) "El uso indebido de datos personales por entidades privadas y la afectación de derechos fundamentales" URL: https://hdl.handle.net/11537/31508

Guillen, C & Sáenz, F., J., (2021) the scientific rigour in research. Some issues from the area of language and literature Teaching. El Guiniguada [ISSN 0213-0610], N. 30, p. 40-51. URL: http://hdl.handle.net/10553/110254

Gutiérrez, F., Almenarez, F., y Calderón, L., (2021) Security perspective of wireless sensor networks. Revista UIS Ingenierías Vol 20. (English Edition) Página de la revista: https://revistas.uis.edu.co/index.php/revistauisingenierias

Haza, A., & Huiza, B., & Rosales, M. (2018). Ni dejar hacer ni dejar pasar: el compromiso de las instituciones bancarias peruanas frente al lavado de activos a través de la implementación de una metodología por riesgo. Derecho PUCP, (80). DOI: https://doi.org/10.18800/derechopucp.201801.008

Hernández, S., Duana, A. (2020). Técnicas e instrumentos de recolección de datos. Boletín científico de las ciencias económicas Administrativas del ICEA. DOI: https://doi.org/10.29057/icea.v9i17.6019

Hernán, E. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. Revista Científica General José María Córdova, Vol. 20 (37), 208-224. DOI: https://doi.org/10.21830/19006586.791

Lencia, V. (s, f). Revisión documental en el proceso de investigación. Universidad tecnológica de Pereira. Recuperado de https://univirtual.utp.edu.co/pandora/recursos/1000/1771/1771.pdf

Illota Hurtado, O. (2019) How artificial intelligence alters landscape of securities. (English Edition) Revista Conjeturas Sociológicas, Núm. 19. URL: http://portal.amelica.org/ameli/jatsRepo/182/182865020/ index.html

Kadobayashi,Y. (2018) UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App. DOI:10.1109/AsiaJCIS.2017.19

Landa, C. (2021) Constitución, Derechos Fundamentales, Inteligencia Artificial y Algoritmos. THEMIS Revista de Derecho. DOI: https://doi.org/10.18800/themis.202101.002

López, B. (2018) “El delito de fraude cometido a través de las redes sociales: problemas de investigación y enjuiciamiento” DOI https://doi.org/10.7238/idp.v0i27.3150

Machado, Y. (2021) El estado de flujos de efectivo, y sus técnicas de análisis e interpretación como una herramienta financiera en la toma de decisiones para las grandes empresas del sector industrial. URL: https://ri.ues.edu.sv/id/eprint/10996/1/G%20983e.pdf

Mayer, L. (2020) El delito de fraude informático: Concepto y delimitación. Revista chilena de Derecho y Tecnología. Vol. 9. DOI: http://dx.doi.org/10.5354/0719-2584.2020.53447

Margarita, A. (2019). La protección de los Datos Personales en el entorno digital. Los estándares de protección de datos en los países Iberoamericanos. Quaestio Iuris. Vol. 12. Rio de Janeiro. DOI: 10.12957/rqi.2019.40175

Martínez, C. (2018) ¿Por qué debemos proteger los datos personales? Revista el Mundo del Abogado (Número 227). Recuperado de 133 https://2019.vlex.com/#/search/content_type:4/datos+personales/p7/WW/vid/704660765

Mendoza, O., (2018) Protection of personal Data in Companies Established in Mexico. Revista IUS Revista del Instituto de Ciencias Jurídicas de Puebla, México. Vol. 12 N.º 41. URL: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870214720 18000100267

Miro, F. & Contreras, R. (2022) Ciberdelitos, análisis en el sistema penal. Editorial Iustitia S.A.C. Lima, Perú.

Momberg, R. y Morales, M. Contractual terms on the use and processing of personal data and article 16 g) of the Chilean Protection Consumer Act (Law 19,496). (English Edition). Rev. chil. Derecho tecnol. Vol 8. DOI: http://dx.doi.org/10.5354/0719-2584.2019.54441

Moncada, A., (2020). Comparación de técnicas de Machine Learning para detección de sitios web de phishing. Revistas U Lima. DOI: https://doi.org/10.26439/interfases2020.n013.4886

Montoya, D. J., Arias, J. C., Ávila, A., (2022) Análisis del estado actual de la seguridad informática en tiempos de pandemia, entregando un conjunto de buenas prácticas, para fomentar la seguridad informática en las organizaciones de la ciudad de Medellín. Revista CIES-ISSN-e 2216-0167. Vol. 13. Núm. 13. Recuperado de: revista.escolme.edu.co/index.php/cies/article/views/384/466

Moreno. D (2018) Tipos de mecanismos para la protección de los servicios informáticos y sus modelos de seguridad. URL: http://repository.unipiloto.edu.co/handle/20.500.12277/4928

Muñoz, L., Diaz, E., & Gallego, S. the responsibilities arisiting from the use of information and communication technologies in health professional

practice. Anales de Pediatría (English Edition), Vol 92, Issue 5. DOI: https://doi.org/10.1016/j.anpedi.2020.03.003

Mushtaque, K. & Ahsan, K. & Umer, Ahmer (2018) Digital Forensic Investigation Models: An Evolution Study. Revista de Gestão da Tecnologia e Sistemas de Informação. DOI: https://doi.org/10.4301/S1807-17752015000200003

Niño, D. (2022) Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico en: Revista CES Derecho. DOI: https://dx.doi.org/ 10.21615/cesder.6386

Olivos, M. (2020) El derecho a la protección de los datos personales en el Perú: 27 años en su incorporación en la Constitución Política del Perú 1993. DOI: https://doi.org/10.35383/ius-usat.v9i1.338

Ollmann, G. (2018) The Phishing Guide: Understanding and Preventing Phishing (English Edition). URL: http://www.technicalinfo.net/papers/Phishing.html

Orellana, C (2017) De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. Revista de Derecho Foro: La protección de los datos personales en la era digital. URL: https://revistas.uasb.edu.ec/index.php/foro/issue/view/57

Oñate, E. (2019). Internet and the importance of a control body for the protection of personal data. Rumbos TS. (English Edition) Un Espacio Crítico Para La Reflexión En Ciencias Sociales, (20), 189-206. Recuperado a partir de: https://revistafacso.ucentral.cl/index.php/rumbos/article/view/358

Oxman, N. (2018) Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing”. DOI: http://dx.doi.org/10.4067/S0718-68512013000200007

Polo, A. (2018) El derecho de datos personales y su reflejo en el consentimiento del interesado. UNED. Revista Derecho Político. DOI: https://doi.org/10.5944/rdp.108.2020.27998

Platero, A. (2019) La seguridad como elemento clave en el tratamiento de datos personales en Europa: especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad. DOI: http://dx.doi.org/10.21503/lex.v17i23.1670

Riande, N. (2021) Noticia de una ficción jurídica: La protección de los datos personales. URL: https://www.tfja.gob.mx/investigaciones/pdf/r_31-trabajo-3.pdf

Rosero, L. (2021) El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático. http://dspace.ups.edu.ec/handle/123456789/21699

Rodríguez, C. (2018) Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos legales y el proceso para propuesta de ley. https://repositorio.uisek.edu.ec/handle/123456789/3220

Troncoso, A. (2018) Del principio de seguridad de los datos al derecho a la seguridad digital. https://dialnet.unirioja.es/servlet/articulo?codigo=6815107

Torres, M. K., & Salazar, F. G. (2019). Métodos de recolección de datos para una investigación. Recuperado de: URL: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/2817

Peñarete, J. (2020) La normatividad en el tratamiento de los datos sensibles de la historia clínica, en el ejercicio del derecho del Habeas Data en Colombia. URL: http://hdl.handle.net/10654/35812

Ping, Y. (2018) Web Phishing Detection Using a Deep Learning Framework. Research Article, Open Access. Vol. 2018. DOI: https://doi.org/10.1155/2018/4678746

Piza Burgos, N. D., Amaiquema Marquez, F. A., & Beltrán Baquerizo, G. (2019). Métodos y técnicas en la investigación cualitativa. Algunas precisiones

necesarias. Revista Conrado, 15(70), 455-459. Recuperado de http://conrado.ucf. edu.cu/index.php/Conrado

Ventura, M. (2021) La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020. Repositorio de la Universidad Privada del Norte. URL: https://hdl.handle.net/11537/28942

Velandia, G., & Escobar A. (2018) Investigation in forensic audit: Review of SCOPUS publications 1976 – 2018. (English Edition). Revista Criminalidad, 61 (3): 279-298. URL: Investigación en auditoría forense: Revisión de publicaciones SCOPUS 1976-2018 (scielo.org.co)

Vinelli, R., (2021) Los Delitos Informáticos y su Relación con la Criminalidad Económica. Ius et Praxis de la Facultad de Derecho Núm. 53, ISSN-6296. DOI: https://doi.org/10.26439/iusetpraxis2021.n053.4995

Villegas, J (2021) Modelo de machine learning en la detección de sitios web phishing. URL: https://hdl.handle.net/20.500.12802/8897

Useche, M. C., Artigas, W., Queipo B. & Perozo, E. (2019). Técnicas e instrumentos de recolección de datos cuali-cuantitativos. Ed. Gente Nueva, Universidad de la Guajira Primera Edición. ISBN: 978-959-6037-04-0 URL: https://repositoryinst.uniguajira.edu.co/handle/uniguajira/467

Weider D, Shruti, N. Nagapriya, T. "A phishing vulnerability analysis of web based systems," IEEE Symposium on Computers and Communications, 2008, pp. 326-331, DOI: 10.1109/ISCC.2008.4625681

Zaragoza, A (2019) Proyecto de robo de datos y fraude a través de canales digitales.URL:https://pplaft.cnbs.gob.hn/wpcontent/uploads/2021/04/Informe-de-proyecto-Robo-de-datos-y-Fraude-a-traves-de-Canales-Digitales.pdf

**ANEXO N° 01**

**MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA**

FACULTAD DE DERECHO Y HUMANIDADES

**ESCUELA:** Escuela Profesional de Derecho

**NOMBRE DE LOS ESTUDIANTES:**

- Kleyder Maycot, Burga Carrero
- Gerardo Alexis, Morales Padilla

**ESCUELA:** Escuela Profesional de Derecho

**ÁMBITO TEMÁTICO:** ESTUDIO DE LOS DELITOS CIBERNÉTICOS Y SU MODALIDAD

| **TÍTULO** | |
|---|---|
| Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022. | |
| **PROBLEMAS** | |
| **Problema General** | ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático? |
| **Problema Específico 1** | ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático? |
| **Problema Específico 2** | ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático? |
| **OBJETIVOS** | |
| **Objetivo General** | Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático. |
| **Objetivo Específico 1** | Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático. |
| **Objetivo Específico 2** | Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático. |

| SUPUESTOS | |
|---|---|
| **Supuesto General** | Los datos personales fueron empleados para la comisión de delitos cibernético se ejecuta, a fin de obtener un lucro patrimonial tomando en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. Los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. En ese sentido, las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático. |
| **Supuesto Específico 1** | El smishing se utilizó como una nueva modalidad de fraude informático, en razón de que, se emplearon datos personales facilitados por las tecnologías de información y comunicación. Dado que, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Esta modalidad va orientada exclusivamente a obtener de la víctima información confidencial, mediante enlaces, para luego pasar a un segundo momento y utilizar estos datos. |
| **Supuesto Específico 2** | La manera más recurrente que se puede advertir, la identificación del phishing como modalidad para la comisión de este hecho delictivo, dado que, el phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. En la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la investigación de delitos de fraude |

| | |
|---|---|
| | informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. |
| **Categorización** | **Categoría 1: Uso de los datos personales**<br>Subcategoría 1: Datos sensibles<br>Subcategoría 2: Recolección de datos<br>**Categoría 2: Fraude Informático**<br>Subcategoría 1: Smishing<br>Subcategoría 2: Phishing |
| **METODOLOGÍA** | |
| **Tipos, diseño y nivel de investigación** | **Enfoque:** Cualitativo<br>**Diseño:** Teoría Fundamentada<br>**Tipo de investigación**: Básica<br>**Nivel de la investigación:** Descriptivo |
| **Muestreo** | **Escenario de estudio:** Lima Centro.<br>**Participantes: Participantes:** Tres Fiscales Provinciales Adjuntas de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Una Fiscal Provincial Titular de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro Una fiscal provincial de la Fiscalía Corporativa, Un Fiscal Superior Titular de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro Especializada en Ciberdelincuencia de Lima Centro.<br>**Muestra:** no probabilística<br>**Muestra:** no probabilística – **Tipo:** De experto.<br>**Muestra Orientada:** Por conveniencia |
| **Técnica e instrumento de recolección de datos** | **Técnica:** Entrevista y análisis de documentos<br>**Instrumento:** Guía de entrevista y ficha de análisis de documentos (sentencias, casaciones) |

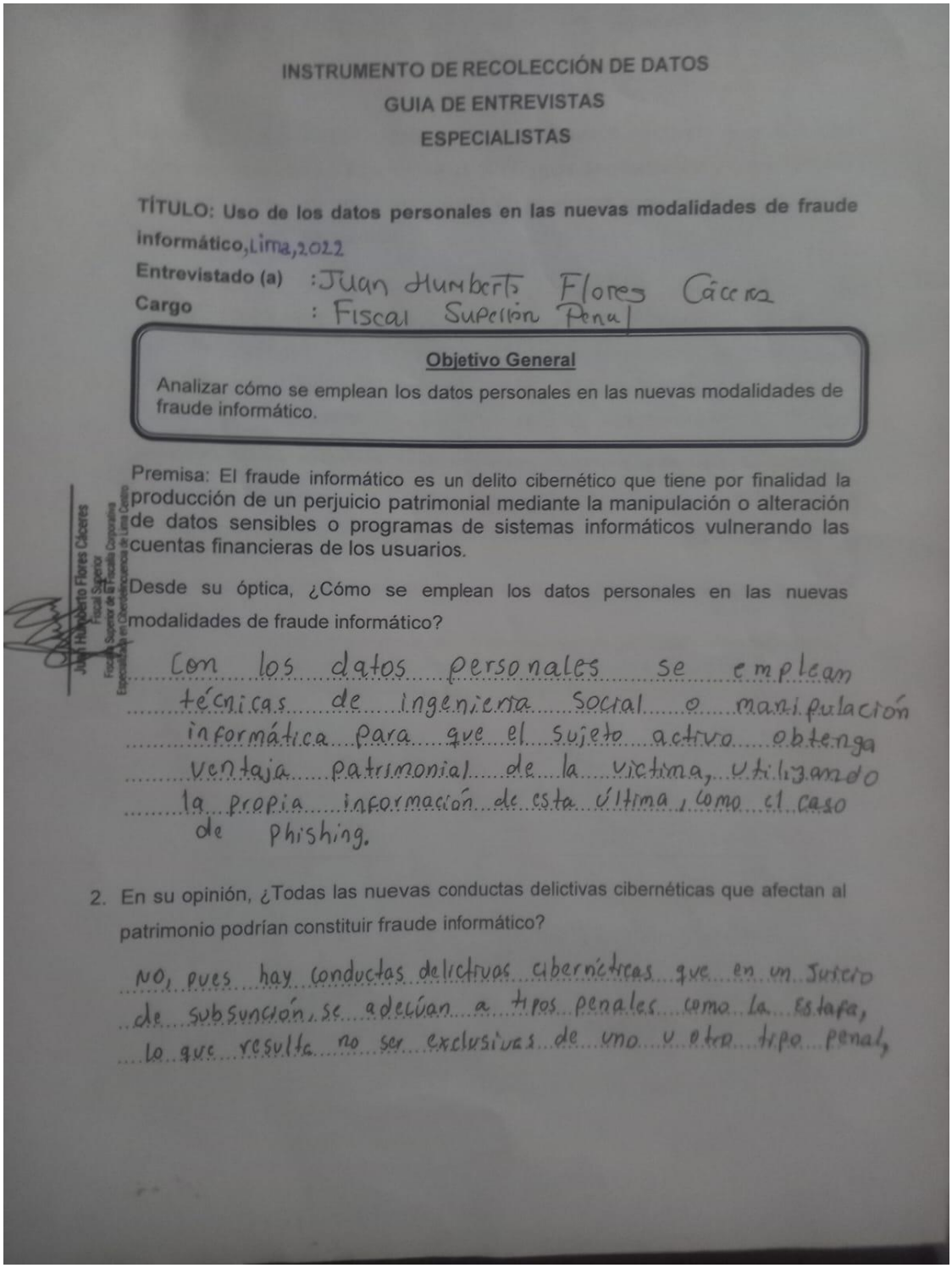
| | |
|---|---|
| **Método de análisis de documentos** | Hermenéutico, analítico, inductivo y comparativo. |

**ANEXO N° 2**

**INSTRUMENTO DE RECOLECCION DE DATOS**

**GUIA DE ENTREVISTAS**

**ESPECIALISTAS**



INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTAS

ESPECIALISTAS

TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022

Entrevistado (a) : Juan Humberto Flores Cáceres

Cargo : Fiscal Superior Penal

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

Juan Humberto Flores Cáceres
Fiscal Superior
Fiscalía Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

Con los datos personales se emplean técnicas de ingeniería social o manipulación informática para que el sujeto activo obtenga ventaja patrimonial de la victima, utilizando la propia información de esta última, como el caso de Phishing.

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

No, pues hay conductas delictivas cibernéticas que en un Juicio de subsunción, se adecúan a tipos penales como la Estafa, lo que resulta no ser exclusivas de uno u otro tipo penal,

debiendo valorarse al caso en concreto.

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

Si, pues tiene su propia estructura normativa que se distingue propiamente de otras figuras que afectan al patrimonio; así, al tenerse la utilización de las TIC's, precisa de una manipulación o argot informático que no aparece en los componentes normativos de la estafa.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Juan Humberto Flores Cáceres
Fiscal Superior
Fiscalía Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

Es una modalidad derivada del Phishing, o de los diversas formas de manipulación informática, que mediante técnicas de ingeniería social, ... obtienen los datos personales - bancarios - de la víctima, para obtener ventajas patrimoniales.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

si, porque partimos de la premisa base sobre el contenido genérico del fraude informático, por medio del cual se utiliza una manipulación informatica para el procesamiento de operaciones bancarias o que el procesamiento de los terminales no cumplen su propósito, precisamente por esa acción desplegada por el sujeto activo.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Medidas de prevención coordinadas con las entidades bancarias, y las vinculadas a ésta, como los proveedores de servicios donde llegan estos mensajes, para que los clientes no sólo expongan un mayor conocimiento sobre estas prácticas, sino además, interioricen cuando se esté frente a estas conductas.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Juan Humberto Flores Cáceres
Fiscal Superior
Fiscalía Superior de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

Exponer la manera como se materializa el phishing, sería un espacio insuficiente para considerar la multiplicidad de aquellas utilizadas por el phisher, pero que bien, las más conocidas o utilizadas se dan en las plataformas como correos electrónicos de la víctima, o páginas webs, suplantando la identidad de bancos.

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

en la actualidad contamos con una fiscalía especializada competente para los delitos previstos en la Ley nº 30096, modificada por la nº 30171, sólo para el distrito fiscal de Lima centro, pero dada la proliferación de estas conductas, se tornan en insuficientes para uniformizar una correcta investigación en todo el país.

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

El abordaje de la investigación es esencial, entendiendo la volatibilidad de las pruebas o evidencia digital, agregando a las medidas preventivas que se debe dar a través de una coordinación interinstitucional como se precisó en párrafos precedentes.

Juan Humberto Flores Cáceres
Fiscal Superior
Fiscalía Superior de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTAS

ESPECIALISTAS

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2023**

**Entrevistado (a)** : Martha Elena Munayco Medina

**Cargo** : Fiscal Provincial Penal

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

Para contestar esta interrogante debemos tener en cuenta que existen muchas modalidades de fraude informático las que de una u otra manera se asemejan a la estafa agravada, es decir existe que mediante las modalidades de phishing, smishing, vishing, etc., se procura capturar datos personales o bancarios del titular de una cuenta bancaria para el subsecuente perjuicio patrimonial, en estos casos la víctima se convierte en un medio o mediante usado para que sea el mismo quien proporcione sus datos personales o de cuenta y a partir de ello realizar el delito de fraude.

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

No necesariamente, en estos tiempos se confunde mucho los delitos informáticos, con los delitos computacionales; en el primer caso el legislador ha querido que hechos se subsuman en la ley 30096; en el segundo caso, los delitos computacionales, están relacionados a todos los supuestos en la que el agente tiene como herramienta de trabajo una computadora, un teléfono o cualquier herramienta tecnológica y de una u otra forma el agente realiza actuaciones en contra de los intereses de la empresa local bien puede ser una estafa, apropiación ilícita, fraude en la administración de personas jurídicas. Tampoco se podría decir que estamos ante un delito informático cuando el agente mediante herramientas tecnológicas utiliza la violencia o amenaza para estorcionar o chantajear a la víctima

MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

No debería ser estrictamente necesario, sin embargo en nuestro vida cotidiana, se dan situaciones en las que se induce a error al sujeto pasivo, así por ejemplo si Juan hace creer que pasa como trabajador de una entidad bancaria realiza llamada a María comunicándole que debe realizar el cambio de su tarjeta por una nueva en la cual se amplia su línea de crédito, para lo cual se amplia su línea de crédito, para la cual se amplia su línea de crédito, para la cual un funcionario PROCEDA a constituirse a su inmueble a recoger la tarjeta llevando todos documento efectivo...

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

El smishing es una de las modalidades más comunes del delito de fraude informático, y generalmente se dan porque las personas reciben un mensaje de texto de una supuesta entidad bancaria para ser beneficiados de algún producto iniciado adjunta un enlace, en donde las personas ingresan acceden al registro información confidencial y reenviado como a los presuntos a bancarios, también cuando la personas un enlace para confirmar determinada operación, también se podría relacionar esta modalidad pesca en los delitos de estafa.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

De cierta forma si hay un procesamiento de datos y transacciones bancarias ilícitas, corresponde también realizar un requerimiento vía situaciones nos encontremos, en todo caso la manera de proceder sobre datos sensibles ante la víctima accede a un enlace y es inmediatamente direccionado a una página web falsa o dañada y al ingresar información personal o confidencial esta información personal o confidencial es interceptada y procesada, para también hacer smishing envía un mensaje de texto al teléfono de la víctima información confidencial mediante enlaces.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

La solución prácticamente es preventiva, realizar campañas de prevención para sensibilizar a las personas para no acceder a enlaces para leer y pasar a una siguiente manito y utilizar el Esperar

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

El phishing; causa modalidad de estafa suplantación, en el cual muchas personas facilm con engaños y entregan información confidencial a personas que usualmente suplantan las identidades de una entidad financiera

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

El Ministerio Público, lamentablemente no posee los instrumentos tecnológicos para combatir el delito de fraude informático ni siquiera los bancos ya que sus sistemas siempre son vulnerados aunque muchas veces por la protección de sus propios trabajadores, el M.P. ni siquiera posee la capacidad tecnológica, logística o humana para procesar estos delitos que día a día siguen incrementándose, ya los delincuentes siempre utilizan tecnología muy avanzada para mantenerse en el anonimato

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

Las alternativas que propongo es realizar campañas de prevención y sensibilizar a los personas para que no accedan a ventanas maliciosas, que no brinden información personal o confidencial en páginas presentadas falsas, que tengan cuidado a ciertos lugares especiales por ejemplo que tengan en cuenta que los bancos cuentan con canales y líneas telefónicas oficiales de atención al ciudadano, no mediante entidades bancarias no realizan llamadas mediante líneas citadas, y lo importante es tipificar estos delitos

MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTAS

ESPECIALISTAS

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.**

**Entrevistado (a)** : Karina Raysa Quispe Alí

**Cargo** : Fiscal Adjunta Provincial Provisional

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial, mediante la manipulación, alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

Conforme a las modalidades de fraude informático: diseño, introducción, supresión, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; se requiere que los ciberdelincuentes obtengan "ex ante" de manera indebida los datos personales o financieros (nombres y apellidos, fecha de nacimiento, números de tarjeta bancaria, números de cuenta bancaria, fecha de vencimiento de la tarjeta, CVV (código valor de validación), entre otros) los mismos que son objeto de uso para concretar el perjuicio a la víctima.

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

En mi opinión, sí constituyen fraude informático, sin embargo, considero que conforme a la globalización y al acceso a la información el delito de fraude

KARINA RAYSA QUISPE ALÍ
FISCAL ADJUNTA
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

informático, constituiría un delito pluriofensivo, afectando no solo el patrimonio, sino también sistemas informáticos, intimidad personal, propiedad intelectual, entre otros bienes jurídicos.

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

Considero que, el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las TICs como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

Bajo mi criterio, el smishing es una modalidad y/o variante del phishing, que consiste en el envío de enlaces maliciosos o perniciosos mediante mensajes de texto remitidos a los equipos móviles (celulares) que tienen como finalidad la de acceder ilícitamente a los datos personales o bancarios de las víctimas con el objeto de causar perjuicio patrimonial o moral.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

KARINA [illegible] QUISPE ALI
FISCAL ADJUNTA
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

Considero que el smishing tiene como principal objeto la obtención de datos financieros, bancarios o personales, los mismos que son utilizados para la concreción de operaciones bancarias indebidas.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Considero que el Estado, las entidades bancarias y las empresas de telecomunicaciones en acción conjunta deberían brindar, realizar y motivar campañas de sensibilización e información concreta, sencilla y accesible para todos los usuarios, de manera que pueda ser de fácil acceso y compresión respecto al uso y restricción de sus datos personales; asimismo, uniformizar e individualizar de manera correcta sus canales de comunicación, acceso y atención al cliente de manera que frente a mensajes, correos electrónicos y otras modalidades, se encuentren informados de no brindar sus datos personales y finalmente implementar un instrumento o protocolo de adecuada identificación de los usuarios. Asimismo, se debe modificar y reformular la regulación y normativa respecto a los datos personales brindados a los trabajadores que laboran en empresas privadas o públicas y que tienen acceso a data sensible y/o personal; aunado a ello, se debería emprender una campaña multiorganizacional de lucha frontal contra el tráfico ilegal de datos que opera en diversos puntos del Perú, a través de los cuales se "vende" o "trafica" con los datos personales.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

KARINA RAYSA QUISPE ALI
FISCAL ADJUNTA
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

Es una modalidad consistente en el envío de "carnadas" o "cebos" mediante mensajes en redes sociales o correos electrónicos, por cuanto, las víctimas al ingresar en estos links remitidos, se recolectan datos de las tarjetas bancarias y de sus respectivos titulares para realizar transferencias de dinero indebidas y no autorizadas.

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

Considero que, el Ministerio Público, consciente de los cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas, ante la necesidad de una lucha efectiva contra la ciberdelincuencia y frente a la realidad delictiva de los delitos informáticos, ha implementado una serie de instrumentos tecnológicos a la Unidad Especializada en Ciberdelincuencia como es la reciente creación del Laboratorio de Ciberdelincuencia y el Área de Peritajes, asimismo, ha reforzado la cooperación con entidades gubernamentales y no gubernamentales a nivel nacional e internacional, a fin de dar una respuesta asertiva frente a las nuevas tendencias de la ciberdelincuencia, sin embargo, al ser la ciberdelincuencia un delito trasnacional, se requiere de una progresiva y mayor implementación de instrumentos tecnológicos que permitan la preservación, conservación e investigación del delito cibernético en consonancia con una adecuada proyección y dación de capital humano para la obtención de dichos fines.

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

El uso adecuado de la información por parte de las entidades bancarias a sus usuarios; la atención especial, preferencial y especializada respecto a cada tipo de usuario y de acuerdo a sus necesidades y conocimientos básicos, para alertar a los mismos al uso de canales digitales o presenciales y a la prevención de acceso a links malintencionados.

KARINA BAYSA QUISPE ALÍ
FISCAL ADJUNTA
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTAS

ESPECIALISTAS

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2013.**

**Entrevistado (a)** : TANIA BOBADILLA CENTURION

**Cargo** : FISCAL ADJUNTA PROVINCIAL TITULAR

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

El delincuente hace uso de herramientas digitales a través de la informática para obtener los datos sensibles sensible de una persona y así utiliza para apropiarse del patrimonio

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

El fraude es un concepto amplio, que no tiene semejanza con el resultado típica, pero todas las conductas delictivas deben constituir el delito del fraude cibernético

Tania S. Bobadilla Centurión
Fiscal Adjunta Provincial Titular
Fiscalía Provincial Corporativa Especializada en
Ciberdelincuencia 4° Despacho

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

Mediante la obtención de datos sensibles de una forma ilegítima, pero que no debe de ser exactamente estrictamente necesario, ya que acorde a cada una de sus modalidades se tiene que ver a través de la consumación y la tentativa.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

Pues al acceder a recepcionar un mensaje el delincuente puede acceder mediante herramientas informáticas a tus datos y apropiarse, haciendo uso de los mismos y generando afectación patrimonial de la víctima.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

Tania S. Robadilla Centurión
Fiscal Adjunta Provincial Titular
Fiscalía Provincial Corporativa Especializada en
Ciberdelincuencia 4° Despacho

Sí considero que otros de las modalidades del smishing se puede recaudar información de las transacciones bancarias por ello su peligrosidad en este tipo de delitos, ya que actualmente, varios personas realizan compras por internet o a través de su tarjeta de crédito en físico transmitido datos de la misma tarjeta.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Con herramientas tecnológicas de seguridad cibernética y sus defensas, concientizando a los personas a no confiar en este tipo de información recibida.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

Se utiliza a través de correos emitidos, enlaces de páginas webs, entre otros mensajes que envían muchos días con las intenciones de la víctima.

Tania S. Bobadilla Centurión
Fiscal Adjunta Provincial Titular
Fiscalía Provincial Corporativa Especializada en Ciberdelincuencia 4° Despacho

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

Los instrumentos que posee el Ministerio Público, especialmente la Fiscalía Especializada en Ciberdelincuencia es remitirse a seguir una ruta informática de buscar el origen personal(es) que difunden este tipo de correos y que se hacen las investigaciones con la policía de investigación.

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

Brindar capacitaciones o charlas sobre la seguridad cibernética, uso correcto de los datos personales, cuidado del phishing y consejos de navegación digitales como Google Meet, zoom, etc.

**Tania S. Bobadilla Centurión**
Fiscal Adjunta Provincial Titular
Fiscalía Provincial Corporativa Especializada en
Ciberdelincuencia 4° Despacho

**INSTRUMENTO DE RECOLECCIÓN DE DATOS**
**GUIA DE ENTREVISTAS**
**ESPECIALISTAS**

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.**

**Entrevistado (a)** : Sigrid Flor Vallejos Ramos

**Cargo** : Fiscal Adjunto Provincial

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

El uso ilegal de los datos personales en las nuevas modalidades de fraude informatico se da mediante la sustracción y manipulación de la información a fin de cometer el ilicito delictivo. Acceso a cuentas del correo electronico, número de tarjetas, redes sociales, tarjetas de debito o credito, el mismo que se manifiesta mediante las siguientes modalidades: clonación de páginas falsas, compra-fraude (sitios falsos ofertas online) etc.

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

No necesariamente, si bien se cumple que el bien jurídico protegido en los delitos de fraude informático es el "patrimonio", este debe cumplir con los elementos constitutivos; sujeto activo genérico, sujeto pasivo genérico, que el sujeto activo implemente una conducta "engañosa" que "induzca al error" a la victima y orientado a la obtención de un beneficio económico.

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

Pienso que el delito de fraude informático se trata de un tipo de resultado material, que se consuma cuando el agente (sujeto activo), motivado por su ánimo lucrativo, afecta los datos informáticos o el programa de un sistema informático de forma; en tal sentido, se admite la tentativa (mediante el empleo de la conducta engañosa que induzca al error), así como la coautoría y la participación delictiva.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

El daño ocasionado a través del smishing es la obtención de datos privados o confidenciales de un cliente suplantado la identidad de una empresa para cometer fraudes, robos y otros delitos informáticos.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

Es, cuando el smishing consiste en pedir a los clientes, usuarios, que confirmen transacciones, de pequeñas deudas, a través de unos enlaces que aparecen en el mensaje de texto. De esta manera, los ciberdelincuentes roban la información confidencial, como credenciales de acceso a cuentas o datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Descartar de inmediato los mensajes desconocidos, no facilitar los datos personales que pide el mensaje, sobre todo si se trata de datos personales o bancarios, no abrir los enlaces que adjuntan, bloquear el número telefónico en caso de no reconocer el origen. También llamarles correo SPAM).

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

El phishing es una modalidad de fraude muy común, en la cual muchas personas fácilmente son captadas y entregan información confidencial a personas que usualmente suplantan la identidad de una entidad financiera o empresarial, luego del cual esta información es procesada, utilizada en un segundo momento para recibir disposiciones patrimoniales de una determinada cuenta.

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTAS
ESPECIALISTAS

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.**

**Entrevistado (a)** : Mauro Zevallos Morales

**Cargo** : Especialista en T.I. para ciberdelincuencia

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

Se emplean con el propósito de validar la identidad de una persona/entidad ante una plataforma tecnológica con el fin de obtener un bien económico y/o la obtención de información

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

no necesariamente, algunas solo califican como fraude.

MAURO NESTOR ZEVALLOS MORALES
Especialista en Tecnologías de la Información
Unidad Fiscal Especializada en
Ciberdelincuencia del Ministerio Público

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

Considero que se puede consumar al inducir a error, en cuyo caso se hace más compleja la obtención de evidencia digital que acredite la atribución de los actos ilícitos.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

El smishing se utiliza como el medio de envío de mensajes el cual contendrá un enlace o link fraudulento que induzca al usuario a ingresar sus credenciales y/o datos personales, y/o sensibles

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

MAURO NESTOR ZEVALLOS MORALES
Especialista en Tecnologías de la Informar
Unidad Fiscal Especializada en
Ciberdelincuencia del Ministerio Público

el acceso de datos y transacciones bancarias usuan a ser utilizados posterior de la obtención de los datos del smishing recogida, el smishing básicamente sería la obtención de dichos datos, mas en el procedimiento

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

mentalizar la capacidad del usuario objetivo de identificar a través de un ataque de este tipo e informar a las empresas de telecomunicaciones al respecto a fin de poner en una lista negra a los mismos

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

En su mayoría a través del ingreso a enlaces fraudulentos que recopilan datos sensibles

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

MAURO NESTOR ZEVALLOS MORALES
Especialista en Tecnologías de la Información
Unidad Fiscal Especializada en
Ciberdelincuencia del Ministerio Público

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

la implementación de sistemas de detección de amenazas que de enlaces maliciosos así como un análisis de archivos adjuntos que puedan ser infectados y/o se consideren como un vector de ataque

MAURO NESTOR ZEVALLOS MORALES
Especialista en Tecnologías de la Información
Unidad Fiscal Especializada en
Ciberdelincuencia del Ministerio Público

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTAS
ESPECIALISTAS

**TÍTULO: Uso de los datos personales en las nuevas modalidades de fraude informático,** Lima, 2022

**Entrevistado (a)** : Irving Lyonel Solsol Vilca

**Cargo** : Especialista en T.I. Para Ciberdelincuencia

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

Premisa: El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?

Se emplean en el Perfilamiento de los Potenciales Victimas a fin de Poder ejecutar desde una suplantacion de identidad, fraude, extorción, entre otros, hasta la comercializacion de los mismos.

2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?

NO, Los ciberdelincuentes en muchos ataques informáticos que tienen propósitos afectar el funcionamiento de Redes de comunicaciones y/o Sistemas informáticos, terminan obteniendo información bancaria

sancionable y que posteriormente termina cometiendose fraudes de personas jurídicas o personas naturales.

3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?

No tengo los conocimientos jurídicos para dar una respuesta.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

Premisa: El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa.

4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?

El phishing tiene por objetivo recolectar información a partir de técnicas de clonación de sistemas, entre otros. En particular, el Smishing es un ataque similar al anterior solo que operatividad se limita a los mensajes de texto para lo cual se camuflan con herramientas para que la victima crea que el mensaje es autentico, según el contexto.

5. Por otro lado, ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?

No, el contenido de un smishing se limita a que el agraviado o víctima sea redirigido a un sistema de información (Página Web, entre otras), la misma que puede ser un sistema clonado o falsa, para que posteriormente los ciberdelincuentes con la información recolectada ejecuten sus actividades delictivas.

6. Según su percepción sobre esta temática, ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?

Que la ciudadanía obtenga o se capacite en temas de fraudes informáticos a nivel de usuario como mínimo.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

Premisa: El phishing se encuentra diseñado con la finalidad de sustraer los datos del usuario obteniendo información privada, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito).

7. Desde su experiencia, ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?

Utilizando los datos recolectados (credenciales de accesos, información bancaria, entre otro) para poder acceder a los sistemas ya sea Paginas wpl o Paginas web financieros y en algunos casos comercializar la información recolectada de muchos usuarios.

8. De acuerdo a su criterio, ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?

Si, el ministerio Publico a traves de sus fiscalias especializadas en especial la de Ciberdelincuencia, junto a sus equipo de Peritos informaticos y Especialista en T.I, tiene la capacidad y los herramientos para investigar estos tipos de delitos.

9. Desde expertise, ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?

Que se desarrolle material que permita la concientizacion sobre esta modalidad de ataque informatico, asi mismo desarrollar estrategias para la adopcion de la cultura en la Poblacion sobre el Conocimiento basico en Seguridad informática.

IRVING LYONEL SOLSOL VILCA
Especialista en Tecnologías de la Información
Unidad Fiscal Especializada en
Ciberdelincuencia del Ministerio Público

**INSTRUMENTO DE RECOLECCION DE DATOS**

**GUIA DE ENTREVISTAS**

**ESPECIALISTAS**

**TÍTULO:** Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.

**Entrevista:** Padilla Virhuez, Meri Liliana

**Cargo:** Socia Principal - Abogada Penalista

**Institución:** Padilla Abogados & Consultores

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

**Premisa:** El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

**1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?**

Los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. Una vez obtenida, esta será usada para fines delictivos como es el delito de phishing.

**2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?**

En mi opinión, si, debido a que el medio de realización de los delitos es mediante plataformas digitales.

**3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?**

Si, jurídicamente, considero necesario que el fraude informático se tenga que configurar mediante la tecnología, ya que, sin los datos personales de la víctima, no podría cometer su perjuicio patrimonial.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

**Premisa:** El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa".

**4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?**

El smishing se comete mediante mensajes de texto que conllevan a que el usuario de a pie, ingresar al enlace que se ha enviado con la única finalidad de ingresar a sus cuentas bancarias a fin de cometer un fraude electrónico, vulnerando los mecanismos de seguridad de la entidad financiera del consumidor.

**5. Por otro lado ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de las terminales electrónicas de las entidades financieras?**

Si, considero que el smishing procesa los datos y transacciones, siendo un virus o un programa pirata informático, que busca recopilar datos personales sensibles; ahora bien, una vez obtenidos los datos sensibles, como, por ejemplo: el documento de identidad, número de tarjeta, clave; es aquí cuando el delincuente cibernético procesa las terminales electrónicas de las entidades financieras para validarlos con los datos sensibles obtenidos y generar el fraude informático.

**6. Según su percepción sobre esta temática ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?**

Dentro mi percepción, la solución para evitar esta modalidad de fraude informático, es que la autoridad competente en telecomunicaciones ingrese un proyecto de ley, en el cual todos los móviles u ordenadores instalen un programa que rebota enlaces sospechosos. Asimismo, el programa debería de verificar segundos o minutos antes que el emisor del mensaje, enviando un aviso a la Policía Nacional del Perú.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

**Premisa:** El phishing se encuentra diseñado con la finalidad de robarle la identidad del usuario obteniendo información privada que es usada por medio de engaños, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito)

**7. Desde su experiencia ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?**

El phishing de manera similar que el smishing, se materializa mediante un medio electrónico. En el caso del phishing es un correo electrónico - de los casos más comunes que he tomado información – el emisor del phishing se hace pasar por una entidad financiera enviando publicidad o alguna información referente a su cuenta bancaria de la víctima, es aquí, cuando el consumidor cae en el anzuelo compartiendo sus datos personales sensibles.

**8. De acuerdo a su conocimiento ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?**

De la información actual que manejo, el Ministerio Publico no cuenta con instrumentos o programas tecnológicos para erradicar las modalidades de fraude informático. Considero que el Ministerio Publico tiene apoyo de otras autoridades como el INDECOPI o la División de Delitos Informáticos de la Policía Nacional del Perú.

**9. En su criterio ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?**

Como alternativa de solución (a diferencia de mi propuesta anterior con el smishing), planteo que el phishing al ser una modalidad de fraude informático que se comente mediante otro medio electrónico, siendo los programas de mensajería instantánea como: Hotmail, Gmail, Yahoo!, entre otros, debiendo detectar correos falsos que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que el programa de mensajería instantánea consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace.


**FIRMA Y SELLO**

**INSTRUMENTO DE RECOLECCION DE DATOS**

**GUIA DE ENTREVISTAS**

**ESPECIALISTAS**

**TÍTULO:** Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.

**Entrevista:** Cuya Berrocal, José Miguel

**Cargo:** Fiscal Provincial del 3 Despacho de Crimen Organizado

**Institución:** Ministerio Publico

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

**Premisa:** El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

**1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?**

Se emplean mediante la sustracción de algún equipo electrónico, logrando ingresar a su información importante del usuario para luego extraer su dinero.

**2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?**

En mi opinión, considero que sí, ya que, el patrimonio es la única finalidad de los ciberdelincuentes.

**3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?**

Nunca he escuchado de las tecnologías de información y comunicación, por lo que, me reservo emitir una opinión jurídico.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

**Premisa:** El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa".

**4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?**

El smishing se utiliza mediante el envió de mensaje de texto, ya que, al ser un mensaje fraudulento, el usuario es inducido a error ingresando al enlace, lo que conlleva a compartir sus datos personales.

**5. Por otro lado ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?**

Considero que el smishing procesa más transacciones bancarias que datos, debido a que, en la actualidad la obtención de datos personales sensibles se pueden conseguir en lugares de dudosa procedencia.

**6. Según su percepción sobre esta temática ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?**

La solución para esta modalidad de fraude informático del smishing, es la educación y prevención financiera en relación a los mensajes de texto fraudulentos, esta tarea debe ser realizada por las mismas entidades financieras y las autoridades estatales.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

**Premisa:** El phishing se encuentra diseñado con la finalidad de robarle la identidad del usuario obteniendo información privada que es usada por medio de engaños, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de crédito o débito)

**7. Desde su experiencia ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?**

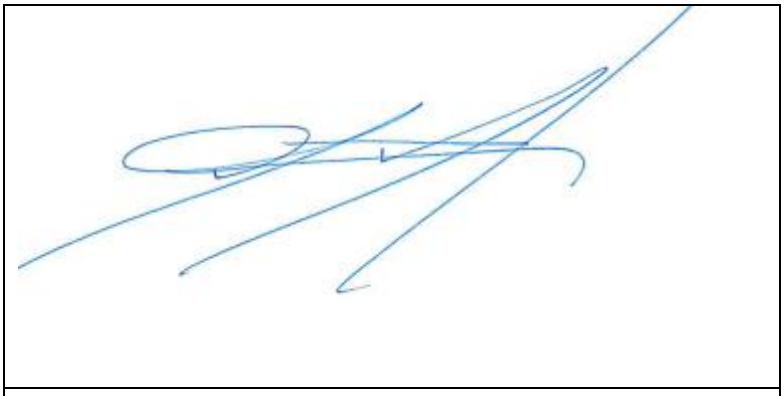
Se utiliza mediante el envió de enlaces engañosos que persuaden al usuario para obtener un supuesto beneficio.

**8. De acuerdo a su conocimiento ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?**

El Ministerio Publico no cuenta con instrumentos tecnológicos para combatir estos delitos cibernéticos, sin embargo, la Policía Nacional del Perú, sí.

**9. En su criterio ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?**

De la misma forma que el smishing, las entidades financieras y otras autoridades públicas deben capacitar a la ciudadanía para evitar ser víctima de estos fraudes informativos.



**FIRMA Y SELLO**

**INSTRUMENTO DE RECOLECCION DE DATOS**

**GUIA DE ENTREVISTAS**

**ESPECIALISTAS**

**TÍTULO:** Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.

**Entrevista:** Bobadilla Centurión, Tania

**Cargo:** Fiscal Adjunta Provincial Titular

**Institución:** Ministerio Publico

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

**Premisa:** El fraude informático es un delito cibernético que tiene por finalidad la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos sensibles o programas de sistemas informáticos vulnerando las cuentas financieras de los usuarios.

**1. Desde su óptica, ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático?**

El delincuente hace uso de herramientas digitales a través de la informática para obtener los datos sensibles de una persona y así utiliza para apropiarse del patrimonio.

**2. En su opinión, ¿Todas las nuevas conductas delictivas cibernéticas que afectan al patrimonio podrían constituir fraude informático?**

El fraude es un concepto engañoso, que no tiene solución con el resultado típico, pero no todas las conductas delictivas deben de constituir el delito del fraude cibernético.

**3. Desde su criterio jurídico, ¿debería ser estrictamente necesario que el fraude informático se configure a través de las tecnologías de información y comunicación utilizando siempre los datos personales de la víctima o se puede consumar al inducir a error al sujeto pasivo?**

Mediante la obtención de datos sensibles de una forma ilegítima, pienso que no debe de ser estrictamente necesario, ya que acorde a cada una de sus modalidades se tiene que ver a través de la consumación y la tentativa.

**Objetivo específico 1**

Determinar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

**Premisa:** El smishing y el phishing son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa".

**4. En vista a la premisa acotada, bajo su propio criterio, ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático?**

Que al acceder o recepcionar un mensaje, el delincuente puede acceder mediante herramientas informáticas a tus datos y apropiarse, haciendo uso de los mismos, generando afectación patrimonial de la víctima.

**5. Por otro lado ¿Considera que a través del smishing se procesa los datos y transacciones bancarias, así como el procesamiento de los terminales electrónicos de las entidades financieras?**

Sí considero que otras de las modalidades del smishing se pueda recolectar información de las transacciones bancarias, por ello su peligrosidad en este tipo de delitos, ya que actualmente, varias personas realizan compras por internet o a través de su tarjeta de crédito en físico transmitiendo datos de la misma tarjeta.

**6. Según su percepción sobre esta temática ¿Cuál sería la solución para que los ciberdelincuentes a través del smishing no recolecten datos sensibles?**

Con herramientas tecnológicas de seguridad cibernética y su difusión, concientizando a las personas a no confiar en ese tipo de información recibida.

**Objetivo específico 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

**Premisa:** El phishing se encuentra diseñado con la finalidad de robarle la identidad del usuario obteniendo información privada que es usada por medio de engaños, utilizando ventanas emergentes o correos electrónicos orientados a ejecutar transacciones bancarias en perjuicio del titular del producto financiero (tarjetas de

crédito o débito)

**7. Desde su experiencia ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático?**

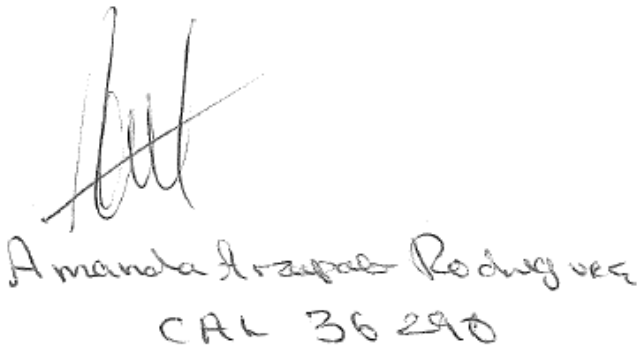
Enlaces remitidos por correos, enlaces de páginas webs, entre otros mensajes que coinciden muchas veces con los intereses de la víctima.

**8. De acuerdo a su conocimiento ¿El Ministerio Público posee los instrumentos tecnológicos necesarios para combatir la comisión del delito de fraude informático bajo la modalidad del phishing?**

Los instrumentos que poseen el ministerio público especializado en delitos de ciberdelincuencia se remiten a seguir una ruta informática y buscar el origen, persona(s) que difunden este tipo de correos y que se hacen las investigaciones con la policía de informática.

**9. En su criterio ¿Qué alternativas de solución plantearía a fin de que se disminuya las cifras de la comisión de fraude informático bajo la modalidad de phishing?**

Brindar capacitaciones o charlas sobre la seguridad cibernética y uso correcto de los datos personales, riesgos del phishing y smishing a través de medios digitales como Google Meet, zoom, entre otros.



**FIRMA Y SELLO**

## ANEXO N° 03

## VALIDACIÓN DE INSTRUMENTO

UNIVERSIDAD CÉSAR VALLEJO

### VALIDACIÓN DE INSTRUMENTO

**I. DATOS GENERALES**

1.1. Apellidos y Nombres: Munayco Medina, Martha Elena

1.2. Cargo e institución donde labora: Fiscal Provincial de la Fiscalía Especializada en Ciberdelincuencia – Ministerio Público.

1.3. Nombre del instrumento motivo de evaluación: Ficha de Análisis de Fuente Documentos.

1.4. Autores del Instrumento: Burga Carrero, Kleyder Maycot y Morales Padilla, Gerardo Alexis

**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. | | | | | | | | | | | | ✓ | |
| 2. OBJETIVIDAD | Esta adecuado a las leyes y principios científicos. | | | | | | | | | | | | ✓ | |
| 3. ACTUALIDAD | Esta adecuado a los objetivos y las necesidades reales de la investigación. | | | | | | | | | | | | ✓ | |
| 4. ORGANIZACIÓN | Existe una organización lógica. | | | | | | | | | | | | ✓ | |
| 5. SUFICIENCIA | Toma en cuanta los aspectos metodológicos esenciales | | | | | | | | | | | | ✓ | |
| 6. INTENCIONALIDAD | Esta adecuado para valorar las categorías. | | | | | | | | | | | | ✓ | |
| 7. CONSISTENCIA | Se respalda en fundamentos técnicos y/o científicos. | | | | | | | | | | | | ✓ | |
| 8. COHERENCIA | Existe coherencia entre los problemas, objetivos, supuestos jurídicos | | | | | | | | | | | | ✓ | |
| 9. METODOLOGÍA | La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos. | | | | | | | | | | | | ✓ | |
| 10. PERTINENCIA | El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico. | | | | | | | | | | | | | ✓ |

**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, 05 de abril del 2023.

MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

FIRMA DEL EXPERTO INFORMANTE

UNIVERSIDAD CÉSAR VALLEJO

## VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

1.1. Apellidos y Nombres: Marchineres Ramos Lidia Lourdes

1.2. Cargo e institución donde labora: Docente de la UCV.

1.3. Nombre del instrumento motivo de evaluación: Ficha de Análisis de Fuente Documentos.

1.4. Autores del Instrumento: Burga Carrero, Kleyder Maycot y Morales Padilla, Gerardo Alexis

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. | | | | | | | | | | | | ✓ | |
| 2. OBJETIVIDAD | Esta adecuado a las leyes y principios científicos. | | | | | | | | | | | | ✓ | |
| 3. ACTUALIDAD | Esta adecuado a los objetivos y las necesidades reales de la investigación. | | | | | | | | | | | | ✓ | |
| 4. ORGANIZACIÓN | Existe una organización lógica. | | | | | | | | | | | | ✓ | |
| 5. SUFICIENCIA | Toma en cuanta los aspectos metodológicos esenciales | | | | | | | | | | | | ✓ | |
| 6. INTENCIONALIDAD | Esta adecuado para valorar las categorías. | | | | | | | | | | | | ✓ | |
| 7. CONSISTENCIA | Se respalda en fundamentos técnicos y/o científicos. | | | | | | | | | | | | ✓ | |
| 8. COHERENCIA | Existe coherencia entre los problemas, objetivos, supuestos jurídicos | | | | | | | | | | | | ✓ | |
| 9. METODOLOGÍA | La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos. | | | | | | | | | | | | ✓ | |
| 10. PERTINENCIA | El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico. | | | | | | | | | | | | ✓ | |

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, 05 de abril del 2023.

Lidia Marchineres R.
FIRMA DEL EXPERTO INFORMANTE
DNI: 07605847
Cel 987 107 906

UNIVERSIDAD CÉSAR VALLEJO

## VALIDACIÓN DE INSTRUMENTO

### I. DATOS GENERALES

1.1. Apellidos y Nombres: Munayco Medina, Martha Elena

1.2. Cargo e institución donde labora: Fiscal Provincial de la Fiscalia Especializada en Ciberdelincuencia – Ministerio Público.

1.3. Nombre del instrumento motivo de evaluación: Ficha de Entrevista

1.4. Autores del Instrumento: Burga Carrero, Kleyder Maycot y Morales Padilla, Gerardo Alexis

### 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. | | | | | | | | | | | | ✓ | |
| 2. OBJETIVIDAD | Esta adecuado a las leyes y principios científicos. | | | | | | | | | | | | ✓ | |
| 3. ACTUALIDAD | Esta adecuado a los objetivos y las necesidades reales de la investigación. | | | | | | | | | | | | ✓ | |
| 4. ORGANIZACIÓN | Existe una organización lógica. | | | | | | | | | | | | ✓ | |
| 5. SUFICIENCIA | Toma en cuanta los aspectos metodológicos esenciales | | | | | | | | | | | | ✓ | |
| 6. INTENCIONALIDAD | Esta adecuado para valorar las categorías. | | | | | | | | | | | | ✓ | |
| 7. CONSISTENCIA | Se respalda en fundamentos técnicos y/o científicos. | | | | | | | | | | | | ✓ | |
| 8. COHERENCIA | Existe coherencia entre los problemas, objetivos, supuestos jurídicos | | | | | | | | | | | | ✓ | |
| 9. METODOLOGÍA | La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos. | | | | | | | | | | | | ✓ | |
| 10. PERTINENCIA | El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico. | | | | | | | | | | | | ✓ | |

### 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, 05 de abril del 2023.

FIRMA DEL EXPERTO INFORMANTE
MARTHA ELENA MUNAYCO MEDINA
FISCAL PROVINCIAL
4to Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

# VALIDACIÓN DE INSTRUMENTO

**I. DATOS GENERALES**

**1.1** Apellidos y Nombres: **Padilla Virhuez, Meri Liliana**

**1.2** Cargo e institución donde labora: Abogada Penalista

**1.3** Nombre del instrumento motivo de evaluación: **Ficha de Análisis de fuente de Documentos**

**1.4** Autor de Instrumento: Burga Carrero Kleyder Maycot y Morales Padilla Gerardo

**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 | Considera información actualizada, acorde a las necesidades reales de la investigación. | | | | | | | | | | | | x | |
| 4. ORGANIZACIÓN | Existe una organización lógica. | | | | | | | | | | | | x | |
| 5. SUFICIENCIA | Toma en cuenta los aspectos metodológicos esenciales | | | | | | | | | | | | x | |
| 6. INTENCIONALIDAD | Está adecuado para valorar las categorías. | | | | | | | | | | | | x | |
| 7. CONSISTENCIA | Se respalda en fundamentos técnicos y/o científicos. | | | | | | | | | | | | x | |
| 8. COHERENCIA | Existe coherencia entre los objetivos y supuestos jurídicos. | | | | | | | | | | | | x | |
| 9. METODOLOGÍA | La estrategia responde a 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 cumple con los requisitos para su aplicación

**IV. PROMEDIO DE VALORACIÓN:** 95

**Los Olivos, 20 de abril del 2023**


FIRMA DEL EXPERTO INFORMANTE
Padilla Virhuez, Meri Liliana
DNI 09518027 Telf.: 936025800

# VALIDACIÓN DE INSTRUMENTO

**V. DATOS GENERALES**

**1.1** Apellidos y Nombres: **Cuya Berrocal, José Miguel**

**1.2** Cargo e institución donde labora: Fiscal Provincial del 3er Despacho en Crimen Organizado

**1.3** Nombre del instrumento motivo de evaluación: **Ficha de Análisis de fuente de Documentos**

**1.4** Autor de Instrumento: Burga Carrero Kleyder Maycot y Morales Padilla Gerardo

**VI. 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 | Considera información actualizada, acorde a las necesidades reales de la investigación. | | | | | | | | | | | | x | |
| 4. ORGANIZACIÓN | Existe una organización lógica. | | | | | | | | | | | | x | |
| 5. SUFICIENCIA | Toma en cuenta los aspectos metodológicos esenciales | | | | | | | | | | | | x | |
| 6. INTENCIONALIDAD | Está adecuado para valorar las categorías. | | | | | | | | | | | | x | |
| 7. CONSISTENCIA | Se respalda en fundamentos técnicos y/o científicos. | | | | | | | | | | | | x | |
| 8. COHERENCIA | Existe coherencia entre los objetivos y supuestos jurídicos. | | | | | | | | | | | | x | |
| 9. METODOLOGÍA | La estrategia responde a 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 | |

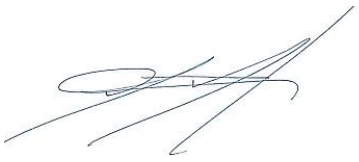
**VII. OPINIÓN DE APLICABILIDAD**

-El instrumento cumple con los requisitos para su aplicación — **SI**

-El instrumento cumple con los requisitos para su aplicación

**VIII. PROMEDIO DE VALORACIÓN:** 95

**Lima, 25 de abril del 2023**



FIRMA DEL EXPERTO INFORMANTE
Cuya Berrocal, José Miguel
Teléfono 998 785 555

**ANEXO N° 04**

**FUENTE DE ANALISIS DOCUMENTAL**

**Objetivo General**

Analizar cómo se emplean los datos personales en las nuevas modalidades de fraude informático.

## I. ANÁLISIS DE R. N° 743-2018 SALA PERMANENTE – LIMA

| Ficha de análisis de fuente de documentos - **Recurso de Nulidad** | |
|---|---|
| **Identificación de la fuente:**<br>Recurso de Nulidad N° 743-2018 - LIMA del veintiséis de octubre de dos mil dieciocho<br>https://static.legis.pe/wp-content/uploads/2019/08/R.N.-743-2018-Lima-Legis.pe_.pdf<br>Concurso aparente de leyes (un caso concreto) [RN 743-2018, Lima] \| LP (lpderecho.pe) | |
| **Texto relevante** | **Análisis del contenido** |
| Según lo expuesto por la **Sala penal permanentemente**, en el 5.4. de los fundamentos de derecho, con relación a los **datos personales**, consideran:<br>Para ingresar al sistema informático utilizaron información confidencial proporcionada para el desempeño de sus funciones (usuario y contraseña) para ingresar al sistema informático con la finalidad de modificar ingresando datos falsos para lograr que | En ese sentido, se debe entender que, el uso de los datos personales, no se generan únicamente mediante la captación de los mismos a través del smishing y phishing, sino más bien, como señala la sala, resulta que, al manipular un sistema informático que cuenta o mantiene información confidencial de una persona natural o jurídica, ingresando, modificando o alterando sin el permiso de los sujetos pasivos se configura de esa forma y se |

| | |
|---|---|
| los administrados tengan un duplicado de licencia pero bajo una categoría que no les correspondía. | consuma el fraude informático bajo las prerrogativas del mismo. |
| **Ponderamiento** | |
| En síntesis, lo que el Recurso de Nulidad Nº 743-2018**,** prevé que, para ingresar al sistema informático se utiliza información confidencial proporcionada por malos elemento de las entidades que tiene bajo su tutela datos personales de los usuarios de sus funciones (usuario y contraseña) para ingresar al sistema informático con la finalidad de modificar ingresando datos falsos para lograr que los administrados tengan un duplicado de licencia pero bajo una categoría que no les correspondía. | |

## II. ANÁLISIS DE LA RESOLUCIÓN FINAL Nº 0002-2023/INDECOPI-CHT

| | |
|---|---|
| Ficha de análisis de fuente de documentos - **Resolución Final de INDECOPI** | |
| **Identificación de la fuente:**<br>Resolución Final Nº 0002-2023/INDECOPI-CHT – Chimbote, el veintisiete de enero de dos mil veintitrés<br>Multan al BCP por permitir 31 consumos no reconocidos con la tarjeta de crédito de consumidor [Resolución 0002-2023/Indecopi-CHT] \| LP (lpderecho.pe) | |
| **Texto relevante** | **Análisis del contenido** |
| Según lo expuesto por Instituto Nacional de Defensa de la Competencia y | En ese mismo orden, debemos advertir que, el **uso de los datos** |

| | |
|---|---|
| de la Protección a la Propiedad y, en el fundamento veintidós y veintitrés -fundamento de los fundamentos de derecho, respecto de los **datos personales**, refieren.<br><br>Por su parte, el artículo 19 del Código establece que los proveedores son responsables por la calidad e idoneidad de los productos y prestar los servicios al consumidor en las condiciones entregar los productos y prestar los servicios al consumidor en las condiciones informadas o previsibles, atendiendo a la naturaleza de estos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta disposición.<br><br>El supuesto de responsabilidad administrativa en la actuación del proveedor impone a este la carga procesal de sustentar y acreditar que no es responsable por la falta de idoneidad del bien colocado en el mercado o el servicio prestado, sea porque actuó cumpliendo con las normas debidas o porque pudo acreditar la existencia de hechos ajenos que lo eximen de responsabilidad. Así, una vez acreditado el defecto por el consumidor o la autoridad administrativa, corresponde al proveedor acreditar que este no le es imputables. | **personales** bajo su propio criterio realza, enaltece y hace énfasis al referir que el artículo 29 de la ley de protección de los datos personales; se establece que cuando sea el caso de tratamiento de datos entre un proveedor se prevé una cláusula específica dentro del contrato de suministros, respecto de los criterios adoptados por las partes de forma particular, todo ello; con el fin de guardar confidencialidad de los datos personales del consumidor. |

| Ponderamiento |
| --- |
| En conclusión, la **Resolución Final Nº 0001-2023/INDECOPI-CCHT** advierte que, se ha demostrado respecto de que los proveedores son responsables por la calidad e idoneidad de los productos y prestar los servicios al consumidor en las condiciones entregar los productos y prestar los servicios al consumidor bajo los criterios y condiciones previstos por ambas partes con la voluntad propia del consumidor, así como la del proveedor. |

**Objetivo Específico N° 1**

Identificar de qué manera se utiliza el smishing para la comisión del delito de fraude informático.

## III. ANÁLISIS SOBRE EL PROYECTO DE LEY Nº 398/2021-CR, QUE PROMUEVE LA PROTECCIÓN DE LOS USUARIOS FINANCIEROS PARA PREVENIR Y SANCIONAR LOS FRAUDES INFORMÁTICOS

| Ficha de análisis de fuente de documentos - **Proyecto de Ley** | |
| --- | --- |
| **Identificación de la fuente:**<br>https://www.osiptel.gob.pe/media/fx0nwsvl/inf-315-oaj-opini%C3%B3n-legal-sobre-el-pl-n%C2%BA-398-2021-cr-que-promueve-la-protecci%C3%B3n-de-los-usuarios-financieros-para-prevenir-y-sancionar-los-fraudes-inform%C3%A1ticos.pdf | |
| **Texto relevante** | **Análisis del contenido** |
| Continuando con ello, es importante traer al análisis el **Proyecto de Ley** del OSIPTEL, en su artículo 1, con | Al dar lectura al **Proyecto de Ley** se puede apreciar que, este apartado normativo establece las medidas de |

| | |
|---|---|
| vinculación a los **fraudes informáticos** considerando que:<br><br>El presente proyecto de ley tiene por objeto establecer medidas de protección a los usuarios de servicios financieros para la prevención y sanción de los fraudes informáticos, a través de la consolidación de denuncias ciudadanas, las que se realizan por medio de ventanillas virtuales, contribuyendo con la Policía Nacional del Perú en la recopilación de información. | protección, buscando sancionar a las entidades financieras que incumplan con los parámetros de seguridad.<br><br>Ahora bien, es preciso indicar que el objeto de la ley indica que el cuerpo normativo está dirigido a usuarios de servicios financieros; asimismo, debe considerarse que los mensajes de texto, correos electrónicos o llamadas telefónicas no son recibidos solamente por usuarios de dichos servicios, sino también por personas que no los usan; razón por la cual se sugiere el uso del término ciudadanos en general. |
| **Ponderamiento** | |
| A manera de conclusión se puede indicar que, el **Proyecto de Ley Nro. 398/2021-CR,** prevé que los **fraudes informáticos** no solamente se expanden por los servicios financieros, sino por diferentes medios perjudicando a los ciudadanos de manera general, esto debido a que, los medios informáticos pueden conectarse por diferentes plataformas, como redes sociales, correos, aplicativos instalados en el celular, entre otros más. Es importante acotar que la pandemia por la COVID-19 no ha sido impedimento para la realización de los **fraudes informáticos** en sus diferentes modalidades más conocidas como el phishing y **smishing**. | |

## IV.ANÁLISIS DEL ARTICULO CIENTIFICO “SEGURIDAD POR CAPAS FRENAR ATAQUES DE SMISHING

| |
|---|
| Ficha de análisis de fuente de documentos – **Artículo Científico** |

<table>
<tr><td colspan="2">Identificación de la fuente:<br><br>http://dx.doi.org/10.23857/dom.cien.pocaip.2017.4.1.enero.115-130<br>URL:http://dominiodelasciencias.com/ojs/index.php/es/index</td></tr>
<tr><td>Texto relevante</td><td>Análisis del contenido</td></tr>
<tr><td>Siguiendo con el análisis, traemos al análisis el Artículo Científico de Ecuador, en el cual han investigado las capas para frenar el ataque del smishing considerando que, hoy en día la tecnología móvil se ha convertido en una necesidad vital para la comunicación de los seres humanos. La convergencia digital ha hecho que a través de un dispositivo móvil podamos realizar múltiples tareas. Sin embargo, los atacantes han visto como oportunidad este avance para perpetrar diferentes ataques.</td><td>Realizando el análisis del Artículo Científico Ecuatoriano, debemos de enfocarnos en las soluciones brindadas ante el ataque de smishing SMS dirigida a teléfonos celulares conocidos como smartphone. Teniendo en cuenta ello, se ha propuesto que la solución parte de la prevención, siendo la educación un pilar importante, por lo que, la aplicación de un programa educacional sobre estos ataques de smishing es una medida de seguridad que se debería abordar desde los primeros años del colegio, explicando que es el smishing,<br><br>En esa misma línea, el usuario nunca debe dar detalles de datos bancarios ni de tarjetas de crédito por teléfono, asimismo, debe de ignorar los mensajes de textos de remitentes y texto desconocido y finalmente, deberá de reportar estas anomalías al departamento de seguridad de las operadoras móviles.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
</table>

A manera de conclusión, se puede precisar que el **Artículo Científico "seguridad por capas frenar ataques de smishing**, busca prevenir el ataque del smishing mediante la educación en sus diferentes niveles (inicial, primaria y secundaria), asimismo, a nivel empresarial, los proveedores de tarjetas de crédito o débito, deben de encargarse de la capacitación constante de su personal, con la finalidad mejorar la instrucción a los usuarios financieros disminuyendo el número de las posibles víctimas del ataque de smishing, finalmente, otra capa de solución a esta modalidad del fraude informático es la instalación de antivirus efectivos desde que se compra el equipo móvil, en otras palabras que el operador telefónico cumpla con instalar predeterminadamente en sus funciones del móvil el aplicativo antismishing.

**Objetivo Específico N° 2**

Identificar de qué manera se utiliza el phishing para la comisión del delito de fraude informático.

## V. ANÁLISIS DE DERECHO COMPARADO; SENTENCIA Nº178 DE LA 9º AUDIENCIA PROVINCIAL DE MADRID Y SENTENCIA Nº00064/2016 JUZGADO DE INSTRUCCIÓN NUM. 3 DE BURGOS

Ficha de análisis de fuente de documentos - Jurisprudencia comparada -

**Sentencia sobre la responsabilidad bancaria por Phishing**

**Identificación de la fuente:**

S.A.P.M. de 12 de marzo de 2018

S.A.P. Burgos de 03 de marzo del 2016

La responsabilidad bancaria por Phishing. Aspectos jurisprudenciales (belzuz.com)

Jurisprudencia: el "phising" como modalidad de estafa informática. - IDIBE

| Texto relevante | Análisis del contenido |
| --- | --- |
| Desde su postura y en este caso, según la sentencia de doce marzo del 2018 en su fundamento 9º, fundamento de derecho; han establecido que, “tanto en la banca por internet, el banco debe comprobar en todo caso la autenticación de cualquier consumo, para determinar la autenticidad de la transferencia (en la mayoría de **fraudes informáticos, por medio de phishing** usualmente el que ordena algún pedido online no es el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondiente las cantidades cargadas. En consecuencia, hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima.<br><br>Respecto de la sentencia en la Audiencia Provincial de Burgos de 03 de marzo del 2016, en su fundamento jurídico 1º, hace referencia a que, existen diferentes modalidades de realización de | Estando al análisis en paralelo de ambas sentencias, respecto del **phishing** como nueva modalidad del fraude informático; debemos entender primero, que, para que se cometa el ilícito penal bajo esta nueva modalidad de fraude informático, es necesario que se capten los datos personales de una persona a través de las páginas webs que se generan con el fin de vender o comercializar un producto determinado hacia el cual está enfocado el consumidor. En ese mismo orden, corresponde analizar la segunda sentencia en cuestión, la cual advierte, que la información que se puede obtener es remitida en algunos casos por las víctimas al ser inducidas por sus cuentas bancarias al activarse a través de un determinado programa (keyloggers) el cual permite la obtención de la información del usuario o consumidor de las diferentes entidades. |

| | |
|---|---|
| este fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que la información que se podría obtener nos podrían indicar como se ha realizado el **phishing** y donde la información que se obtuvo ha sido enviada, si hay más víctimas que entidades bancarias han sido introducidas en el programa para ser activado en caso de keyloggers, así como facilitar información que pudiera llevar a la identificación de otros miembros de la organización. | |

**Ponderamiento**

En síntesis, lo que la **SENTENCIA P.A.M. de 12 de marzo de 2018** refiere que, la comisión del delito de **fraude informáticos, por medio de phishing** usualmente se realiza a través del que ordena algún pedido online no es el titular de la cuenta) es un riesgo a cargo del banco. Asimismo, la Sentencia **A.P. Burgos de 03 de marzo del 2016,** sostiene que, el fraude informático a través del phishing no requiere una estructura propia de esta modalidad, por eso es que, cuando se cometa este tipo de fraude es fundamental realizar un informe técnico forense y post análisis del equipo informático de la víctima, toda vez que la información que se podría obtener nos podría indicar como se ha realizado el **Phishing**.

## VI. ANÁLISIS DEL BOLETÍN SEMANAL - SBS INFORMA N° 26

Ficha de análisis de fuente de documentos - **Boletín Semanal**

| **Identificación de la fuente:**<br>https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/74 | |
|---|---|
| **Texto relevante** | **Análisis del contenido** |
| Siguiendo con este análisis y en concordancia con el **Boletín Semanal - SBS Informa N° 26** de Perú, en realizando un proyecto normativo con vinculación a las **modalidades de fraude informático** teniendo en consideración que:<br><br>El mayor número de transacciones a través de canales digitales o electrónicos, así como el creciente uso de las tarjetas para adquirir bienes y servicios en comercios online, hacen necesario un refuerzo en los mecanismos de seguridad implementados en cautela de los derechos de los usuarios. En ese sentido, el proyecto normativo plantea que las empresas ofrezcan, en todos los casos y tipos de tarjetas, la posibilidad de activación del servicio de notificaciones sobre las operaciones realizadas; además, de una serie de medidas de seguridad para el procesamiento y aprobación de las transacciones. | Al dar lectura al Boletín Semanal, se puede apreciar que este proyecto normativo, busca reforzar los mecanismos de seguridad en las transacciones digitales debido a que con acceso a internet; es una realidad que también expone al usuario a otro tipo de riesgos, como el **fraude cibernético** en sus diversas modalidades (phishing, carding, smashing, entre otros), para los cuales puede existir poca información que le permita al consumidor conocer las prácticas de seguridad que deben ser adoptadas. |

| Ponderamiento |
| --- |
| A manera de conclusión, se puede indicar que el **Boletín Semanal - SBS Informa Nro. 26 de la SBS,** prevé que, en este proyecto se busca brindar mayores mecanismos de protección en las etapas de contratación, uso y cancelación de dichas tarjetas; así como fortalecer las medidas de seguridad de las operaciones y productos financieros vinculados a las mismas. Asimismo, mediante el precitado Boletín Semanal, se analizó estadísticamente el crecimiento de los pagos a través de los medios electrónicos habiendo crecido las transacciones monetarias, lo que incrementó las modalidades de fraude informático, sin embargo, esta medida no ha reducido los fraudes informáticos como es el phishing. |

## ANEXO N° 05: Matriz de triangulación de datos de entrevista

| Problema de Investigación | Guía de entrevista P1 | Guía de entrevista P2 | Guía de entrevista P3 | Guía de entrevista P4 | Guía de entrevista P5 | Guía de entrevista P6 | Guía de entrevista P7 | Guía de entrevista P8 | Guía de entrevista P9 | Categorías Emergentes | Ponderamiento de resultado de entrevista |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ¿Cómo se emplean los datos personales en las nuevas modalidades de fraude informático? | Se emplean en el perfilamiento de las potenciales víctimas a fin de poder ejecutar desde una suplantación de identidad, fraude, acceso ilícito, hasta la comercialización de los mismos. | Debemos tomar en consideración que existen muchas modalidades de fraude informático las que de una u otra manera se asemejan a la estafa agravada (numeral 5 del artículo 196 A del C.P), en el sentido que mediante las modalidades de phishing smishing vishing, etc., se procura capturar datos personales o bancarios del titular de una cuenta bancaria para el subsecuente perjuicio patrimonial, en estos casos a la | Conforme a las modalidades de fraude informático: diseño, introducción, supresión, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; se requiere que los ciberdelincuentes obtengan “ex ante” de manera indebida los datos personales o financieros (nombres y apellidos, fecha de nacimiento, números de | El uso ilegal de los datos personales en las nuevas modalidades se da mediante la sustracción y/o manipulación de la información a favor del ciberdelincuentes (acceso a cuentas del correo electrónico, numero de celular, redes sociales, tarjetas de debido y/o crédito), el mismo que se manifiesta mediante las siguientes modalidades : clonación de páginas falsas, compras fraudulentas, | Con los datos personales se emplean técnicas de ingeniería social o manipulación informática para que el sujeto activo obtenga ventaja patrimonial de la víctima, utilizando la propia información de esta última, como el caso de Phishing. | Se verifican con el propósito de validar la identidad de una persona natural o jurídica ante una plataforma tecnológica con el fin de obtener un lucro económico y/o la obtención de información. | Los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. Una vez obtenida, esta será usada para fines delictivos como es el delito de phishing | Se emplean mediante la sustracción de algún equipo electrónico, logrando ingresar a su información importante del usuario para luego extraer su dinero. | El delincuente hace uso de herramientas digitales a través de la informática para obtener los datos sensibles de una persona y así utiliza para apropiarse del patrimonio. | Perfilamiento de la victima<br><br>Hipervínculos incluidos<br><br>Cultura informática | Los datos personales en las nuevas modalidades de fraude informático se emplean en el perfilamiento de las potenciales víctimas a fin de poder ejecutar desde una suplantación de identidad, debiendo de tomar en consideración que una vez que el delincuente obtiene estos datos personales, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. Asimismo, los datos personales se emplean mediante una base de datos que es alterada para obtener información relevante de los usuarios. En ese sentido, las nuevas conductas delictivas cibernéticas que afectan al patrimonio, no constituyen un fraude informático, debido a que, en estos tiempos, se confunde muchos los delitos informáticos, con los |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | víctima se le envía enlaces o mediante llamadas para que sea el mismo quien proporciones sus datos personales o de cuenta y a partir de ello realizar delitos de fraude.<br><br>También, se da el caso de aquellas personas que no reciben llamadas, pero sus datos personales, previamente han sido obtenidos mediante la vulneración o acceso indebido a sistemas bancarios incluyendo la RENIEC. Una vez que el delincuente obtiene estos datos personales o financieros como | tarjeta bancaria, números de cuenta bancaria, fecha de vencimiento de la tarjeta, CVV (código valor de validación), entre otros) los mismos que son objeto de uso para concretar el perjuicio a la víctima. | falsas ofertas online, suplantación de identidad, suplantación de tarjetas bancarias, falsos prestamos, falsas encomienda s, etc. | | | | | | | delitos computaciones; que están relacionados a todos los eventos en la que el agente tiene como herramienta de trabajo una computadora, un teléfono o cualquier herramienta tecnológica y de una u otra forma el agente realiza actuaciones en contra de los intereses de la empresa lo cual bien puede ser una estafa . Finalmente, el delito de fraude informático desde su origen y evolución, requiere o necesita la intromisión, acceso, modificación de datos y sistemas informáticos para su consumación, necesitando las TICs como medio o herramienta para consumar los medios comisivos que se encuadran en su descripción típica, mientras que la inducción a error al sujeto pasivo encuentra identificación objetiva con el tipo penal de estafa agravada. Por lo que, en nuestra vida cotidiana, se dan situaciones en las que se induce a error al sujeto pasivo, así por ejemplo si Juan haciéndose pasar como trabajador de |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | nombres, número de DNI, ubigeo, número de cuenta, tarjeta o clave TOKEN, proceden a introducir o procesar estos datos para obtener un provecho económico y subsecuente perjuicio patrimonial a la víctima. | | | | | | | | | una entidad bancaria realiza llamada a María comunicándome que debe realizar el cambio de su tarjeta por una nueva en la cual se amplía su línea de crédito, para lo cual un funcionario de PROSEGUR se constituirá a su inmueble a recoger la tarjeta llevando además documentos a firmar, María quien en ese momento requería de dinero procede a entregar su tarjeta y luego del cual recibe una llamada del banco en el sentido que desde su cuenta, se habían realizados transferencias de dinero, otra modalidad es cuando la persona accede a una página clonada en la cual consigna información personal y bancaria. |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ¿De qué manera se utiliza el smishing para la comisión del delito de fraude informático? | Es una modalidad derivada del phishing, o de las diversas formas de manipulación informática, que mediante técnicas de ingeniería social, obtienen los datos personales - bancarias - de la víctima, para obtener ventajas patrimoniales. | El smishing es una de las modalidades más comunes del delito de fraude informático, y generalmente se dan porque las personas reciben un mensaje de texto de una supuesta entidad bancaria para ser beneficiario de algún producto enviando adjunto un enlace, en donde la persona al acceder al mismos digita información confidencial y reservada como datos personales o bancarios, también cuando la persona recibe un enlace para confirmar determinada operación, | Bajo mi criterio, el smishing es una modalidad y/o variante del phishing, que consiste en el envío de enlaces maliciosos o perniciosos mediante mensajes de texto remitidos a los equipos móviles (celulares) que tienen como finalidad la de acceder ilícitamente a los datos personales o bancarios de las víctimas con el objeto de causar perjuicio patrimonial o moral | El daño ocasionado a través del smishing es la obtención de datos privados o credenciales de un cliente suplantando la identidad de una empresa para cometer fraudes, robos u otros delitos informáticos. | El phishing tiene por objetivo recolectar información a partir de técnicas de clonación de sistemas, entre otros. En particular, el smishing es un ataque similar al anterior solo que su operatividad se limite a la mensajería de texto, para lo cual se camuflan con herramientas para que la víctima crea que el mensaje es auténtico, según el contexto. | El smishing se utiliza como el medio de envío de mensajes el cual contendrá un enlace o link fraudulento que inducen al usuario a ingresar sus credenciales y/o datos personales, y/o sensibles. | El smishing se comete mediante mensajes de texto que conllevan a que el usuario de a pie, ingresar al enlace que se ha enviado con la única finalidad de ingresar a sus cuentas bancarias a fin de cometer un fraude electrónico, vulnerando los mecanismos de seguridad de la entidad financiera del consumidor. | El smishing se utiliza mediante el envió de mensaje de texto, ya que, al ser un mensaje fraudulento, el usuario es inducido a error ingresando al enlace, lo que conlleva a compartir sus datos personales. | Que al acceder o recepcionar un mensaje, el delincuente puede acceder mediante herramientas informáticas a tus datos y apropiarse, haciendo uso de los mismos, generando afectación patrimonial de la víctima. | | El smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios; por ello, las instituciones financieras informan a los clientes que ellos no envían mensajes de texto con hipervínculos incluidos, mucho menos solicitan o piden dar claves o información personal y confidencial a través de un mensaje. Muchas veces, el smishing se limita a que el agraciado o víctima sea redirigido a un |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | también se podría relacionar esta modalidad de pesca en los delitos de estafa en la cual muchas personas son felicitadas por haber resultado ganadoras en un concurso para el cual se les adjunta un enlace que al acceder consignar información sensible | | | | | | | | | sistema de información (página web, entre otros), la misma que pueda ser un sistema clonado o falso para que posteriormente los ciberdelincuentes con la información recolectada ejecutar sus actividades delictivas. En tanto, el smishing va orientado exclusivamente a obtener de la víctima información confidencial – mediante enlaces para luego pasar a un segundo momento y utilizar estos datos. Ante esto, se podría decir que el smishing consiste en pedir a los clientes, usuarios que verifiquen transacciones de procedencia dudosa a través de un enlace que aparece en el mensaje de texto. De |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | esta manera, los ciberdelincuentes roban información confidencial, como credenciales de acceso a cuentas y datos bancarios. |
| ¿De qué manera se utiliza el phishing para la comisión del delito de fraude informático? | Exponer la manera como se materializa el phishing, sería un espacio insuficiente para considerar la multiplicidad de aquellas utilizadas por el phisher, pero que bien, las más conocidas o utilizadas se dan en las | El phishing es una modalidad de estafa muy común, en el cual muchas personas fácilmente son captadas y entregan información confidencial a personas que usualmente suplantan la identidad de una entidad financiera o empresarial, luego del cual esta | Es una modalidad consistente en el envío de “carnadas” o “cebos” mediante mensajes en redes sociales o correos electrónicos, por cuanto, las víctimas al ingresar en estos links remitidos, se recolectan datos de las tarjetas bancarias y de sus | Las formas de recolección de datos en el phishing son a través del email, spam, entrega a través de la web, hacker, malware, manipulación de enlaces, troyanos, ransomware, publicidad y/o anuncios maliciosos. | Utilizando los datos recolectados (credenciales de accesos, información bancaria, entre otros. Para poder acceder a los sistemas ya ser páginas web financieras y en algunos casos comercializar la información recolectada de muchos usuarios | En su mayoría a través del ingreso a enlaces fraudulentos que se recopilan datos sensibles. | El phishing de manera similar que el smishing, se materializa mediante un medio electrónico. En el caso del phishing es un correo electrónico - de los casos más comunes que he tomado información – el emisor del phishing se hace pasar por una entidad | Se utiliza mediante el envió de enlaces engañosos que persuaden al usuario para obtener un supuesto beneficio. | Enlaces remitidos por correos, enlaces de páginas webs, entre otros mensajes que coinciden muchas veces con los intereses de la víctima. | | La materialización del phishing ocurre a través de varias modalidades, siendo esta múltiple su captación y recepción de datos esenciales de las víctimas a través de redes sociales o correos manipulados y que tiende a buscar las necesidades de las víctimas. Flores (2023), Munayco (2023), Quispe (2023), Vallejos (2023), Zevallos (2023), Solsol (2023) y Bobadilla (2023) coinciden que, en la actualidad, mediante la formalización de una fiscalía especializada ha permitido otorgar mejoras en la |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | plataformas como correos electrónicos de la víctima, o páginas webs, suplantando la identidad de bancos. | información es procesada o utilizada en un segundo momento para realizar disposiciones patrimoniales de una determinada cuenta y en otros casos utilizar estos datos para suplantar identidad y generar préstamos. Lo que llama la atención en este caso, es de personas que sin ser partícipes de algún sorteo o concurso dan como cierta información en el sentido que han sido favorecidos con un premio y acceden a enlaces maliciosos o ingresan datos a determinada página. | respectivos titulares para realizar transferencias de dinero indebidas y no autorizadas. | | | | financiera enviando publicidad o alguna información referente a su cuenta bancaria de la víctima, es aquí, cuando el consumidor cae en el anzuelo compartiendo sus datos personales sensibles. | | | | investigación de delitos de fraude informático, sin embargo, no es suficiente ya que existen ciertas deficiencias. No obstante, algunos autores expresan su progreso mediante el equipo de fiscales y peritos informáticos para indagar y articular de forma correcta la investigación de estos delitos. Los usuarios para no ser víctimas de estas modalidades de fraude informático, deben de tener una cultura informática preventiva que permita a la población en tener conocimiento mediante capacitaciones presenciales o virtuales a no abrir información que ellos no conocen su procedencia y utilizar herramientas de seguridad básicos. La alternativa de solución, para erradicar el phishing es la creación de programas que puedan detectar correos falsos que se hacen pasar como entidades financieras bloqueando o eliminando inmediatamente los mensajes fraudulentos. En la actualidad esto no sucede, debido a que el programa de mensajería instantánea |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | consulta si deseas eliminarlo o no, y es aquí donde causa curiosidad al usuario haciéndole ingresar al enlace. De la misma forma que el smishing, las entidades financieras y otras autoridades públicas deben capacitar a la ciudadanía para evitar ser víctima de estos fraudes informativos. |

UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES**

**ESCUELA PROFESIONAL DE DERECHO**

# Declaratoria de Autenticidad del Asesor

Yo, SANTISTEBAN LLONTOP PEDRO PABLO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Uso de los datos personales en las nuevas modalidades de fraude informático, Lima, 2022.

", cuyos autores son BURGA CARRERO KLEYDER MAYCOT, MORALES PADILLA GERARDO ALEXIS, constato que la investigación tiene un índice de similitud de 17.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

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

LIMA, 26 de Junio del 2023

| **Apellidos y Nombres del Asesor:** | **Firma** |
|---|---|
| SANTISTEBAN LLONTOP PEDRO PABLO<br>**DNI:** 09803311<br>**ORCID:** 0000-0003-0998-0538 | Firmado electrónicamente por: PSANTISTEBANL el 01-07-2023 22:41:42 |

Código documento Trilce: TRI - 0551257

INVESTIGA UCV