Universidad César Vallejo

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El uso de aplicativos bancarios perjudican a los clientes en los delitos informáticos

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORA:

Quipuscoa Panduro, Giovanna Milagros (orcid.org/0000-0001-5943-9948)

ASESOR:

Mgtr. Palomino Gonzales, Lutgarda (orcid.org/0000-0002-5948-341X)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA-PERÚ

2023

Dedicatoria

Mi tesis va dedicado a mi familia, los cuales me han ayudado en cada uno de mis logros, y sobre todo quiero servir de ejemplo a mi hija para enseñarle que se termina, lo que uno empieza, la perseverancia es uno de los grandes valores que deseo inculcarle.

Giovanna Milagros Quipuscoa Panduro

Agradecimiento

Gracias al apoyo de la Mg. Lutgarda Palomino Gonzales en colaboración de la universidad César Vallejo, los cuales con sus constantes observaciones hacen que se pueda tener un trabajo de primer nivel cumpliendo con las normas establecidas.

Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, PALOMINO GONZALES LUTGARDA, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis Completa titulada: "El uso de aplicativos bancarios perjudican a los clientes en los delitos informáticos", cuyo autor es QUIPUSCOA PANDURO GIOVANNA MILAGROS, constato que la investigación tiene un índice de similitud de 7.00%, 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 Completa 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, 21 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
LUTGARDA PALOMINO GONZALES **DNI:** 22422843 **ORCID:** 0000-0002-5948-341X	Firmado electrónicamente por: LUPALOMINOG el 04-12-2023 22:01:33

Código documento Trilce: TRI - 0657919

INVESTIGA UCV

Declaratoria de originalidad del auto

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, QUIPUSCOA PANDURO GIOVANNA MILAGROS estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "El uso de aplicativos bancarios perjudican a los clientes en los delitos informáticos", es de mi autoría, por lo tanto, declaro que la Tesis:

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

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

Nombres y Apellidos	**Firma**
GIOVANNA MILAGROS QUIPUSCOA PANDURO **DNI:** 47073038 **ORCID:** 0000-0001-5943-9948	Firmado electrónicamente por: GQUIPUSCOAP el 21-11-2023 18:23:31

Código documento Trilce: TRI - 0657920

INVESTIGA UCV

Índice de contenidos

Índice De Tablas

Resumen

El cual tuvo como objetivo determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios. La metodología es de enfoque cualitativo de tipo básica, con diseño de teoría fundamentada, ya que busca recopilar conocimientos existentes de teorías del sobre el tema, el escenario de estudio tiene tres enfoques para su descripción partiendo como primer punto el escenario de la fiscalía de ciberdelincuencia ya que, al ser, la única fiscalía a nivel nacional se obtuvo un análisis completo de la problemática. Como siguiente escenario se tiene la DIVINDAT que es la unidad de investigación de alta tecnología del cual se tuvo la parte operacional del problema como último escenario se tiene el aspecto jurídico desde la perspectiva de los litigantes penalistas los cuales ayudara a la investigación para obtener un mejor resultado. Por lo cual se llegó a la conclusión que los delitos informáticos de tipo bancario han tenido un aumento significativo con el avance tecnológico. El problema radica que no hay una adecuada tipificación, por ser una ley especial son muy lesivos, existe una brecha entre la normatividad ya que no se encuentra debidamente regulada y esto trae consigo que muchos casos queden impunes.

***Palabra clave*:** Delitos informáticos, ciberdelincuencia, fraude informático, suplantación de identidad.

Abstract

The objective of which was to determine how computer crime harms the client in the use of banking applications. The methodology is a basic qualitative approach, with a grounded theory design, since it seeks to compile existing knowledge of theories on the subject. The study scenario has three approaches for its description, starting from the scenario of the cybercrime prosecutor's office as the first point. Since, being the only prosecutor's office at the national level, a complete analysis of the problem was obtained. The next scenario is the DIVINDAT, which is the high-tech investigation unit of which the operational part of the problem was taken. The last scenario is the legal aspect from the perspective of the criminal litigants, which will help the investigation to obtain a better result. Therefore, it was concluded that banking-type computer crimes have had a significant increase with technological advancement. The problem is that there is no adequate classification, because it is a special law they are very harmful, there is a gap between the regulations since it is not properly regulated and this means that many cases go unpunished.

Keywords: Cybercrime, cybercrime, computer fraud, phishing.

I. INTRODUCCIÓN

Con el transcurso de los años la tecnología ha tomado mayor significancia en la vida cotidiana, ya que brindo una serie de beneficios tanto en el sector laboral, económico, social y cultural, sin embargo, ello también generó que aparecieran nuevas formas delictivas, especialmente en el ámbito bancario ya que uno de los instrumentos a través del cual nos comunicamos es mediante un teléfono móvil el cual tiene los aplicativos necesarios para realizar todas nuestras transacciones bancarias sin necesidad de ir una entidad bancaria, siendo así el teléfono móvil el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos, en nuestro país hasta el mes de abril del 2022, hubo 7, 297 denuncias presentadas en el Ministerio Público en todo el territorio nacional, siendo el fraude informático y la suplantación de identidad los delitos más denunciados (los funcionarios del Ministerio Público, 2022) sin embargo al ser una fiscalía nueva aún falta más estudios que recabar, toda esta problemática ha motivado el presente estudio.

Los aplicativos bancarios son descargados obligatoriamente por aquellas personas que realizan distintas transacciones interbancarias como giros, pagos, movimientos interbancarios, y demás, por lo que hoy en día en nuestro país existen gran cantidad de aplicativos móviles o APP bancarios llamadas Banca Móvil. Los más populares son BBVA Perú, Interbanck App, Banca Móvil BCP, Scotiabank App y billeteras digitales como Yape, plim, Angora, las cuales son utilizadas por gran cantidad de usuarios, aplicaciones bancarias que tienen como distintivo su forma de funcionamiento, ya que funcionan en base a la operatividad de un número de celular, y se caracteriza principalmente por la forma en que los clientes pueden usarlo desde cualquier lugar, para ello el único requisito es que cuenten con acceso a internet y un dispositivo móvil. (Datos Lr, 2022)

La aplicación de tecnologías de información y la comunicación (TIC) ha tomado gran relevancia, especialmente en los países subdesarrollados de Latinoamérica. En el ámbito laboral, muchos prefieren el teletrabajo, y las ventas

online crecieron, esto trajo consigo que se utilice más plataformas digitales con el objetivo de llegar a los clientes, en este sentido los bancos tuvieron que innovar y desarrollar aplicativos bancarios más sencillos. para que a sus clientes se les facilite la forma de pago y compras. (Huamanñahui et.al, 2022).

A nivel internacional se tiene que la actividad delictiva, cada año adquiere nuevas formas, métodos de delinquir, esto se ha ido desarrollando e incrementando con el paso de los años, hoy en día los delitos cibernéticos son los más comunes en Ucrania y en todo el mundo, a su vez este desarrollo tecnológico que se presenta día a día también ha afectado al sector bancario debido a la cantidad de delitos cometidos al obtener acceso a códigos de tarjetas bancarias y la incautación ilegal de fondos de cuentas crece cada año, la principal propagación de formas virtuales delictivas se debe al rápido desarrollo de la tecnología, y se requiere un conocimiento especializado de los funcionarios, (Sergei et al, 2021).

Debido a todas estas nuevas formas delictivas, las cuales no han sido motivo de estudios a gran escala, es que se origina el presente trabajo de investigación el cual tuvo como problema general el siguiente: ¿El delito informático perjudica al cliente en el uso de aplicativos bancarios? Asimismo, formula el primer problema específico PE.1: ¿El fraude informático perjudica al cliente en el uso de aplicativos bancarios? De igual manera, se formula el segundo problema específico PE.2: ¿La suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios?

Igualmente, este estudio presenta justificaciones en tres niveles:

Justificación Teórica, el presente trabajo de investigación tuvo como propósito determinar de qué modo la utilización de aplicativos bancarios perjudica a los clientes, desde la obtención de teléfonos móviles, pueden acceder a la mayoría e incluso en algunos casos a todo los sistemas, datos informáticos, lo cual trae consigo que se cometan delitos informáticos que es un nuevo delito y se encuentra contemplado en una ley especial, para mitigar el incremento de ilícitos bajo esta modalidad que son los aplicativos bancarios, se busca sugerir cambios en la legislación actual en cuanto a delitos informáticos. De acuerdo con el convenio sobre la (Ciberdelincuencia ,2001)

Justificación Metodológica, este trabajo de investigación es cualitativa demuestra que es un proceso inductivo encuadrado en un ambiente sencillo, esto es producido por la relación que guarda entre los participantes de la investigación extrayendo sus vivencias e ideología del empleo de un instrumento de medición predispuesto. (Hernández –Sampieri, 2014)

Justificación Practica, este trabajo de investigación buscó proponer una reforma legal o sistematizar y poner en práctica el texto normativo ya existente, respecto a los delitos informáticos, de igual forma enmendar los distintos métodos de las entidades bancarias que tuvo como objetivo salvaguardar la seguridad de sus clientes en cuanto al uso de los aplicativos, para que mediante un trabajo en conjunto con el Ministerio Público, logren sancionar los ilícitos involucrados con delitos informáticos.

Una vez analizado los temas y al problema planteado, el siguiente paso consistió en establecer el siguiente objetivo general: Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios, como primer objetivo específico: Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios. Asimismo, el segundo objetivo específico fue: Establecer de qué manera la suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios.

II. MARCO TEÓRICO

Conforme con los antecedentes internacionales se tiene lo siguiente:

Ferruzola y Cuenca (2014) tuvo como objetivo responder ante un incidente de este tipo, aun cuando no se tengan vastos conocimientos informáticos, el tipo de investigación de este artículo es descriptivo con un enfoque cualitativo y llego a la conclusión que el problema radica en las medidas de cómo resolver estos delitos, ya que primeramente los delitos informáticos quedan impunes, por lo antes dicho, no se encuentran incorporados en una normatividad especifica. En el código penal ecuatoriano que está vigente, existe una forma jurídica que hacen que estos delitos aún no se adecuen al tipo penal, lo que perjudica al agraviado, ya que, al no estar dentro de los delitos comunes, no se puede establecer una pena o lo asemejan a otro delito como un simple robo o hurto.

Mayer (2017) tuvo como objetivo diferenciar entre un delito informático y otros delitos sería de fondo y no meramente de forma, su tipo de investigación es descriptivo con un enfoque cualitativo del cual se concluyó en que una de la característica informática, por una parte, atracción debe precisarse dinámicamente en la forma de sus usos que es mediante redes en tanto este sistema sea de interconexión a distancia y abundante entre las personas establece por otra parte, un bien jurídico protegido sistemático de carácter colectivo, cuya tutela debe comprobarse en términos especialmente limitado

Bourdillon (2023) tuvo como objetivo centrar los diferentes tipos de fraude y cómo afecta la aceptación de la economía digital en Nigeria, las diferentes técnica para ayudar a detectar y mitigar estos fraudes, su tipo de investigación es descriptivo con un enfoque cualitativo la investigación concluyo el crecimiento de la economía digital se ve obstaculizado por los crecientes intentos de los estafadores, que dañan gravemente las billeteras, la certidumbre y la percepción de seguridad de los clientes, así como el estado-nación. se ocupa de las estrategias para hacer frente a los fraudes en línea, sin duda será fascinante para los expertos en los

campos económico y financiero que se ocupan de problemas similares a diario y la necesidad de tomar precauciones contra los delitos económicos y financieros

Banda y Phiri (2019) tuvo como objetivo analizar el procedimiento para un mecanismo de defensa contra el hombre a la vanguardia como uno de los muchos ejemplos en los que la informática móvil enfrenta desafíos en cuanto a las trampas de seguridad su tipo de investigación es descriptivo con un enfoque cualitativo la investigación concluyo que el internet se usa cada vez más, pero el hecho de que Internet no se haya desarrollado con una capa de identidad adecuada es un riesgo de seguridad importante. La fatiga de contraseñas y el fraude en línea son un problema creciente y están dañando la confianza de los usuarios, en cualquier caso, las futuras soluciones de gestión de identidad tendrán que funcionar en entornos informáticos móviles, La gestión de la identidad móvil tendrá que admitir una cantidad considerable de variedades de tecnologías de la información y dispositivos con requisitos críticos como la usabilidad en movimiento, la privacidad, la escalabilidad y el ahorro de energía.

Sergei et al. (2021) tuvo como objetivo analizar y sistematizar la experiencia teórica y las medidas prácticas para combatir el delito cibernético en el sector bancario con el fin de identificar formas prometedoras de combatir los delitos en el ciberespacio de Ucrania, su tipo de investigación es descriptivo con un enfoque cualitativo la investigación concluyo en la actualidad, en el país de Ucrania se puede apreciar cierta dificultad en cuanto a la lucha contra el ciberdelito en el ámbito bancario. Un paliativo a este problema podría ser la aplicación de algunas normas tendientes a la prevención e investigación completa de aquellos delitos que se cometen en el ámbito de la tecnología. Las diversas vivencias que se dan principalmente en los países desarrollados muestran un sistema eficiente en cuanto a la lucha contra los delitos provenientes del ciberespacio, el cual consiste en acciones que están coordinadas a nivel del sector público y privado acerca de los puntos que tienen que ver con la puesta en práctica de un catálogo de diversos delitos cibernéticos.

En los antecedentes nacionales se tiene lo siguiente:

Villavicencio (2014) tuvo como objetivo determinar la territorialidad cuando se comete un delito informático ya que el ciberespacio no presenta suficiente permanencia utilizo una investigación un enfoque cualitativo de tipo no experimental. Concluyo su investigación la ley de delitos informáticos tiene como objetivo luchar contra los actos tendientes a menoscabar los sistemas y datos informáticos, la confiabilidad de las comunicaciones, actos que tienen como fin disminuir el patrimonio, la fe pública y el menoscabo de la libertad sexual, delitos que son realizados a través de la ayuda de la tecnología.

Arellano (2022) estableció como objetivo determinar cuáles son las deficiencias legislativas en la Ley N° 30096 del cual utilizo una investigación un enfoque cualitativo de tipo no experimental , concluyo que el fraude informático una conducta que se encuentra regulado por un agente especializado en tecnología, afianzándose de métodos informáticos con uso a internet como medio de consumación del delito, así como por medio de la obtención de datos personales, a fin de violar el derecho a la intimidad y privacidad, a través obtención de los datos personales mediante diferentes fraudes informático con el propósito de causar daño patrimoniales a persona o empresas a través de cuentas bancarias o aplicativos análogos digitales.

Monja Esquivel (2022) tuvo como objetivo abordar e investigar los delitos informáticos enfocándome en el tema de Suplantación De Identidad en las entidades Bancarias Bancos, se utilizó una investigación cualitativa del tipo descriptivo y se concluyó que los delincuentes constantemente están en la búsqueda de burlar los sistemas de seguridad que protegen la identidad de las personas, para ello se las ingenian para apropiarse de manera ilegítima de la información de las personas y para ello lo hacen a través falacias o embustes tendientes a generar error en las víctimas, todo ello se conoce con el nombre de robo de identidad. Este fenómeno está siendo usado en las páginas de internet, los criminales inducen a error a las víctimas con el objetivo de hacerlos vulnerables y esto se debe al poco conocimiento que tienen los clientes acerca de los temas de fraude informático.

Lujan (2022) tuvo como objetivo general analizar el ámbito jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021, su investigación es de enfoque cualitativo, de tipo fenomenológico se concluye la investigación que para tener efectividad para el tratamiento penal se debe tener un marco legal que continuamente se está actualizando ya que las modalidades de este delito, también irán cambiando, por ello es preciso que los operadores de justicia desarrollen capacidades especializadas en informática que permita un mejor manejo.

Huamanñahui y Gamboa (2022) tuvo como objetivo realizar una revisión sistemática exhaustiva de la investigación sobre las aplicaciones móviles que ayudan a prevenir los delitos informáticos. Su enfoque de investigación es mixto y su tipo de estudio es sistemática porque va de lo especifico a lo general, llega a la conclusión ha conseguido identificar y analizar cuáles son las técnicas más utilizadas para la detección de delitos informáticos, la clasificación de los delitos informáticos, las palabras más utilizadas en los artículos, las palabras clave más utilizadas, los artículos más citados y los autores que presentan concurrencia. en su investigación a partir de las preguntas de investigación planteadas y analizadas con la revisión sistemática de literatura entre 2017 y 2021 en varias bases de datos. Estático, Machine Learning, Minería de datos, Red neuronal, Deep learning, Red neuronal de lógica difusa, Técnicas de visión artificial, Técnicas biométricas, Criptografía, Herramientas forenses, Cifrado de red, Proxies, Cortafuegos y Seguro de responsabilidad civil cibernética. La técnica más utilizada es el aprendizaje automático.

Los bancos en la actualidad se han ido convirtiendo en móviles, con relación a los aplicativos bancarios (APP) que sirven para otorgar servicio de distintos tipos operaciones económicas, siendo así que la Banca Móvil se le considera “una de las principales revoluciones tecnológicas con relación a los clientes”. Este modelo de servicios genera que los clientes puedan realizar cualquier tipo de transacción financiera de su casa, siendo el único requisito contar con un celular que tenga el aplicativo que cuente con internet. (Leão, Brantes, Sanibo y Werneck ,2018)

La generación llamada Millennials y Centennials poseen un desarrollado manejo financiero, por lo que, requieren la utilización de los servicios financieros mediante aplicativos móviles bancarios (Banca Móvil) o medios virtuales. Además, sostienen que cerrando la brecha digital los países y regiones se han desarrollado a través de los procedimientos de pagos móviles. (Bermeo, Valencia, Duque, Garcés y Luna,2019)

Los delitos cibernéticos o informáticos son acciones que transgreden y afectan a los cibernautas causados por criminales que se encargan de robar información secreta de los clientes con el fin de manipularla y sacar provecho de aquella información. El modo como actúan estos delincuentes está en función en base al nivel instructivo y métodos de convencimientos que ellos usan, todo ello a través de correos ficticios de entidades bancarias, links de páginas inexistentes, recompensas destinadas en a hacer caer en error, virus, entre otros. Los delitos informáticos implican engaño, fraude, robo extorsión y otros tipos de delitos asociados. (Almenar Pineda, 2017)

En el Derecho penal no se tiene un concepto generalizado acerca de los delitos informáticos, se considera que este tipo de delitos son aquellos en los que para lograr su comisión se utiliza un sistema automático de procesamiento de datos o de transmisión de dato con lo que excluye la existencia de un nuevo interés social. Existe una segunda opinión doctrinal el cual hace una distinción de ambas situaciones, esto es, en primer lugar, la utilización de la informática como medio innovador que vulnera bienes jurídicos que ya están protegidos en clave penal, esto es el “delito computacional”, mientras que en segundo lugar clasifica aquellas acciones que vulneran un nuevo interés social. (García Cantizano, 2012)

El delito informático, señalando son aquellas conductas típicas, antijurídicas, culpables y punibles, en las que la computadora, sus técnicas y funciones ejercen un rol fundamental, ya sea como método, medio o fin en el resultado de los fines ilícitos del sujeto activo, estos es lograr un beneficio propio ocasionando un daño económico al sujeto agraviado. Asimismo, estos tipos de delitos pueden ser conceptualizados como aquella conducta típica, antijurídica, culpable y punible en

la que el sujeto activo del delito emplea cualquier medio informático con el fin de alcanzar un provecho ilícito en detrimento de la víctima. (Salinas Siccha,2008)

La víctima más usual del delito informático es la persona jurídica, esto se debe al intercambio económico en la cual llevan a cabo sus actividades, esta es la razón por la cual son los grupos más perjudicados por los delincuentes a través del uso de computadoras, los cuales son: el ámbito bancario, las instituciones públicas, la industria de transformación, etcétera. (Gutiérrez Francés,1991)

Hay tres factores que contribuyen al aumento de los casos de fraude cibernético. El primero es el factor de anonimato, que permite a los delincuentes operar sin ser detectados hasta que es demasiado tarde para que las autoridades averigüen quién es el responsable del fraude. La siguiente explicación del aumento de los delitos de fraude cibernético es la jurisdicción. Esto se debe al hecho de que los delitos cibernéticos dificultarían que las autoridades judiciales determinen el lugar donde se llevará a cabo el procedimiento legal. La ausencia de cooperación jurisdiccional entre naciones, como las del sudeste asiático, América del Sur y África, es uno de los factores que hace que la aplicación de la ley esté sujeta a límites y le da a este carácter el nombre adicional de "sin fronteras". (Hayes al.,2015)

Los ciberdelincuentes recopilan información mediante phishing y spoofing donde el impostor utiliza la información de la víctima sin su consentimiento. El phishing se define como el envío de correos electrónicos innecesarios a clientes corporativos de diferentes instituciones manipulándolos para que compartan la información de su cuenta personal a través de sitios web falsos (Hassan et al. 2012)

El phishing como una actividad fraudulenta que incluye la invención de una copia de una página de internet ya creada con el fin de inducir en error a un cibernauta y que producto de ello logre enviar sus datos personales, financieros o de contraseña. El phishing es un intento de engañar a un usuario para que revele información privada, tales como sus datos personales de sus cuentas bancarias y tarjetas de crédito, mediante el envío de enlaces maliciosos que los llevan a un sitio web falso. Algunos afirman que los correos electrónicos son la única vía de ataque.

Las personas comparten más información personal en línea debido al aumento sustancial en el uso de Internet. Como consecuencia, los ciberdelincuentes ahora pueden acceder a una gran cantidad de datos personales y transacciones financieras. El phishing es un ejemplo de un tipo de delito cibernético muy eficiente que permite a los delincuentes engañar a los usuarios y tomar datos cruciales (Alkhalil al.,2021)

Aplicativo Bancario, se le denomina al servicio que es proporcionado por un banco que utiliza un sistema informático y que para su operatividad es necesario instalar un aplicativo en el dispositivo celular, cuya función financiera es la de realizar pagos, transferencias, entre otros. (Leão, Brantes, Sanibo y Werneck, 2018)

Fraude informático se determina por la acción de los ciberdelincuentes por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios. (Iftikhar al, 2021)

Suplantación de identidad, los hackers sustraen la información de los usuarios para utilizarlos en su propio beneficio. Las finalidades para realizar estos actos pueden ser diversas a su vez existen muchas formas de beneficiarse del acceso no autorizado de los datos informáticos. (Hassan et al, 2012)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

La presente investigación es de tipo básico o pura, debido a que tuvo concordancia con el tema “El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos” existe un vacío legal frente al tema planteado, Por lo tanto, se facilitó el análisis y la formulación de nuevas teorías es así como se obtuvo nuevos estudios y modelos de investigación de la realidad problemática. la investigación básica tuvo como fin proponer nuevos conocimientos científicos que se orienten al entendimiento del problema social. (Hernández –Sampieri, 2014)

Por otro lado, el diseño es teoría fundamentada debido a que buscó recopilar conocimientos existentes e información de teorías sobre el tema de estudio que este caso vino a hacer “El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos”, lo que se busco fue describir y explicar, mediante el análisis inductivo con el fin que se establecio una teoría determinada del objeto de estudio. (Hernández –Sampieri, 2014)

3.1.2 Diseño de investigación:

hizo referencia al plan o estrategia concebida del cual se obtuvo la información que se deseó, la teoría fundamentada consistió en obtener información que corresponda a la categorías y subcategorías a fin de construir nuevas teorías, conceptos a partir directamente de los datos obtenidos en la encuesta, por lo cual se menciona que se desarrolló inductivamente porque parte de un conjunto de datos que en un primer punto no había una explicación al fenómeno estudiado respecto a los efectos jurídicos de la aplicación normativa y doctrinaria de la institución jurídica aplicativos bancarios y delitos informáticos contra el patrimonio en el contexto nacional y derecho comparado.(Hernández- Sampieri, 2014)

3.2 Categorías, Subcategorías y matriz de categorización:

En la presente investigación está conformado por categorías, subcategorías y criterios, (Hernández- Sampieri, 2014)

se detalla en la siguiente:

Tabla 1

Categoría

Categorías	Subcategorías	Criterio 1	Criterio 2
Aplicativos Bancarios	Banca Móvil	Aplicaciones instaladas en el smartphone	Token digital
Delitos Informáticos	Fraude Informático	Hacking	Phishing
	Suplantación de Identidad	Robo de identidad	Suplantación digital

3.3 Escenario de estudio:

El problema de investigación se encuentra en el territorio peruano, porque la causal es uso de aplicativo bancarios para arremeter contra las victimas en los delitos informáticos ya que se encuentra normado en una ley especial Ley Nº 30096.

El escenario de estudio tiene tres enfoques para su descripción partiendo como primer punto el escenario de la fiscalía de ciberdelincuencia ya que, al ser, la única fiscalía a nivel nacional se obtendría un análisis completo de la problemática de nuestra investigación. Como siguiente escenario se tiene la DIVINDAT que es la unidad de investigación de alta tecnología en el cual se obtendría la parte operacional de problema de investigación debido al ser una ley especial, se podría

obtener información como se opera la problemática, como ultimo escenario se tiene el aspecto jurídico desde la perspectiva de los litigantes penalistas los cuales ayudara al trabajo de investigación para obtener un mejor resultado.

3.4 Participantes:

Tabla 2

De participantes

N/O	Apellidos y Nombres	Grado Académico	Cargo	Institución	Años de Experiencia
	Ángel Ubaldo Gonzales Farfan	Magister	Fiscal Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro	Ministerio Público	20 años
	Alan Roldan Araujo Chavez	Magister	Jefe de la Unidad Fiscal Especializada en Ciberdelincuencia	Ministerio Publico	5 años
	Benji Gregorio Ramos Espinoza	Magister	Abogado penalista	Estudio Jurídico Espinoza	14 años
	Albaro Martín Román Arroyo	Magister	Abogado Penalista	Catedrático	8 años
	Luis Edgardo Huamán Santamaría	Coronel PNP	Coronel PNP jefe de la DIVINDAT	Coronel	18 años
	Hegel Covarrubias Maihua	S1 PNP	S1 PNP de la DIVINDAT	Superior de Primera	7 años

3.5 Técnicas e instrumentos de recolección de datos

La presente investigación tuvo como finalidad la recopilación de información necesaria para la obtención de resultados. Por lo cual, se aplicó la técnica de la entrevista, y se basó en la realización de una guía de entrevista que implico relacionar las preguntas con los objetivos de la investigación, por ello se tomó las opiniones obtenidas de los expertos, que consistió en recibir distintas criterios e informaciones de profesionales especializadas en la materia. (Arnau y Sala, 2020)

Tabla 3

Validación de instrumentos – Guía de entrevista

Instrumento	Datos generales	Cargo o Institución	
Guía	David Saul Paulett Huayon	Docente UCV-Lima Este	Aceptado
De	Luis Edison Molocho Vega	Docente UCV-Lima Este	Aceptado
Entrevista	Juan Manuel Ñiquen Quesquen	Docente UCV-Lima Este	Aceptado
	Manuel Moises Valdivia Cotrina	Docente UCV-Lima Este	Aceptado

3.6 Procedimientos:

La presente investigación se realizó con la recolección de información, siguiendo el siguiente procedimiento: Como primer punto se determina la rama del derecho que se realizó en el estudio en este proyecto en este caso fue derecho penal, luego se formuló el tema deseado el cual se presentó a la asesora para su aprobación, una vez obtenida la aprobación se identificó el problema general, específicos al igual que sus respectivos objetivos posterior a ello se recopiló de los artículos científicos, tesis nacionales como internacionales, que guarden relación con la categorías y subcategorías. Al igual que las teorías, conceptos generales con ello se desarrolló el marco metodológico que consta de tipo, diseño, enfoque de investigación, escenario, procedimientos. Para concluir con los aspectos

administrativos, detallando los recursos y presupuestos de la presente investigación.

Con todos estos procedimientos se puedo obtener como resultado la matriz de constancia, la elaboración de las preguntas para la entrevista ya que se logró concretar y delimitar el tema en base a la categoría y subcategoría en torno a los objetivos.

3.7 Rigor científico:

Para el presente trabajo de investigación, con ayuda de los objetivos se corroboro el rigor científico, ya que el instrumento debe tener relación con los objetivos, los cuales deben tener credibilidad, debido a que se busca la aproximación de los resultados de la investigación en base a la problemática, se entiende por transferencia a todo aquello que se deprende que cada investigación por tal motivo se dice que es autónoma por tanto no se puede generalizar para cada investigación se transfiere información para obtener otros resultados, en cuanto con relación a la dependencia se menciona que es complejo por lo cual dificulta estabilidad de los datos ya que cada trabajo no se puede replicar exacto y por último se menciona que conformabilidad que se basa en que los resultados de la investigación debe garantizar la veracidad de las descripciones realizadas por los participantes, por ello la entrevista la cual será validados por cuatro expertos de los cuales se debió cumplir con el porcentaje que garantizo su viabilidad de este, siendo aprobados. (Hernández et al., 2014)

3.8 Método de análisis de la información:

Para la presente investigación el método para la recopilación de datos se realizará mediante la aplicación de la triangulación debido a que implica la combinación de múltiples fuentes de información con el fin de obtener una comprensión más integral e imparcial de la realidad que se está estudiando. Este enfoque permite verificar los hallazgos y disminuir posibles sesgos, codificación abierta, se tiene al aporte de la norma y el participante con relación al trabajo,

codificación axial se debe a los conceptos obtenidos que contribuyen a los resultados y codificación selectiva aportes de los participantes que se basaron para decir el trabajo. (Hernández et al., 2014).

3.9 Aspectos éticos:

El código de Ética de investigación de la universidad Cesar vallejo, tuvo como pilar fundamental, crear en sus estudiantes, jóvenes investigadores con honestidad y responsabilidad, capaces de cumplir con la buenas prácticas para lograr promoción de principios éticos, para ello se debió cumplir estándares de rigor científico a su vez se protegió el bienestar del alumnado y la propiedad intelectual, con ello se evitó el plagio de manera total.(Consejo Universitario de la Universidad César Vallejo, Resolución 0470-2022).

IV. RESULTADOS Y DISCUSIÓN

El presente capitulo tuvo como finalidad describir los resultados obtenidos con la utilización del instrumento de recolección de datos el cual fue la entrevista, por lo cual se necesitó participante de los diferentes campos operarios, para poder responder con a la interrogantes a fin que responder los objetivos general y consecuentemente los objetivos específicos, y así poder determinar si el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos para ello se realizó la siguiente pregunta:

Tabla 4

Resultados de la pregunta 1

Pregunta n.º 1 Desde su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos?

PARTICIPANTE	RESPUESTA
Araujo	Bueno en primer lugar los ciberdelincuentes buscan diferentes manera captar los datos sensibles que vendrían a ser datos personales, datos referentes a estos aplicativos móviles a fin de que puedan acceder a los mismos y de esta manera llevar o conseguir los fines delictivos con el presente caso sería el tema de delito informático, eh lo común en este tipo de casos y lo que se presenta en la lo cotidiano este que estos delincuentes a través de diferentes formas como son las llamadas telefónicas mensajes de texto correos electrónicos buscan captar el tema de los datos de estas cuentas o estos aplicativos instalan en los dispositivos móviles y ya con estos datos pueden realizar los diferentes actos delictivos no como en el presente caso o con la mayoría de casos el presente es el delito de fraude informático
Covarrubias	El uso de la tecnología está haciendo escalable, está siendo masificado, no limita por ejemplo el uso de las personas para ese aplicativo no, más que todo se debe colocar en el tema de la medida de seguridad que debe tener cada persona en el uso de la tecnología y aplicación de ciertas medidas de seguridad como la contraseña segura no o cuando enseñas que no son fáciles fácil de adivinar por ejemplo he visto usuarios que utilizan claves secretas como su fecha de nacimiento porque la

aplicación para hacer transacciones le piden 6 dígitos pero el cajero la ATM te pide cuatro dígitos y normalmente ponen fecha de nacimiento 1984 ,1983 o cuatro veces cero o cuatro veces 1 y esa es una falla bastante grave entre las prácticas de buena seguridad es decir de seguridad en la clave de 6 dígitos que piden para transacciones en internet banca móvil Banco por internet he visto que esta aplicación este contraseñas decir dígitos pero 123456 que es lo más común, los delincuentes informáticos lo saben y esa es la vulneración y es por eso que el usuario es el eslabón más débil en una cadena de lo que es la ciberseguridad tratándose de buscar el error del usuario.

Espinoza Los usuarios de aplicativos bancarios que son víctimas de delitos informáticos se ven perjudicados económicamente, además no solo son víctimas de sustracción de dinero sino también de sus datos informáticos y personales que podrían ser utilizados para otros delitos.

Gonzales Bueno, de qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos, principalmente y partir de la experiencia aquí de las investigaciones que se dan, puede ser por dos motivos en primer lugar por un mal uso y segundo lugar por algo que es ajeno a ellos, porque sufren la pérdida o el extravió o robo del equipo de alguna manera se pueden exponer, pero de qué manera perjudica, prácticamente eso, en la indebida utilización le puede perjudicar, pero de allí no le encontraría otras razones de momento, cuando hablo del uso indebido lo indico porque pueden cometer desde el inicio del error por no bajar el aplicativo correcto, de pronto pueden ser víctima de un phishing evidentemente

Huamán Es una repuesta muy lógica los perjudica de forma económica su patrimonio se ve vulnerado porque estos delincuentes se hacen a sus cuentas y prácticamente le sustraen el dinero que tienen su cuenta de ahorro.

Román	Los exponen una manera casi ilimitada porque lo que suele suceder a través de estos aplicativos es que, corrompiéndose las claves o los accesos de los clientes de las personas naturales, hay delincuentes mafias que están enquistadas que se encargan de entrar a estos aplicativos y hacer operaciones sustrayendo dinero de las cuentas de ahorro de las tarjetas de crédito operaciones digamos de a otras empresas inclusive creadas de manera forzada para desviar estos fondos económicos de los clientes no entonces me parece que la situación es bastante delicada y que las entidades financieras tampoco toman ciertamente los controles mínimos indispensables para proteger a los clientes

Tabla 5

Resultado de la pregunta 2

Pregunta n.º 2 En su opinión ¿Por qué los clientes financieros han optado por el uso de aplicativos bancarios instalados en el smartphone?

PARTICIPANTE	RESPUESTA
Araujo	Evidentemente por la rapidez del servicio que les ahorra tiempo he y les hace las operaciones más rápidas, la innovación de utilizar la tecnología para una operación bancaria es innegable que es muy útil a nivel mundial entonces qué duda cabe que el propio uso se justifica por eso ahorra tiempo, que halla todo en ese espacio un tema de mal uso y niveles de seguridad que podría darse en cada caso puntual que lo hace más o menos riesgoso eso es otra cosa.
Covarrubias	Es de fácil uso, el celular lo tienes todo el tiempo a tu lado y tienes cierta confianza porque es un equipo que tienes en tu poder entonces si quieres hacer una transacción bancaria o una compra por internet o lo que tu gustes hacer, entras al aplicativo pon tu contraseña y puedes transacción sin tener que desplazarte un Banco o a un agente y te facilite las cosas bastante.
Espinoza	La gran mayoría opta por este aplicativo porque permite controlar todo desde nuestro celular y se nos hace más práctico realizar los pagos de servicios, transferencias de dinero, etc.

Gonzales	Evidentemente por la rapidez del servicio que les ahorra tiempo he y les hace las operaciones más rápidas, la innovación de utilizar la tecnología para una operación bancaria es innegable que es muy útil a nivel mundial entonces qué duda cabe que el propio uso se justifica por eso ahorra tiempo, que halla todo en ese espacio un tema de mal uso y niveles de seguridad que podría darse en cada caso puntual que lo hace más o menos riesgoso eso es otra cosa.
Huamán	Este es parte del avance de la tecnología del mundo globalizado ya no se quiere ir a las ventanillas para de los bancos para hacer una gestión física y de transferencia de dinero para retirar y como para también ahorrar no todo se hace a través del sistema se tecnológicos que facilitan la vida del hombre, pero también a facilitar la vida al hombre y constituyen una amenaza porque puede ser aprovechado por los delincuentes criminales cibernéticos para poder ingresar los aplicativos y como te fraude informático.
Román	Bueno debo asumir que igual que cualquier otra persona por el mismo acceso a la tecnología la facilidad y el ahorro el tiempo que se genera a través de estos aplicativos y que evitan muchas veces tener que desplazarse al Banco.

Tabla 6

Resultado de la pregunta 3

Pregunta n.º 3 Desde su perspectiva. ¿Qué factor ha influenciado para que se incremente el delito informático?

PARTICPANTE	**RESPUESTA**
Araujo	En realidad sería el desconocimiento que tienen las víctimas respecto al cuán delicado es compartir los datos personales respecto a sus aplicativos, sus datos personales este es el factor primordial para que los ciberdelincuentes quieran realizar este tipo de delitos el poco conocimiento que tiene respecto a la comisión de estos delitos, es común inexperiencia se ve de que solamente con una llamada telefónica sin la víctima previamente haberse informado tener certeza respecto a que se está comunicando con personal de por ejemplo una propia entidad bancaria comparte y datos sensibles no claves autoritativas token digital entre otros

	datos que permiten la realización de este tipo de delito y Así mismo debemos de tener en cuenta que en la actualidad también este ya los delincuentes no solamente por ejemplo en la organización de delitos comunes como son los robos hurtos ya no solamente lo realizan con la finalidad de poder obtener sus dispositivos móviles no sino el de acceder a estos aplicativos que vienen siendo instalados en los móviles esto con la finalidad de poder tener un mayor acceso al respecto al contenido patrimoniales de su víctima
Covarrubias	Después de la de la pandemia por Covid19 se masificó el uso de la tecnología recordemos que la pandemia las personas tuvieran encerradas y no podían comprar y si quieren comprar ropa o que quieran continuar estudios desde su casa empezaron de manera forzada a hacer uso de tecnología y realizaban compras por internet sus pagos de servicio por internet sus pago de cursos este académico por internet recibían las clases por internet entonces digamos esa situación de la pandemia empujó la sociedad peruana hacia este el uso de las nuevas tecnologías, porque anteriormente la gente era muy reacia a la tecnología yo recuerdo que mi papá se iba al hacer cola para el servicio de luz no le gustaba pagar por internet no le gustaba para poder por aplicativo pesar que lo iban a engañar cuando ya no pudo hacer cola ni siquiera había atención en los servicios básicos entonces la única manera era hacer los pagos por internet entonces digamos que la pandemia los empujó la sociedad peruana hacia el uso de la tecnología.
Espinoza	Uno de los factores que influye mucho para el incremento de este delito es la falta del reporte, las victimas de estos delitos no siempre ponen en conocimiento a las entidades bancarias, del mismo modo, los bancos o empresas no reportan estos delitos por temor a una pérdida reputacional que lleve a la pérdida de clientes y por otro lado se tiene la dificultad para poder rastrear estos delitos.
Gonzales	Principalmente creo yo el descuido ya se cómo le indicaba yo por quizás hacer una descarga de la app incorrecta, ser víctima de phishing o principalmente compartir demasiados datos, es decir estamos acostumbrados a entregar nuestros datos de tal manera que no medimos los riesgos y la consecuencia nos tomamos una foto o hacemos una selfi estoy en el banco pagando y lo cuelgo en el Facebook y quien me hace ingeniería social, empieza a trazar que tipo de cliente son y se dan cuenta soy un cliente que maso menos promete tener buenos ingresos, porque a

	cada rato cuelgo mis fotos que trabajo en un minera o que soy un próspero comerciante, que estoy en la puertita del banco y justo es un banco conocido, poco a poco voy copilando información que de alguna manera me puede exponer, me pude mostrar los datos que se supone cualquier persona no sabría fácilmente a esto le sumamos el hecho que de pronto no llevar este buena medidas lo es ciberseguridad lo que es clave, no tener claves sólidas, que al repetir las claves, entonces son varios factores que de alguna influyen por más que el aplicativo sea muy bueno el problema siempre es el uso.
Huamán	Mira acá tiene que ver la teoría el fin de la pena no previsión general, la prevención especial acá lamentablemente las penas para este delito son mínimo 8 años y son considerados como delitos no violentos entonces se hace que las autoridades el Poder Judicial como también de misterio público y no le dan la importancia del caso no la misma sociedad no lo ve tan grave más caos impacto una persona que es víctima de un robo de un celular en forma violenta en la calle un asalto a mano armada en El Mundo físico que un delito que se comete en el ciberespacio, se equipara como los delitos de cuello blanco donde no hay violencia pero sí el delincuente tiene mucha astucia porque se esconde las redes en el ciberespacio su dificultad para ubicarlo es ese notorio.
Román	La facilidad con la que se puede hoy en día tener acceso a estos aplicativos informáticos es básicamente también la consecuencia de que estas operaciones esos delitos se comentan cada día más, cualquier persona con un celular y con una conexión a internet fácilmente puede descargarse el aplicativo y eso por parte de digamos de la persona natural del cliente, por parte de los bancos que también muchos se han puesto en la línea si no son todos de tener estos aplicativos y estos aplicativos a su vez me parecen hola bastante delicados porque por ejemplo en el Banco BCP en el Banco scotiabanck en estos dos aplicativos puedes tramitar préstamos sin necesidad de tener que desplazarse al Banco y firmar no hacen los controles debidos.

Análisis Convergente:

De los participantes se pudo obtener por medio de la entrevista que el perjuicio sufrido por los clientes en el uso de aplicativos bancarios en los delitos

informáticos sería el fin patrimonial ya que el principal propósito de los ciberdelincuentes fue obtener su información digital con el fin de sustraer todos los ahorros de su posible víctima, sumado al hecho de que estos aplicativos son los de mayor utilización ya que su uso es de relativa facilidad y esto ha generado el incremento de este tipo de delito.

Análisis Divergente:

Los participantes sostuvieron que el perjuicio se origina por el deficiente uso en cuanto al manejo del cliente respecto a los aplicativos bancarios, uno de estos factores es debido a la instalación de un aplicativo de dudosa procedencia; otro factor que da origen al perjuicio seria que el nivel mínimo de seguridad que los cliente (contraseñas) que los clientes le otorga a sus dispositivos, los ciberdelincuentes hacen ingeniería social, es decir dejan una ventana abierta, al exponer su vida en las redes sociales, lo cual los hizo blancos más fáciles de este tipo de delito.

Codificación:

Después de los resultados de las entrevistas se optado por desarrollar la codificación abierta, axial y selectiva del objetivo general. Como primer punto tenemos a la **codificación abierta**. Si bien la categoría de delitos informáticos se encuentra en una ley especial N° 30096, los participantes han dicho que lamentablemente las penas para estos delitos son mínimas y son considerados como delitos de cuello blanco, por tal motivo al no darle la importancia del caso, la misma sociedad no lo ve tan grave y desconoce del tema. De los conceptos obtenidos contribuyen en la elaboración de la **codificación axial**, Se tiene que la extracción de la información de los aplicativos bancarios se utilizó con el fin de obtener un beneficio patrimonial en desmedro de patrimonio de los clientes dentro de sus cuentas bancaria, lo cual se encuentro contemplado en la ley especial N°30096 el cual no está siendo bien valorada según los participantes y esto se debe al desconocimiento de la víctima y falta de una sanción más drástica. Como último punto tenemos a la **codificación selectiva**, La ley de delitos informáticos tuvo como objetivo luchar contra los actos tendientes a menoscabar los sistemas y datos

informáticos, la confiabilidad de las comunicaciones, actos que tuvo como fin disminuir el patrimonio (Villavicencio, 2014)

Tabla 7

Resultado de la pregunta 4

Pregunta n.º 4 En su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en el fraude informático?

PARTICPANTE	**RESPUESTA**
Araujo	En realidad el uso de aplicativos bancarios es una ventaja para los consumidores es una ventaja para los clientes no que te permite como ya te expliqué anteriormente realizar diferentes actividades diarias con mucha más rapidez antes era necesario para realizar el pago de un servicio que tengamos que acudir propiamente al Banco de acudir a los agentes para poder realizar estas actividades sin embargo con la globalización ha permitido de que se puedan incrementar tecnologías de información comunicación y de esta manera poder realizar este tipo de actividades de manera mucho más rápida en cuestión de minutos y segundos, como en todo como en toda implementación siempre vamos a correr bien y en ese sentido la modernización de respecto a la posibilidad de realizar diferentes actividades bancarias a través de los aplicativos móviles o aplicativos digitales a conllevado a incremento de este tipo de delitos dentro de información antes solamente se cometió este delito con poca afluencia en vista que solamente podías realizar estas actividades entras en internet por banca por internet por banca por internacionalmente realizada sin embargo con el tema de haberse implementado los aplicativos bancarios o los aplicativos móviles ya el fraude informático se ha incrementado.
Covarrubias	Eso es muy complejo responder porque no es tanto por la aplicación móvil ó el de la página web no le van a publicar Internet es más que todo que la persona cae en el engaño por ejemplo una campaña de fishing o su contraseña es débil o si no instalan una aplicación de tipo Maxwell en el celular sin que se dé cuenta y diferentes factores no es generalmente por el tipo de aplicativos más que todo por el nivel de seguridad que el usuario aplica en sud transacción de sus operaciones en este medio virtual.

Espinoza	Primero, los usuarios se ven perjudicaos porque alteran sin autorización los datos ingresados y realizar malversación de los fondos o ahorros, asimismo, los estos sujetos pueden alterar o borrar información almacenada.
Gonzales	Para el caso de fraude informático, el uso del aplicativo no lo perjudica quiero dejar de manera puntual, el aplicativo esta hecho de tal manera que sirve, el error de alguna u otra manera, siempre va estar en el usuario, sí es posible que de pronto se pueda advertir diferencias entre un banco y otro, en la medida en que tipo de medida de seguridad se toma para acceder unos usan token en otro código, hay aplicativos que no son tan buenos y demoran otros son muy veloces entonces son factores que si bien es cierto existen pero eso de pronto considero yo no desdicen no este se echan y descartan la efectividad del aplicativo el problemas siempre a veces es como escudo la falta el excesiva confianza y lo que indicaba el exponer siempre nuestros datos nos hacen víctimas de los ciberdelincuentes así que si el uso es si el aplicativo perjudica no estoy muy seguro no creo que sea.
Huamán	Lo perjudica de forma económico y aparte de eso de que ya una persona que ha sido objeto ya de fraude ya deja de confiar en el uso de tus aplicativos y las empresas también que se dedican a realizar estos aplicativos deben mejorar su sistema de ciberseguridad a finde evitar que personas ajenas al sistema ingresen sorprendan a sus clientes , es fácil que el cliente busque alternativas no a ver que diga que financiera es la mejor la que tiene mejor sitio de seguridad a fin de repente cambiar de entidad financiera, esa es la forma que perjudica a los lientes en lo que es fraude.
Román	Un poco hemos dado respuesta en la primera pregunta que es este endeudamiento al cual algunos clientes no son todos se ven expuestos a que se cometan estos actos delictivos informáticos

Tabla 8

Resultado de la pregunta 5

Pregunta n.º 5 ¿Cree usted que el hacking perjudica a los clientes en el uso de aplicativos bancarios	
PARTICIPANTE	**RESPUESTA**
Araujo	Si es normal se ve en la experiencia en la praxis de que al momento de que por ejemplo las víctimas de estos delitos no saben de la forma cómo se había cometido el mismo indican de que en todo momento han tenido

	acceso a su tarjeta bancaria nunca han compartido sus cuentas nunca han compartido ningún tipo de información respecto a sus aplicativos bancarios por los datos sensibles de datos sensibles personales tarjetas bancarias sin embargo al momento de que se realiza por ejemplo un tema de un análisis digital forense respecto a los dispositivos electrónicos donde estarían instalados aplicaciones bancarias vinculadas a sus cuentas bancarias se advierte de este la existencia diferente software o este malware que tendrían como finalidad la captación de los datos de los aplicativos en ese sentido al momento que se obtiene dicha información y le preguntas a la víctima hoste de qué manera has habría podido este instalarse dicho malware en dicho los agraviados indican Ah no es que si en alguna oportunidad de ingresar a una página de dudosa y es en sentido ya se tiene mayores detalles respecto a la forma de cómo el ciberdelincuente habría captado los datos sensibles de cuentas bancarias o datos personales los cuales son utilizados para la realización de estos delitos de fraude informático
Covarrubias	Depende hay pruebas de penetración a sistemas informáticos mide el nivel de seguridad de un sistema informático y orientado correctamente nos ayuda a los administradores sistema al terminar el nivel de seguridad de un sistema entonces por ese lado correcto y es necesario sin embargo un ataque hacking con la finalidad de obtener información confidencial del usuario de forma fraudulenta montos económicos en agravio del usuario obviamente es perjudicar y esa actividad están penadas.
Espinoza	Definitivamente, los hackers son un grupo de personas que obtienen el acceso no autorizado a diversos sitios web aprovechando vulnerabilidades existentes y comprometen los dispositivos digitales.
Gonzales	Claro que sí. Es decir si la pregunta es el hacking perjudica a los clientes claro pero más que el hackeo no hablamos tanto de un hackeo si investigamos un poco más allá en hackeo implica todo un trabajo muy especializado no necesariamente para justo dar con las claves o los datos cualquier usuarios del aplicativo el hackeo es más que eso es algo técnicamente más complicado aquí más de una u otra manera lo que se hace es ingeniería social y pues finalmente bueno usted está tocando el tema de fraude no la estafa puede de alguna manera pueden conseguir algún tipo de dato pero no sé si el hacking en si tenga que ver directamente con este tipo.

Huamán	Lógico un hacking es una actividad que lo realiza un delincuente cibernético a fin de sustraer el dinero de sus víctimas a través marwell, ingería social para poder ingresar a obtener las credenciales del cliente y poder prácticamente vaciarle sus cuentas de esta manera lo perjudica de manera económica y se beneficia la persona que hace el hacking
Román	Por supuesto digamos la manera más tradicional el hacking de intervenir las cuentas o los aplicativos y perjudicar a los clientes.

Tabla 9

Resultado de la pregunta 6

Pregunta n.º 6 En su opinión ¿En qué medida el uso de aplicativos bancarios puede considerarse un canal seguro para realizar operaciones bancarias?

PARTICIPANTE	**RESPUESTA**
Araujo	Tiene que haber un trabajo conjunto de prevención más que todo por parte de las entidades bancarias nivel nacional con la finalidad de poder sensibilizar a los consumidores o clientes respecto a lo delicado que es compartir los datos de sus cuenta bancaria o uso de sus aplicativos móviles en la realización de cualquier actividad cualquier transacción que pretenda realizar a través de los aplicativos más que todo es un tema de prevención y también tiene que ser un trabajo articulado por parte también del Estado también tiene como como finalidad salvaguardar a la personas y en ese sentido a los clientes de las diferentes entidades bancarias del país es un trabajo de prevención que tiene que ser articulado entre la empresa privada y sector público ya que con la prevención se va a disminuir y es mi perspectiva de la comisión de estos delitos
Covarrubias	El aplicativo bancario tiene un nivel de seguridad altos no estamos hablando de algo básico tienen este exige una contraseña de 6 dígitos de existe una validación del equipo antes de vincularse con la tarjeta, existe un toquen en virtual que se hizo para la autenticación del de la operación bancaria no puedo no podemos afirmar que sea una medida de seguridad básica, es una medida se seguridad bastante segura avanzada. el problema es el usuario cague en engaños y proporciona digamos su token de transacción o toquen validación mediante una campaña de fishing , cae en el engaño y proporciona este tipo de datos que son de único y exclusivo uso del usuario y en varias oportunidades se ha demostrado el Banco ha

	demostrado que el usuario es quien proporciona a través del engaño porque cayó un engaño en fishing y el mismo proporciona esa información al atacante sin conocimiento pero es víctima de sus propios actos
Espinoza	Bueno, es seguro en la medida que el usuario no entregue información confidencial, hay que tener en cuenta que el banco no llama al usuario para solicitar el código de verificación de la tarjeta (CVV), tampoco el código token, ni los datos para acceder a la cuenta.
Gonzales	En la medida que se realice con las esté las recomendaciones de ciberseguridad correctas tener una buena clave una clave sólida optar por un Banco que tenga una reputación en ciberseguridad buena lo sabemos ahí bancos este que le denominan Banco de vitrina no son bancos que tienen una gran experiencia banco que muchas veces están afiliados a tiendas por departamento o tienen una finalidad específica muy diferentes a bancos que tienen pues mucha experiencia en el sector bancario nacional y que tienen de alguna u otra manera muchísimo más sólida su infraestructura informática entonces puede considerarse seguro sí en la medida en que sepamos qué Banco nos ofrece un buen servicio y cómo nosotros hacemos uso de ese servicio
Huamán	Es una pregunta difícil de responder ,la seguridad en informática en ciberseguridad no es 100% total siempre hay una brecha cada vez que los sistemas se van perfeccionando se tapan los las los parches que solo los huecos la puerta traseras donde puede ingresar un ciber atacante, los ciber atacantes están tratando siempre nuevamente encontrar nuevas formas de ingreso a los sistemas nueva forma de hackear, es una lucha constante entre el bien el mal y lamentablemente el uso de estos aplicativos puede ser seguro un mes dos mes 3 meses.
Román	Yo creo que tendremos que salir un poco del aplicativo de celular tal vez volver a los métodos tradicionales que es el desplazamiento principal al Banco o tal vez a través de computadora que en una otra manera tiene una mayor seguridad, el aplicativo bancario es muy riesgoso porque si pierdo el celular y lamentablemente estas mafias estos delincuentes haciendo uso del hacking intervienen los celulares los aplicativos

---

Análisis Convergente:

De los participantes se tuvo que la forma en el cual el fraude informático perjudica al cliente en el uso de aplicativos bancarios se origina a raíz de que el delincuente alteran sin autorización los datos de la posible victima con el fin de malversar su cuentas por medio de los aplicativos bancarios, además de borrar la información almacenada, y esto se debió a que su contraseña de seguridad fue muy débil o existe un marwell que copia los datos de estos equipos, lo cual es aprovechado por los ciberdelincuentes para cometer hacking que es una técnicas cada vez más sofisticadas, ya que al igual que la tecnología avanza el ciberdelincuente encuentra nuevas formas de apropiarse de la información financiera de los clientes.

Análisis Divergente:

El perjuicio fue de forma económica por lo cual, al sufrir este tipo de fraude, los clientes dejan de confiar en la tecnología es por ellos que se ve que las entidades bancarias cada vez más ofrecen distintos servicios para captar a los clientes que han sufrido de estas pérdidas.

Codificación:

De los resultados obtenidos de las entrevistas se busca desarrollar la codificación abierta, axial y selectiva del primer objetivo específico. Se tiene a la **codificación abierta**, el Fraude informático se encontró en una ley especial N° 30096, en el artículo 8, sin embargo, no se le da importancia requerida pese a que con el aumento significativo que ha tenido la tecnología, no se le está dando la relevancia necesaria por lo cual se estuvo masificando cada vez más este delito. De los conceptos obtenidos contribuyen a la elaboración de la **codificación axial** se tiene que el hacking es una forma de engañar al cliente de estos aplicativos, para poder obtener sus informaciones y poder vaciar sus cuentas esto se deber a la instalación de un aplicativo erróneo o al estudio meticulosos que tiene los ciberdelincuentes con la ingeniería social. Como último punto tenemos a la **codificación selectiva**, sostuvo que esta era digital, todo es más sencillo en las actividades bancarias, sin embargo, deja expuesto para que los ciberdelincuentes puedan acceder a nuestra información y sea más fácil cometerse este delito. (Alkhalil, 2021)

Tabla 10

Resultado de la pregunta 7

Pregunta n.°7 ¿Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad?

PARTICIPANTE	RESPUESTA
Araujo	Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad o sea por el hecho de tener aplicativo bancarios y pueda el ciber delincuente entrar a este a este aplicativo puede llegar a esto a generar una suplantación de identidad al obtener tus cuentas pueden acceder a tu información por ejemplo tus aplicativos bancarios. **creo yo que solamente se configura de fraude informático mas no de suplantación de identidad**
Covarrubias	Yo creo que son dos delitos diferentes porque la finalidad de obtener este la credencial de acceso al Banco a la banca por internet de un usuario es con fines netamente económicos con finalidad de sustraer el dinero más no suplantar la identidad de la persona son delitos muy diferentes y no se vinculan entre ellos.
Espinoza	Bueno, considero que no perjudica a los clientes, solo los expone a estar más propensos a que se les suplante su identidad por la misma naturaleza del delito.
Gonzales	El uso de aplicativos en la suplantación de identidad está vinculado, si está vinculado, sobre todo cuando de pronto ya se pueda acceder a los dado del cliente, logro saber que de pronto el cliente pueda ser una potencial victima luego de hacer ingeniería social y por la brecha de seguridad que tiene algunas operadoras puedo hacer que el número telefónico lo cambien de titularidad, se puede hacer de manera virtual telefónica entonces debido a esa brecha que hay pasan a fraude, de pronto es conocido, “oye me quede sin línea que paso” en esos minutos ya le están vaciando la cuenta, y la persona hasta que se dan cuenta para el carro, o sale del trabajo, recién llama primero antes de llamar al banco llaman a la operadora preguntando qué pasa con mi línea ese teléfono está vinculado aplicativos inmediatamente le están haciendo la transferencia, ahora muchas veces no solo están haciendo transferencia hay personas que aprovechan ello para

	solicitar dinero a los contactos que pueden aparecer ahí se está cometiendo una suplantación de identidad.
Huamán	Bien el delincuente, vamos hacer un recuento de como el delincuente ha ido evolucionando en el campo de los delitos informáticos, por ejemplo hay una modalidad conocida como el TIC transfer en inglés que decirle ladrón transparent qué hacían los delincuentes antes tenían los teléfonos robaban los teléfonos raqueteo salta y robo sustraían de la bolsa de los clientes en los supermercados lo primero que hacían era llevarlo a un mercado negro las Malvinas o mercadillos que hay en los conos vendían los teléfonos para que se han utilizado como teléfono ahora no, ahora lo que busca los delincuentes es sacarle el máximo provecho a toda la información que tienen en el teléfono, tal es así que lo primero que buscan lo delincuentes es el ver si esa persona tiene aplicativos bancarios instalados en su celular y buscan a una persona un metodista un informático que se encarga de buscar la contraseña o ingresar al sistema para el fin de hacer la transferencia es lo que está pasando y como lo hace hoy la fuerza bruta ahí y por bots automatizados que van probando las claves hasta que lo encuentran y otra es que lamentablemente nos falta a nosotros como sociedad tener una cultura de ciberseguridad qué hacemos nosotros ponemos claves fáciles de recordar fáciles de adivinar no ponemos la fecha de nuestro cumpleaños en nombre papá ponemos la fecha de nacimiento el papá y la mamá el hermano el famoso 1234561 delincuentes eso ya saben ingresamos fácilmente, en una oportunidad nosotros encontramos una computadora y un hacker y sus archivos y ellas habían información de clientes de la entidad financiera con los montos que tenían en sus cuentas y con la clave de ingreso de sus cuentas aquí viene la clave es 11111222 ,fecha de cumpleaños ósea fácil de romper
Román	Si duda es una situación constante ver como suplantan a los clientes, mediante esas mafias, estos delincuentes que el hacking.

Tabla 11

Resultado de la pregunta 8

Pregunta n.°8 En su opinión ¿Qué mecanismos de seguridad se debería implementar los bancos y los clientes con aplicativos bancarios para evitar que roben su identidad?

PARTICIPANTE	RESPUESTA
Araujo	**Es que ahí ya no estaríamos ante un delito de fraude informático ahí estaríamos ante un delito de estafa y un delito de suplantación de identidad sería el medio para cometer el delito de estafa.**
Covarrubias	Bueno existen varias medidas que se pueden tomar como campaña de concientización quizás simplemente un una autenticación en dos pasos pero sin embargo creo que la mejor forma de que menos ustedes sean víctimas de este tipo de delitos es que los usuarios conozcan los mecanismos con lo cual este los atacantes los hackers o siguientes eh los engañan y poder detectar a tiempo el engaño o estafa o la campaña de Fishing en la cual está este cayendo y poder identificarlo correctamente y poder evitar la entrega de credenciales de sus accesos al Banco.
Espinoza	Considero que los bancos deberían de implementar programas de prevención ante delitos informáticos y lo más importante que debería hacer es capacitar a los usuarios de aplicativos bancarios.
Gonzales	Como indicaba yo creo que los mecanismos de seguridad principalmente deberían comenzar con el usuario con el cliente el mantener este clave sólidas optar por un Banco que ofrezca más de un nivel de seguridad al momento de acceder llámese una clave un reconocimiento dactilar, facial, token o amarrado a una clave que te envíen a tu correo en ese momento todas esas medidas coadyuvan pero quien las ofrecen determinados bancos ,no todos entonces quieren gastar en eso otros bancos sí pueden ofrecer eso hace al cliente que va a depender mucho ello.
Huamán	No más tanto porque robe su identidad sino para que efectúen las transferencias ahí hay que defender eso y tiene un mecanismo de seguridad de 2 pasos doble autenticación y que el Banco entonces protocolos está por ejemplo si me roban la tarjeta y hace una transferencia con la tarjeta el banco está en la obligación de comunicar al correo o aun teléfono que tú tienes no muchas veces no lo hacen o sea está en el papel que no se cumple.
Román	Bueno creo que lo más lo más práctico sería el cliente desea que se tengan estas actividades, el aplicativo virtual por ahí creo que tendríamos un gran porcentaje de personas me incluyo que no autorizamos el uso de

	aplicativos y con eso creo que liberaríamos una gran cantidad de problemas y lo otro es hacer mayores controles que el aplicativo.

Tabla 12

Resultado de la pregunta 9

Pregunta n.º 9 Desde su perspectiva ¿El token digital cumple la función de doble seguridad para que mitigar la suplantación de identidad digital?

PARTICIPANTE	**RESPUESTA**
Araujo	Es una medida seguridad con la finalidad de poder asegurar que efectivamente titular de la cuenta bancaria viene realizando las transacciones o las actividades comerciales entre el uso del aplicativo tendría esa finalidad pero como ya te expliqué los ciberdelincuentes o delincuentes a este han superado estas medidas de seguridad que plantean las entidades bancarias en ese sentido y te hablo de la práctica yo por ejemplo este mi competencias laborales a nivel nacional y organizó actividades con orientaciones o acompañamientos a nivel de todo El País y este en todos los institutos fiscales lo que he podido observar con mayor incidencia es de que para la obtención de estos tokens digital o claves autoritativas se comunican con sus víctimas a través de diferentes medios de comunicación WhatsApp en sentido es que las víctimas con desconocimiento respecto a la información valiosa que están brindando brindan las claves autoritativas que se les hace llegar a su correo electrónico a sus números telefónicos asociados a sus aplicativos móviles y de esta manera ya los ciberdelincuentes con previa anuencia entre comillas lograr obtener el tema de estas claves autoritativas y de esta manera realizar estos delitos
Covarrubias	Sí la validación ha sido creada con la finalidad de obtener una capa más de seguridad por ejemplo si yo ingreso a mi correo electrónico Gmail en este caso coloco mi correo y mi contraseña ingreso al sistema verdad mi correos si yo ingresada desde cualquier otro dispositivo con mi correo contraseña me ha pedido una ubicación del factor qué quiere decir esto que me ha llegado por este medio o por correo una contraseña única de acceso entonces con

	ese código con esa contraseña única de acceso voy a colocarla en el panel de ingreso y voy a validar mi acceso es recomendable los usuarios utilicen un doble factor de seguridad en cualquier sistema que lo permita es una capa más de seguridad es necesario
Espinoza	Bueno, considero que sí, justamente uno de los principales beneficios que se brinda a las personas que trabajan con el token digital es minimizar el riesgo de fraudes y delitos electrónicos.
Gonzales	Si por su puesto, todo lo que sume para los efectos de incrementar los niveles de ciberseguridad de prevenir antes que hacen las cosas si todo suma.
Huamán	Para esa función fue creado el token digital pero el problema está donde lo tenemos lo tenemos en los aparatos celulares y qué pasa si el aparato celular se pierde o te roban, basta que con lo que el delincuente con los medios serial que ya te indiqué con anterioridad a través de bots o través de la fuerza bruta ingresé a tu aplicativo bancario lógicamente el código va a llegar al teléfono le va a dar OK y se aprueba la transferencia
Román	El Famoso toque digital me parece que no, me parece que el toquen físico si lo hacía era una herramienta útil pero ahora con ese toque en digital que está muchas veces comprometido sincronizado con el celular volvemos al error de confiar la tecnología.

Análisis Convergente:

De los participantes, se obtuvo que la suplantación de identidad perjudica a los clientes en el uso de aplicativos bancarios porque este delito está vinculado con el hecho que sea cometido un delito informático, lo cual deja expuesto los datos del cliente, es decir los contactos de estos y el fin sería solicitar dinero en nombre del agraviado. Por lo cual el ciberdelincuente saca el máximo provecho a toda la información que tiene el teléfono.

Análisis Divergente:

Se considera que la suplantación de identidad no tiene que ver con el uso de aplicativos bancarios ya que son delitos totalmente diferentes, a su vez si existiera cierta similitud seria por la naturaleza del delito.

Codificación: De los resultados obtenidos de las entrevistas se busca desarrollar la codificación abierta, axial y selectiva del segundo objetivo específico. Se tiene a la **codificación abierta** tenemos que la suplantación de identidad se encontró contemplado en la ley especial N° 30096 el articulo 9 el cual menciona que al extraerse la información se puede utilizar los datos de este para algún provecho.

De los conceptos obtenidos contribuyen a la elaboración de la **Codificación axial** si bien es cierto existe suplantación de identidad en el código penal sin embargo en la ley especial es más específica, ya que menciona que se debe acceder a los datos informáticos y así obtener un provecho de este**.** Como último punto se menciona a la **codificación selectiva** menciona que el impacto económico de gastos en seguridad cada vez aumenta y son innecesarios, debido a que los ciberdelincuentes encuentran la manera de infringir la seguridad. (Oloyede,2022)

Como siguiente punto a tratar dentro de este capítulo se vera la **Discusión de resultados** en el cual se redactará aplicando del método de triangulación, respecto a los hallazgos encontrados en las entrevistas, las teorías y los antecedentes de investigación.

De los resultados obtenidos de la recolección de datos, se tiene que el participante Huamán menciono que el delito informático al ser enmarcado dentro de una norma especial pierde relevancia respecto a los otros delitos que se encuentra dentro del código penal contra el patrimonio, al no considerarlo un delito relevante pese a que también pertenecer a delito patrimonial, el Poder judicial y Ministerio público no le da mayor lesividad, el cual está sustentado con la teoría de García Cantizano que sostuvo que al no tener un concepto generalizado de los delitos informáticos, se consideró este tipo de delito, son aquellos que para lograr su comisión se utilizó un sistema automático de procesamiento de datos lo que excluye la existencia de un nuevo interés social, por otro lado las teorías que sostuvieron, Pineda y Siccha mencionaron que ciberespacio es una figura delictiva subjetiva, ya que comprende de un mundo informático, Colón Ferruzola y Cuenca, en su investigación sostuvo que el problema de los delitos informáticos radico que

no hay adecuada tipificación del código penal, de igual forma Mayer en su objetivo menciono la diferencia entre un delito informático y otros delitos siendo de fondo y no meramente de forma Sergei menciono que los delito bancarios es un tema nuevo por cual aún no se puede llegar a una adecuada lucha contra la ciberdelincuencia en el sector bancarios mediante los aplicativos bancarios, por ultimo Lujan sostuvo que para tener la efectividad para el tratamiento penal de debe tener marco legal que continuamente se esté actualizando, debido a que las modalidades de este delito, también irán cambiando, por ello es preciso que los operadores de justicia desarrollen capacidades especializadas en informática que permita un mejor manejo.

Respecto al **primer objetivo específico** de la investigación "Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios".

Por un lado, los resultados obtenidos los participantes Araujo, Espinoza, Gonzales, Huamán sostuvieron que el aplicativo bancario Si, promovió el fraude informático considerando que pese a tener un canal seguro para realizar operaciones bancarias, sin embargo el usuario es el que tienen que seguir las recomendaciones de ciberseguridad correctas para evitar caer en ese tipo de delito, debido a que las técnicas que se están utilizando para vulnerar los datos informáticos del cliente es hacer ingeniería social además que el ciberdelincuente se especializa en perpetrar el hecho delictivo, como lo menciono el participante Covarrubias el problema es que el usuario cae en el engaño y proporciona sus datos informáticos a través de una campaña de fishing por lo cual se tuvo que tener en consideración que este tipo de engaño agravia al usuario debido a que de forma fraudulenta consigue las información de estos aplicativos bancarios sustrae el monto económico, trayéndolo perjuicio y esta actividad está penada.

Gutiérrez Francés en su teoría menciono que el agraviado más común es la persona jurídica, ya sea una entidad bancaria o una institución pública. De igual forma se corroboro con la teoría Hayes que explico que el anonimato es el factor fundamental para que se cometan estos delitos informáticos, y como están en el ciberespacio es difícil encontrar una jurisdicción acorde a su vez que no existe una

cooperación entre naciones para mitigar el creciente aumento de delitos de fraudes informáticos

según Arellano en su investigación sostuvo que el fraude informático es una conducta que se encuentra regulado por un agente especializado hoy en tecnología afianzándose de métodos informáticos cómo uso a internet como medio de consumación del delito así por medio de la obtención de datos personales a fin de violar el derecho a la intimidad y privacidad a través de la obtención de datos personales mediante diferentes fraudes informáticos con el propósito de causar daño patrimonial a la persona o empresa a través de cuentas bancarias y aplicativos análogos digitales. Del mismo modo Bourdillon en su investigación sostuvo que el principal sector que se ve perjudicado es el estado financiero en este sentido se habla sobre las entidades bancarias, sin embargo, por más que esta entidad quiera estar a la vanguardia se ve obstaculizado por los ciberdelincuentes

Finalmente, respecto al **segundo objetivo específico** de la investigación: "Establecer de qué manera la suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios"

De los resultados obtenidos los participantes Gonzales, Huamán y Román menciono que si bien es cierto, el uso de aplicativos bancarios facilita las transacciones económicas, se hace un intercambio económico más llevadero sin embargo esto también ha generado un mayor riesgo de desmedro económico, por lo cual los delincuentes sacan el mayor provecho a toda la información que tiene el teléfono en el cual ya se ha cometido fraude informático en el uso de aplicativos, al tener información relevante del cliente, este ciberdelincuente se hace pasar por el agraviado y solicita préstamos a los contactos de estos por lo cual con esta figura se estaría cometiendo la suplantación de identidad, el problema radica primordialmente que el clientes es el eslabón más débil debido a que no tiene una cultura de ciberseguridad y se blanco más fáciles.

Cómo se mencionó en la teoría de Hassan el phishing es una manera de perpetrar la seguridad mandando correo electrónico innecesarios a los clientes por lo cual comparten información de su cuenta personal y así cometen el hecho delictivo, de igual forma la teoría de Alkhalil menciono que las personas comparten

más información personal como consecuencia al aumento significativo en el uso de internet y aun no se puede mitigar debido a que la suplantación de identidad aún es un tema muy novedoso

Banda y Phiri sostuvo que debido al gran avance tecnológico que cada vez va en aumento, es que la identidad digital se desactualiza y se vuelve más vulnerable para los usuarios, esto trae consigo que los usuarios se vean la necesidad de adquirir tecnología de última gama, De igual forma Monja afirmo que los delincuentes constantemente están en la búsqueda de burlar los sistemas de seguridad que protegen la identidad de las personas para ellos se ingeniaron para apropiarse de manera ilegítima de la información de las personas y lo hacen a través de mentiras o engaño qué hacen generar error en las víctimas todo ello se conoce con el nombre de suplantación de identidad este fenómeno está siendo usado en las páginas de Internet los criminales introducen a error a las víctimas con el objetivo de hacerlos vulnerables esto se debió al poco conocimiento que tuvieron los clientes acerca de los temas de suplantación de identidad.

V. CONCLUSIONES

Primero con la investigación se llega a la conclusión del primer objetivo general el cual se dice que los delitos informáticos de tipo bancario han tenido un aumento significativo con el avance tecnológico y al ser un tema novedoso no se puede llegar a una adecuada lucha contra la ciberdelincuencia en el sector bancario. El problema en los delitos informáticos radica que no hay una adecuada tipificación por lo cual estos delitos al estar en una ley especial son muy lesivos, existe una brecha entre la normatividad, ya que no se encuentra debidamente regulada y esto trae consigo que muchos casos queden impunes y no se puede dar una adecuada sanción.

Segundo del primer objetivo específico se puede determinar que fraude informático se ve más afectado el sector bancario, ya que al estar a la vanguardia con la tecnología crea programas de fácil acceso, es por ello que los ciberdelincuentes ven como punto fácil a los clientes que utilizan estos aplicativos, así como se menciona en la teoría de fraude informático es difícil aun de poder mitigar este problema ya que aún existe anonimato por parte del ciberdelincuente, además de que al estar en el ciberespacio es difícil de localizarlo y al no tener una norma concreta, no existe una adecuada cooperación para reducir este tipo de delito.

Tercero del segundo objetivo específico se concluye que debido al avance tecnológico nos hemos vuelto más expuestos a que se vuelva más fácil acceder a nuestra información personal, ya que el ciberdelincuente utiliza ingeniería social, además para que se cometa el delito de la suplantación de identidad es a consecuencia del delito de fraude informático, que se cometió por la sustracción de equipo móvil, esto se debe a que el ciberdelincuente quiere sacar el máximo provecho de este medio tecnológico, las empresas bancarias gastan en compran seguridad para este tipo de delito, sin embargo los ciberdelincuentes encuentra la forma de perpetrar sus hechos delictivos por tal motivo se sostiene que aun este delito es un tema aun novedoso.

VI. RECOMENDACIONES

Como recomendación se sugiere que se modifique la Directiva Nº.006-2012-MP-FN Criterios Sobre Competencia Fiscal, debido a que al producirse un delito primigenio que puede ser el hurto o robo, para que se cometa un delito informático se tiene que la Fiscalía que recibe el delito primigenio, analiza que los hechos denunciados le competen a la Fiscalía especializada en ciberdelincuencia, procede a inhibirse y lo remite a la Fiscalía de Ciberdelincuencia, ésta a su vez por la directiva ya mencionada por conexidad y amparados en el art. 31 y 32 del Código Procesal Penal, lo devuelve a la fiscalía provincial para que haga una investigación, a esta figura se le llama “contienda de competencia negativa” y genera más retardo en la investigación, por lo cual se debe tener en cuenta que la fiscalía de ciberdelincuencia es especializada y puede ver delitos comunes, con esto facilitaría que la evidencia que es digital no se pierda, debido a que es muy volátil. Además, hay que tener en cuenta que esta fiscalía es nueva por tal motivo se debe modificar la norma ya existente para un mejor manejo.

La superintendencia de banca y seguros debe supervisar la materia financiera y bancaria en cuanto al uso y manejo de los aplicativos bancarios, dando disposiciones específicas para evitar que exista vulneración logrando se dé el correcto uso del cliente y seguridad a los bancos que brindan el servicio.

Conforme lo descrito por los participantes se recomienda que exista una adecuada orientación y educación informática para el correcto funcionamiento de los aplicativos bancarios, y así evitar que se cometan phishing, ya que se ha visto reflejado que las personas más vulnerables a ser agraviados por estos delitos son las personas que desconocen de tecnología, a su vez que los bancos diseñen un doble control para evitar que se cometa suplantación de identidad.

REFERENCIAS

Ahmad, Iftikhar & Iqbal, Shahid & Jamil, Shahzad & Kamran, Muhammad. (2021). A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques. lingüística Antverpiensia. 2021. 3509-3517. https://www.researchgate.net/publication/352668394_A_Systematic_Literature_Review_of_E-Banking_Frauds_Current_Scenario_and_Security_Techniques

Alkhalil, Z., Hewage, C., Nawaf, L. y Khan, I. (2021). Ataques de phishing: un estudio exhaustivo reciente y una nueva anatomía., 1–23. https://doi.org/10.3389/fcomp.2021.563060

Almenar Pineda, F. (2017). El delito de hacking. Universidad de València. El delito de hacking - Dialnet (unirioja.es)

Arnau-Sabatés, L., y Sala Roca, J. (2020). La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad. Departamento de Teorías de la Educación y Pedagogía Social, Universidad Autónoma de Barcelona. https://docplayer.es/192625327-La-revision-de-la-literatura-cientifica-pautas-procedimientos-y-criterios-de-calidad.html

Arellano Casimiro, Gisela Lisset, Galindo Martinez, Sofia Emilia (2022) Deficiencias legislativas en el tratamiento de la Ley N° 30096, Ley de delitos informáticos – fraude informático, Lima 2019 – 2021. https://repositorio.ucv.edu.pe/handle/20.500.12692/102672?locale-attribute=es

Banda & Phiri (2019). Challenges of Identity Management Systems and Mechanisms: A Review of Mobile Identity. https://www.researchgate.net/publication/331952305_Challenges_of_Identity_Management_Systems_and_Mechanisms_A_Review_of_Mobile_Identity

Bermeo, M., Valencia, A., Duque, B., Garcés, L., & Luna, T. (2019). Factores de uso de los medios de pago móviles en millennials y centennials . 22(53), 77–102. https://doi.org/10.22395/seec.v22n53a4

Bourdillon O. Omijeh. (2023). El efecto del fraude en línea en la adopción de la economía digital en Nigeria: una revisión. Revista Africana de Gestión e Investigación Empresarial, 10 (1), 26–33. Obtenido de https://publications.afropolitanjournals.com/index.php/ajmbr/article/view/380

Convenio Sobre La Ciberdelincuencia Serie de Tratados Europeos - N° 185 Budapest, 23.XI.2001 (2001) Domingo 22 de setiembre de 2019. El peruano. http://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2292019/22-09-2019_CONVENIO.pdf

Datos Lr (2022, 7 de octubre) Yape vs. Plin: ¿cuáles son las diferencias y ventajas de ambas apps? La República. https://larepublica.pe/datos-lr/respuestas/2022/06/16/yape-vs-plin-ventajas-de-cada-app-bancaria-y-en-que-se-diferencian-evat

Ferruzola Gomez, E. C., & Cuenca Espinoza, H. A. (2015). Cómo responder a un Delito Informático. CIENCIA UNEMI, 7(11), 43-50. https://doi.org/10.29076/issn.2528-7737vol7iss11.2014pp43-50p

García Cantizano, M. d. C. (2012). Delincuencia informática en el ordenamiento jurídico penal peruano. Gaceta Jurídica–N78B, 69-72.

Gutiérrez Francés. (1991) María. Fraude informático y estafa. Madrid: Ministerio de Justicia

Hassan, A., Lass, F. y Makinde, J. (2012). Ciberdelincuencia en Nigeria: causas, efectos y salida. ARPNJ Ciencia y Tecnología, 2(7), 626-631. https://scholar.google.com/citations?user=8AzvPuQAAAAJ&hl=en

Hayes, B., Jeandesboz, J., Simon, S., Mitsilegas, V. y Scherrer, A. (2015). Los desafíos de la aplicación de la ley de la ciberdelincuencia: ¿realmente nos estamos poniendo al día?

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6a. ed. --.). México D.F.: McGraw-Hill.

Huamanñahui & Gamboa. (2022) Mobile Applications for Cybercrime Prevention: A Comprehensive Systematic Review. Revista Internacional de Informática Avanzada y Aplicaciones. https://www.researchgate.net/publication/365116530_Mobile_Applications_for_Cybercrime_Prevention_A_Comprehensive_Systematic_Review

Leão, F., Brantes, J., Sabino, A., & Wernck, J. (2018). introdução. Brazilian Business Review, 15, 176/190. https://doi.org/10.15728/bbr.2018.15.2.5.

Lujan Ccorahua, Zakir Temir (2022). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2022. https://repositorio.ucv.edu.pe/handle/20.500.12692/89722

Mardones, Rodolfo E.; Ulloa Martínez, Jorge B. & Salas, Gonzalo (2018). Usos del diseño metodológico cualitativo en artículos de acceso abierto de alto impacto en ciencias sociales [48 párrafos]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 19(1), Art. 8, https://www.qualitative-research.net/index.php/fqs/article/view/2656

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho, 44(1), 261-285. https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_abstract

Ministerio público (2022). Reporte Delitos informáticos registrados a través de denuncias ingresadas en el Ministerio Público a nivel nacional. https://andina.pe/agencia/noticia-conoce-las-modalidades-mas-comunes-delitos-informaticos-y-como-denunciarlos-el-peru-901507.aspx

Resolución N.º 0470-2022/UCV. Código de Ética en Investigación de la Universidad César Vallejo (19 de julio del 2022) https://www.ucv.edu.pe/wp-content/uploads/2020/09/RCUN%C2%B0470-2022-UCV-Aprueba-actualizacion-del-Codigo-de-Etica-en-Investigacion-V01.pdf

Oloyede, Kunle & Ajibade, Idris & Obunadike, Callistus & Phillips, Adeniyi & Shittu, Olayemi. (2022). A Review of Cybersecurity as an Effective Tool for Fighting Identity Theft across United States. 10.0130/2023993920. https://www.researchgate.net/publication/371698199_A_Review_of_Cybersecurity_as_an_Effective_Tool_for_Fighting_Identity_Theft_across_United_States

Monja Esquivel, Giuliana Marina (2022). Delitos informáticos en las entidades bancarias -suplantación de identidad. http://repositorio.ulasamericas.edu.pe/handle/upa/1953

Salinas Siccha, R. (2008). Derecho penal. Parte especial, 5.

Sergij S. Vitvitskiy, Oleksandr N. Kurakin, Pavlo S. Pokataev , Oleksii M. Skriabin and Dmytro B. Sanakoiev (2021). Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis. Banks and Bank Systems, https://www.businessperspectives.org/index.php/journals/banks-and-bank-systems/issue-375/peculiarities-of-cybercrime-investigation-in-the-banking-sector-of-ukraine-review-and-analysis

Villavicencio, F. (2014). Delitos informáticos. Revista IUS ET VERITAS, N° 49, diciembre 2014 https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

ANEXO

Matriz de categorización apriorística

PROBLEMAS	OBJETIVOS	CATEGORÌAS	SUBCATEGORIAS
General ¿El delito informático perjudica al cliente en el uso de aplicativos bancarios?	**General** Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios	Aplicativos Bancarios	-Aplicaciones instaladas por el smartphone
Específico 1 ¿El fraude informático perjudica al cliente en el uso de aplicativos bancarios?	**Específico 1** Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios	Delitos Informáticos	-Fraude Informático -Suplantación de Identidad
Específico 2 ¿La suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios?	**Específico 2** Establecer de qué manera la suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios		

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "**Guía de entrevista**". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	
Institución donde labora:	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Guía de entrevista)

Nombre de la Prueba:	Guía de entrevista
Autores:	Giovanna Milagros Quipuscoa Panduro
Procedencia:	Tabla de categorización
Administración:	Participantes
Tiempo de aplicación:	40 minutos
Ámbito de aplicación:	Diferentes escenarios
Significación:	La presente entrevista busca, responder la problemática planteada en el proyecto de investigación.

4. Soporte teórico

Escala/ÁREA	Subescala (categorías)	Definición
Derecho/Penal	Delitos informáticos	Es un tipo de actividad ilegal, delictiva y que va en contra de la ética por medio del uso de dispositivos electrónicos y del internet con el principal objetivo de poder vulnerar y ocasionar daños patrimoniales o personales a terceras personas o instituciones.
Derecho/Penal	Fraude informático	Se determina por la acción de los ciberdelincuentes por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios.
Derecho/Penal	Suplantación de identidad	sustraen la información de los usuarios para utilizarlos en su propio beneficio. Las finalidades para realizar estos actos pueden ser diversas a su vez existen muchas formas de beneficiarse del acceso no autorizado de los datos informáticos.

5. **Presentación de instrucciones para el juez:**

A continuación, a usted le presento la Guía de entrevista elaborado por Giovanna Milagros Quipuscoa Panduro en el año 2023-I De acuerdo con las siguientes categorías y subcategorías califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintácticay semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías del instrumento:

- Primera Categoría: DELITOS INFORMATICOS
- Objetivo de la categoría: Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios

Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
DELITOS INFORMÁTICOS	Desde su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos?	3	4	3	
	En su opinión ¿Por qué los clientes financieros han optado por el uso de aplicativos bancarios instalados en el smartphone?	3	3	3	
	Desde su perspectiva. ¿Qué factor ha influenciado para que se incremente el delito informático?	4	3	3	

- Sub-Categoría: FRAUDE INFORMÁTICO
- Objetivo de la categoría: Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
FRAUDE INFORMÁTICO	En su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en el fraude informático?	4	4	3	
	¿Cree usted que el hacking perjudica a los clientes en el uso de aplicativos bancarios?	3	3	3	
	En su opinión ¿En qué medida el uso de aplicativos bancarios puede considerarse un canal seguro para realizar operaciones bancarias?	4	3	3	

- Sub-Categoría: SUPLANTACIÒN DE IDENTIDAD
- Objetivo de la categoría: Establecer de qué manera la suplantación de identidad perjudica al cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
SUPLANTACIÓN INFORMÁTICO	¿Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad?	3	4	4	
	En su opinión ¿Qué mecanismos de seguridad se debería implementar los bancos y los clientes con aplicativos bancarios para evitar que roben su identidad?	3	3	4	
	Desde su perspectiva ¿El token digital cumple la función de doble seguridad para que se pueda mitigar la suplantación de identidad digital?	4	4	3	

David Saul Paulett Hauyon
DNI:43316595

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "**Guía de entrevista**". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:		
Grado profesional:	Maestría (x)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa (x)	Social ( ) Organizacional ( )
Áreas de experiencia profesional:		
Institución donde labora:		
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Guía de entrevista)

Nombre de la Prueba:	Guía de entrevista
Autores:	Giovanna Milagros Quipuscoa Panduro
Procedencia:	Tabla de categorización
Administración:	Participantes
Tiempo de aplicación:	40 minutos
Ámbito de aplicación:	Diferentes escenarios
Significación:	La presente entrevista busca, responder la problemática planteada en el proyecto de investigación.

4. Soporte teórico

Escala/ÁREA	Subescala (categorías)	Definición
Derecho/Penal	Delitos informáticos	Es un tipo de actividad ilegal, delictiva y que va en contra de la ética por medio del uso de dispositivos electrónicos y del internet con el principal objetivo de poder vulnerar y ocasionar daños patrimoniales o personales a terceras personas o instituciones.
Derecho/Penal	Fraude informático	Se determina por la acción de los ciberdelincuentes por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios.
Derecho/Penal	Suplantación de identidad	sustraen la información de los usuarios para utilizarlos en su propio beneficio. Las finalidades para realizar estos actos pueden ser diversas a su vez existen muchas formas de beneficiarse del acceso no autorizado de los datos informáticos.

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento la Guía de entrevista elaborado por Giovanna Milagros Quipuscoa Panduro en el año 2023-I De acuerdo con las siguientes categorías y subcategorías califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías del instrumento:

- Primera Categoría: DELITOS INFORMATICOS
- Objetivo de la categoría: Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios

Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
DELITOS INFORMÁTICOS	Desde su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos?	3	3	3	
	En su opinión ¿Por qué los clientes financieros han optado por el uso de aplicativos bancarios instalados en el smartphone?	3	3	3	
	Desde su perspectiva ¿Qué factor ha influenciado para que se incremente el delito informático?				

- Sub-Categoría: FRAUDE INFORMÁTICO
- Objetivo de la categoría: Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
FRAUDE INFORMÁTICO	En su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en el fraude informático?	3	3	3	
	¿Cree usted que el hacking perjudica a los clientes en el uso de aplicativos bancarios?	3	3	3	
	En su opinión ¿En qué medida el uso de aplicativos bancarios puede considerarse un canal seguro para realizar operaciones bancarias?	3	3	3	

- Sub-Categoría: SUPLANTACIÒN DE IDENTIDAD
- Objetivo de la categoría: Establecer de qué manera la suplantación de identidad perjudica al

cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
SUPLANTACIÓN INFORMÁTICO	¿Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad?	3	3	3	
	En su opinión ¿Qué mecanismos de seguridad se debería implementar los bancos y los clientes con aplicativos bancarios para evitar que roben su identidad?	3	3	3	
	Desde su perspectiva ¿El token digital cumple la función de doble seguridad para que se pueda mitigar la suplantación de identidad digital?	3	3	3	

Firma del evaluador
DNI:

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "**Guía de entrevista**". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:		
Grado profesional:	Maestría (x)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa (x)	Social ( ) Organizacional ( )
Áreas de experiencia profesional:		
Institución donde labora:		
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Guía de entrevista)

Nombre de la Prueba:	Guía de entrevista
Autores:	Giovanna Milagros Quipuscoa Panduro
Procedencia:	Tabla de categorización
Administración:	Participantes
Tiempo de aplicación:	40 minutos
Ámbito de aplicación:	Diferentes escenarios
Significación:	La presente entrevista busca, responder la problemática planteada en el proyecto de investigación.

4. Soporte teórico

Escala/ÁREA	Subescala (categorías)	Definición
Derecho/Penal	Delitos informáticos	Es un tipo de actividad ilegal, delictiva y que va en contra de la ética por medio del uso de dispositivos electrónicos y del internet con el principal objetivo de poder vulnerar y ocasionar daños patrimoniales o personales a terceras personas o instituciones.
Derecho/Penal	Fraude informático	Se determina por la acción de los ciberdelincuentes por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios.
Derecho/Penal	Suplantación de identidad	sustraen la información de los usuarios para utilizarlos en su propio beneficio. Las finalidades para realizar estos actos pueden ser diversas a su vez existen muchas formas de beneficiarse del acceso no autorizado de los datos informáticos.

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento la Guía de entrevista elaborado por Giovanna Milagros Quipuscoa Panduro en el año 2023-I De acuerdo con las siguientes categorías y subcategorías califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías del instrumento:

- Primera Categoría: DELITOS INFORMATICOS
- Objetivo de la categoría: Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios

Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
DELITOS INFORMÁTICOS	Desde su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos?	3	3	3	
	En su opinión ¿Por qué los clientes financieros han optado por el uso de aplicativos bancarios instalados en el smartphone?	3	3	3	
	Desde su perspectiva. ¿Qué factor ha influenciado para que se incremente el delito informático?	3	3	3	

- Sub-Categoría: FRAUDE INFORMÁTICO
- Objetivo de la categoría: Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
FRAUDE INFORMÁTICO	En su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en el fraude informático?	3	3	3	
	¿Cree usted que el hacking perjudica a los clientes en el uso de aplicativos bancarios?	3	3	3	
	En su opinión ¿En qué medida el uso de aplicativos bancarios puede considerarse un canal seguro para realizar operaciones bancarias?	3	3	3	

- Sub-Categoría: SUPLANTACIÒN DE IDENTIDAD
- Objetivo de la categoría: Establecer de qué manera la suplantación de identidad perjudica al

cliente en el uso de aplicativos bancarios

Sub Categoria	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
SUPLANTACIÓN INFORMÁTICO	¿Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad?	3	3	3	
	En su opinión ¿Qué mecanismos de seguridad se debería implementar los bancos y los clientes con aplicativos bancarios para evitar que roben su identidad?	3	3	3	
	Desde su perspectiva ¿El token digital cumple la función de doble seguridad para que se pueda mitigar la suplantación de identidad digital?	3	3	3	

Firma del evaluador
DNI 09316514
MG. JUAN M. QUIÑONEZ QUISPE
DOCENTE

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "**Guía de entrevista**". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:		
Grado profesional:	Maestría (x)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa (x)	Social ( ) Organizacional ( )
Áreas de experiencia profesional:		
Institución donde labora:		
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Guía de entrevista)

Nombre de la Prueba:	Guía de entrevista
Autores:	Giovanna Milagros Quipuscoa Panduro
Procedencia:	Tabla de categorización
Administración:	Participantes
Tiempo de aplicación:	40 minutos
Ámbito de aplicación:	Diferentes escenarios
Significación:	La presente entrevista busca, responder la problemática planteada en el proyecto de investigación.

4. Soporte teórico

Escala/ÁREA	Subescala (categorías)	Definición
Derecho/Penal	Delitos informáticos	Es un tipo de actividad ilegal, delictiva y que va en contra de la ética por medio del uso de dispositivos electrónicos y del internet con el principal objetivo de poder vulnerar y ocasionar daños patrimoniales o personales a terceras personas o instituciones.
Derecho/Penal	Fraude informático	Se determina por la acción de los ciberdelincuentes por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios.
Derecho/Penal	Suplantación de identidad	sustraen la información de los usuarios para utilizarlos en su propio beneficio. Las finalidades para realizar estos actos pueden ser diversas a su vez existen muchas formas de beneficiarse del acceso no autorizado de los datos informáticos.

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento la Guía de entrevista elaborado por Giovanna Milagros Quipuscoa Panduro en el año 2023-I De acuerdo con las siguientes categorías y subcategorías califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy especifica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías del instrumento:

- Primera Categoría: DELITOS INFORMATICOS
- Objetivo de la categoría: Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios

Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
DELITOS INFORMÁTICOS	Desde su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos?	4	4	4	
	En su opinión ¿Por qué los clientes financieros han optado por el uso de aplicativos bancarios instalados en el smartphone?	4	4	4	
	Desde su perspectiva. ¿Qué factor ha influenciado para que se incremente el delito informático?	4	4	4	

- Sub-Categoría: FRAUDE INFORMÁTICO
- Objetivo de la categoría: Identificar de qué manera el fraude informático perjudica al cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
FRAUDE INFORMÁTICO	En su experiencia ¿De qué manera el uso de aplicativos bancarios perjudica a los clientes en el fraude informático?	4	4	4	
	¿Cree usted que el hacking perjudica a los clientes en el uso de aplicativos bancarios?	4	4	4	
	En su opinión ¿En qué medida el uso de aplicativos bancarios puede considerarse un canal seguro para realizar operaciones bancarias?	4	4	4	

- Sub-Categoría: SUPLANTACIÒN DE IDENTIDAD
- Objetivo de la categoría: Establecer de qué manera la suplantación de identidad perjudica al

cliente en el uso de aplicativos bancarios

Sub Categoría	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
SUPLANTACIÓN INFORMÁTICO	¿Considera usted que el uso de aplicativos bancarios perjudica a los clientes en la suplantación de identidad?	4	4	4	
	En su opinión ¿Qué mecanismos de seguridad se debería implementar los bancos y los clientes con aplicativos bancarios para evitar que roben su identidad?	4	4	4	
	Desde su perspectiva ¿El token digital cumple la función de doble seguridad para que se pueda mitigar la suplantación de identidad digital?	4	4	4	

Firma del evaluador
DNI: 43234498
Manuel Moises Valdivia Cotrina.
Maestro Derecho Penal.

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada " El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos",cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos"
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante La respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si deseaparticipar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ningunaotra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificaral participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora: Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en lainvestigación antes mencionada.

Nombre y apellidos: Angel Gonzales Fartan

Fecha y hora: 21/09/23 09:22 a.m.

Firma:

Angel Ubaldo Gonzales Fartan
Fiscal Adjunta Superior
Fiscalía Superior de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada " El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos",cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos"
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante La respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si deseaparticipar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ningunaotra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificaral participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora: Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en lainvestigación antes mencionada.

ALAN ROLDAN ARAUJO CHAVEZ
Fiscal Adjunto Provincial
Unidad Fiscal Especializada en Ciberdelincuencia
del Ministerio Público

Nombre y apellidos: Alan Roldan Araujo Chavez

Fecha y hora: 21/09/2023 09:52

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada " El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos",cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos"
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante La respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si deseaparticipar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ningunaotra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificaral participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora: Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en lainvestigación antes mencionada.

Nombre y apellidos: Luis Edgardo HUAMAN SANTAMARIA

Fecha y hora: 23/09/2023

OA-00228623
Luis Edgardo HUAMAN SANTAMARIA
CORONEL PNP
JEFE DIVINDAT
DIRINCRI-PNP

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada " El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos",cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos"
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante La respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si deseaparticipar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ningunaotra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificaral participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora: Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en lainvestigación antes mencionada.

Nombre y apellidos: Hegel Covarrubias Maihua

Fecha y hora: 23/09/2023 10:24

SA-31542918
Hegel COVARRUBIAS MAIHUA
S1 PNP

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada " El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos",cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos"
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante La respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si deseaparticipar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ningunaotra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificaral participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora: Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en lainvestigación antes mencionada.

Nombre y apellidos: BONY ESPINOZA ROMA

Fecha y hora: 05/10/23

Anexo 3

Consentimiento Informado

Título de la investigación: El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos

Investigadora: Giovanna Milagros Quipuscoa Panduro

Propósito del estudio

Le invitamos a participar en la investigación titulada “El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos”,cuyo objetivo es : Determinar de qué manera el delito informático perjudica al cliente en el uso de aplicativos bancarios.Esta investigación es desarrollada por estudiantes pregrado de la carrera profesional Derecho, de la Universidad César Vallejo del campus Lima este, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

El teléfono móvil es el medio tecnológico más usado en la actualidad y que mediante estos aplicativos bancarios son potenciales medios comisivos de delitos informáticos

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: “El uso de aplicativos bancarios perjudica a los clientes en los delitos informáticos”
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 40 minutos y se realizará en el ambiente de la institución en donde se encuentre el participante Las respuestas al cuestionario o guía de entrevista serán codificadas usando un número identificación y, por lo tanto, serán anónimas.

Los principios que rige el presente consentimiento son:

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigadora:

Quipuscoa Panduro Giovanna Milagros email: gquipuscoap@ucvvirtual.edu.pe

y Docente asesor Mag. Lutgarda Palomino Gonzales

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Álvaro Martín Román Arroyo

Fecha y hora: 02 de octubre de 2023