UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de arequipa, 2020

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Zambrano Gomez, Alexandr Arturo (ORCID: 0000-0002-0474-0941).

ASESOR:

Mg. Vargas Huamán, Esaú (ORCID: 0000-0002-9591-9663)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, causas y formas del Fenómeno Criminal.

LIMA - PERÚ

2021

DEDICATORIA

La presente tesis está dedicado a mi madre Ninfa Martha quien me dio la vida forjo mi camino con sus sabios consejos, a mi amada esposa y compañera de vida Fiorella, para mi hija Emilia Fernanda y mi futuro hijo que se encuentra en camino.

AGRADECIMIENTOS

Al docente Esaú VARGAS HUAMAN asesor del taller de titulación quien con sus sabias enseñanzas logró que se cumpla el objetivo de culminar la presente investigación y a la Universidad Cesar Vallejo por brindarme la oportunidad de sustentar la tesis.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de investigación titulado “el uso de la Banca Móvil en los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020” tuvo como objetivo general determinar si el uso de banca móvil promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020. Para el cual se utilizó el método de investigación básico propio de la investigación cualitativa, cuyos resultados obtenidos mediante la técnica recolección de datos y la guía de entrevista, conforme lo descrito mayoritariamente por los expertos mediante el uso masificado de las aplicaciones móviles bancarias durante el año 2020 estando en pandemia se ha llegado a la conclusión que el uso de la Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio, el Fraude Informático y la clonación de datos informáticos, toda vez que para hacer uso fraudulento de los aplicativos es necesario que los datos informáticos de los clientes bancarios sean previamente clonados para poner en funcionamiento el aplicativo, instrumento utilizado posteriormente para cometer el Fraude Informático y Delitos Informáticos Contra el Patrimonio.

Palabras claves: Delitos Informáticos, Fraude Informático, Datos Informáticos, Banca Móvil y Aplicativos Móviles Bancarios.

ABSTRACT

The present research work entitled "The use of Mobile Banking in Computer Crimes Against Heritage in the city of Arequipa, 2020" had the general objective of determining whether the use of mobile banking promotes computer crimes against property in the city of Arequipa, 2020. For which the basic research method of qualitative research was used, whose results obtained through the data collection technique and the interview guide, as described mostly by the experts through the mass use of mobile applications During the year 2020, being in a pandemic, it has been concluded that the use of Mobile Banking promotes computer crimes against wealth, computer fraud and the cloning of computer data, since to make fraudulent use of the applications is It is necessary for the computer data of bank customers to be previously cloned to put into operation the application, an instrument later used to commit computer fraud and Computer Crimes Against Patrimony.

Keywords: Computer Crimes, Computer Fraud, Computer Data, Mobile Banking and Mobile Banking Applications.

I.INTRODUCCIÓN.

La situación actual que vive el mundo respecto a la pandemia por el brote del sars cov 2 (Covid-19), que según Calzada y Calzada (2020) la enfermedad se trata de un síndrome respiratorio agudo severo causante de neumonía grave entre sus causas de muerte más frecuentes, tal situación ha hecho que los hábitos y costumbres de las personas cambien de manera significativa en diferentes aspectos de su vida cotidiana, tal es el caso que, en la actualidad las personas por temor al contagio, facilidad a su acceso y practicidad en su manejo, han optado por el uso y manejo de la aplicativos móviles bancarios (Banca Móvil), instalada en dispositivos celulares de clientes bancarios, dichos aplicativos son ofertados por las diferentes entidades Bancarias para realizar operaciones económicas interbancarias entre personas, instituciones, comercios nacionales e internacionales, cubriendo necesidades de pago de bienes y servicios entre otros, para tal efecto los clientes bancarios han aprovechado la explosión de la tecnología financiera conocida como Fintech, según Pérez, Benito y Ramos (2020) denominada como empresa dedicada a emprender negocios innovadores haciendo uso de tecnologías, cuya finalidad es atender necesidades financieras, lo cual ha generado a su vez que personas inescrupulosas, accedan maliciosamente a información confidencial de clientes bancarios, para generar el denominado Fraude Informático utilizando para ellos la clonación de datos informáticos sensibles de clientes.

Al mismo tiempo para nuestra sociedad en la actualidad, el uso de Banca Móvil, se ha vuelto casi de manera forzosa entre quienes realizan diferentes operaciones interbancarias como giros, pagos, transferencias bancarias entre otros, existiendo actualmente en Perú un sinfín de aplicativos móviles bancarios o APP bancarias denominadas Banca Móvil, pudiendo nombrar entre los más usados durante la pandemia al aplicativo YAPE, creado por el Banco de Crédito del Perú, y billeteras móviles cuya particularidad en su funcionamiento es que funciona asociado solo a un número celular sin la necesidad de poseer una cuenta bancaria registrada en el sistema financiero, cuya característica principal es que los usuarios pueden estar en cualquier lugar, siendo el único requisito el acceso a internet y un dispositivo móvil, del mismo modo, el Estado peruano para

durante la pandemia, ha optado por facilitar bonos económicos a la población, que fueron transferidos a diferentes entidades financieras, quienes realizaron los desembolsos a través de Banca Móvil utilizando datos sensibles de los beneficiarios, por otro lado es importante mencionar que durante el año 2020 muchos usuarios de Banca Móvil han sufrido la vulneración de sus aplicativos, lo cual ha generado un incremento en los delitos informáticos contra el patrimonio, fenómeno que ha motivado el presente trabajo de investigación.

Por ello, el Departamento de Investigación de Delitos de Alta Tecnología - Arequipa durante el año 2020 estando en vigor el estado de emergencia decretado por el Estado Peruano mediante Decreto Supremo Nro. 044-2020-PCM del 16 de marzo del 2020, ha visto incrementado la recepción de denuncias por delitos informáticos contra el patrimonio, realizadas haciendo uso de Banca Móvil, operaciones denunciadas que se registraron mediante la clonación de datos informáticos, información que posteriormente fueron introducidos en los aplicativo móviles bancarios desde donde se realizaron operaciones fraudulentas, delito penado conforme Art. 8 del Decreto Legislativo Nro. 30096 y su modificatoria Decreto Legislativo Nro. 30171. Por ello, surge el presente problema general de investigación: ¿De qué manera el uso de banca móvil promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020? formulando el problema general, se realizó la formulación del primer problema específico: ¿De qué manera el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020? Asimismo, se tiene como segundo problema específico: ¿Por qué el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020?

El enfoque teórico de la presente investigación es conocer de qué manera el uso de Banca Móvil o aplicativos móviles bancarios, son utilizados por personas inescrupulosas quienes accediendo en todo o parte a los sistemas, datos informáticos o copiando datos sensibles de acceso a las mismas, generan fraudes informáticos, perjudicando el patrimonio económico de personas naturales y/o jurídicas, para lo cual se buscara establecer qué medidas de seguridad deberán tomar los usuarios y las entidades bancarias encargadas de brindar estos servicios, para mitigar el incremento de ilícitos cometidos haciendo

uso de Banca Móvil y sugerir los cambios necesarios en la legislación actual referente a los delitos informáticos.

Por otro lado, para el enfoque metodológico se buscará analizar jurisprudencia, dispositivos legales y demás fuentes del derecho que sirvan para analizar la tesis postulada, del mismo modo se utilizará técnicas y procedimientos para analizar la información recolectada, lo que nos servirá para demostrar como el uso de la Banca Móvil y los aplicativos móviles bancarios fueron utilizados en los Delitos Informáticos Contra el Patrimonio en Arequipa 2020. Respecto al enfoque práctico de la presente investigación se buscará plantear una reforma legal o implementar un texto normativo a la legislación existente respecto a los delitos informáticos en el Perú, asimismo reformas en la implementación y medidas de seguridad que deberán tener las entidades Bancarias y Financieras para brindar el acceso a la Banca Móvil o aplicativos móviles bancarios, esto con la finalidad de coadyuvar al proceso de investigación y obtener una mejor legislación para sancionar los ilícitos relacionados a los Delitos Informáticos.

Por otro lado, la presente investigación busca alcanzar, el siguiente objetivo general: Determinar si el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020. A partir del objetivo general, se planteó el primer objetivo específico: Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020. Asimismo, el segundo objetivo específico: Identificar si el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020.

Frente a los temas analizados y al problema propuesto, se procede a plantear el siguiente supuesto general: El uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020. A partir del supuesto general, se planteó el primer supuesto específico: El uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020. Asimismo, el segundo supuesto específico: El uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020.

II. MARCO TEÓRICO.

Para el presente estudio de investigación es necesario desarrollar antecedentes nacionales e internacionales, tales como:

Por un lado, León (2018) en su tesis titulada “vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la ley Nro. 30096 y su modificatoria en el Distrito Cercado Lima 2017”. Tuvo como objetivo general determinar cuáles son los vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley Nro. 30096 y su modificatoria en el Distrito Cercado Lima 2017. Por otro lado, respecto a la metodología el diseño de investigación fue no experimental – descriptivo, siendo el instrumento utilizado para la recolección de datos las encuestas y entrevistas. Concluyendo que, cuando se investiga este tipo de delitos, se tiene mucha dificultad para obtener las pruebas necesarias para incriminar a los autores no pudiendo penalizar a los delincuentes.

Por otro lado, Blossiers (2018) en su tesis titulada “el Delito Informático y su incidencia en la Empresa Bancaria”. Tuvo como objetivo general determinar cuál es el impacto de los Delitos Informáticos en la Empresa Bancaria. Por otro lado, respecto a la metodología el diseño aplicado a la investigación fue documental. Concluyendo que las empresas bancarias surten un impacto económico tanto para ellos como para sus clientes por la sustracción de fondos, siendo estos últimos quienes podrán alterar la estabilidad jurídica de los Bancos, teniendo la potestad para iniciar procesos civiles y/o penales en aras de obtener un resarcimiento económico.

Finalmente, Carreño y Hurtado (2019) en su tesis titulada “factores que influyen en la adopción de Banca Móvil en los Millennials en lima urbana”. Tuvo como objetivo general identificar los factores que influyen en la adopción de la Banca Móvil en los Millennials en Lima urbana. Por otro lado, respecto a la metodología de investigación fue cuantitativa con diseño no experimental transversal. Concluyendo que, el factor preponderante para el uso de Banca Móvil es el hábito respuesta dada por los encuestados quienes mencionaron ser usuarios habituales y naturales de Banca Móvil.

Asimismo, se analizaron antecedentes internacionales, siendo los siguientes:

Por un lado, Celli (2019) en su tesis “Las nuevas tecnologías y los Delitos Informáticos. Análisis de la ley 26.388. modificación del Código Penal argentino”. Tuvo como objetivo general, indagar si el ordenamiento jurídico argentino brinda las herramientas necesarias para controlar estos delitos producidos mediante el uso de nuevas tecnologías. Por otro lado, la metodología de investigación utilizada fue descriptiva. Concluyendo que, este tipo de delitos permite a los delincuentes actuar desde cualquier lugar, manteniendo total reserva de su identidad siendo la internet una herramienta de gran valor, que usada indebidamente causa grandes daños.

Por otro lado, Rojas (2016) en su tesis titulada “Evaluación de la seguridad de aplicaciones móviles bancarias”. Tuvo como objetivo general, proponer una taxonomía de malas prácticas de seguridad y una clasificación asociada que permita categorizar las aplicaciones móviles bancarias de la plataforma Android desarrollada por los Bancos Chilenos. Por otro lado, la metodología de investigación fue descriptiva. Concluyendo que, los aplicativos móviles no cuentan con enlaces para reportar posibles vulnerabilidades o peligros de seguridad, siendo derivados a los servicios de atención al cliente quienes desconocen los temas.

Finalmente, Gámez, Mantilla y Romero (2018) en su tesis titulada “descripción del desarrollo de la banca virtual en Colombia periodo 2013-2017”. Tuvo como objetivo general, describir el desarrollo de la bancarización virtual en Colombia, periodo 2013-2017. Por otro lado, respecto a la metodología utilizada en la investigación fue descriptiva. Concluyendo que, los canales digitales bancarios durante el periodo de estudio se han incrementado, siendo que para el año 2020 las operaciones bancarias pasaran de ser presenciales a virtuales, por lo que se debieran robustecer las plataformas tecnológicas.

Seguidamente es indispensable analizar la literatura acerca de las categorías de investigación y así estudiar las teorías relacionadas al tema, que a continuación se procede a plantear.

Respecto a la **Banca Móvil**, Leão, Brantes, Sanibo y Werneck (2018), señalan que los Bancos actualmente son más móviles, en referencia a los aplicativos bancarios (APP) que utilizan para brindar servicios, considerando a la Banca Móvil como (…) "tercera revolución tecnológica en la atención al cliente". Este tipo de servicios permite a los usuarios realizar cualquier tipo de transacción bancaria vinculada a una cuenta corriente, siendo el único requisito la transferencia de datos que brindan los operadores de comunicaciones o la conexión a una red Wi-Fi. Asimismo, Bermeo, Valencia, Duque, Garcés y Luna (2019), sostienen que la generación denominada Millennials y Centennials poseen alto manejo financiero, por ende, solicitan el uso de los servicios financieros a través de aplicativos móviles bancarios (**Banca Móvil**) o medios virtuales. Asimismo, sostienen que cerrando la brecha digital los países y regiones se han desarrollado a través de los procedimientos de pagos móviles.

Dentro de este marco Arias y Valdivia (2021) sostienen que la Banca móvil, se da en uso debido a múltiples factores con más interacción durante el mes de marzo del 2020, cuando se decretó el estado de emergencia por las situaciones sanitarias que vivía la nación, de esta manera las entidades financieras buscaban satisfacer las necesidades de los usuarios para evitar contagios de la covid-19. Por otro lado, Torres y Marín (2017) se refieren a la **Banca Móvil** o aplicativos móviles bancarios, como la amplificación del comercio electrónico o m-commerce, cuya utilización permite mayor flexibilidad y movilidad entre los usuarios, asimismo hacen mención a que, el m-commerce, ha rediseñado con su aplicación en una seria de servicios financieros entre los cuales se encuentran los servicios bancarios, desde donde los usuarios interactúan haciendo uso de dispositivos celulares en cualquier momento y espacio.

Del mismo modo Abendaño (2018) se refiere a la **Banca Móvil** como una quinta generación en la evolución del sistema bancario, identificándose a la generación de los Millennials, como clientes potenciales quienes realizan acceso a sus

recursos financieros a través de Banca Móvil. Asimismo, para Kapoor, Vij (2020) la **Banca Móvil** actualmente es tendencia en la industria bancaria quienes utilizan las aplicaciones móviles para obtener nuevos clientes, quienes utilizan estos canales para realizar diferentes acciones como verificar saldos, transferencia de dinero y pagos en línea entre otras, lo que para las empresas bancarias se traduce en un aumento en las ventas, mientras que para Louw y Nieuwenhuizen (2020) en Sudáfrica los bancos que operan, han digitalizado sus operaciones bancarias haciendo uso de la **Banca Móvil** para brindar un mejor servicio a los usuarios.

Finalmente, cuando se habla de tecnología financiera en la actualidad debe hacerse mención a la **Fintech**, por lo que según Palomino, Velásquez, Marcos y Seclen (2019), Vargas (2019) y García (2018) sostienen que las Fintech con tecnologías impulsadas en servicios e inclusión financiera dirigida hacia la población, quienes haciendo uso de este tipo de herramientas acceden a realizar operaciones de pagos, transferencias, compras, prestamos, ahorros y seguros, utilizando para ese fin la tecnología de telefonía móvil, las denominadas aplicaciones APP.

Lamas y Lamas (2018), los **Delitos Informáticos** son conductas que tienen como objetivo atacar los sistemas de dispositivos de seguridad, “invasión a computadoras, correos o sistemas de datos mediante una clave de acceso, conductas típicas que únicamente pueden ser cometidas a través de la tecnología” (p.271). Asimismo, Mayer y Oliver (2020) dentro de sus delimitaciones para los **Delitos Informáticos**, sostienen que, desde el punto de vista de los bienes jurídicos afectados, este tipo de delitos son los denominados de tipo patrimonial, identificándolos como fraude informático, que a su vez tiene conexo el bien jurídico llamado funcionalidad informática, ya que mediante el uso de los sistemas informáticos se realizan las operaciones de almacenamiento, tratamiento y transferencia de datos.

Por otro lado, Santacruz y Hermosa (2019), refieren que los **Delitos Informáticos** se encuentran relacionados con la interceptación ilegal de información, daño o supresión de información, considerando este tipo de delitos

como una de las mayores amenazas en cuanto al crimen que existen. Por otro lado, Núñez y Carhuancho (2020) se refieren a los **Delitos Informáticos** como ciberdelincuencia, identificando la modalidad Sim Swapping cuya particularidad es dejar sin servicio de cobertura a los dispositivos móviles celulares, donde se encuentran instalados los aplicativos bancarios, desde conde clientes realizan diversas actividades como pagos entre otros por la situación actual de la COVID-19.

Mientras que Mayer (2018), establece los medios de comisión de los delitos informáticos, diferenciando al **Fraude Informático**, que viene a ser el perjuicio patrimonial "a través de la alteración o manipulación de datos o programas de sistemas informáticos", estando relacionados con el Phishing y Pharming. Por otro lado, Saltos, Robalino y Pasmiño (2021) consideran que las personas que cometen los delitos informáticos como el **Fraude Informático** poseen conocimientos en informática, quienes en muchas ocasiones se encuentran en lugares estratégicos para acceder a información sensible de clientes, que para el caso de los fraudes informáticos están en los bancos. Asimismo, para Mayer (2017) el **Fraude Informático** se da cuando se manipulan los datos del sitio web de un Banco, esto para realizar la transferencia de fondos económicos de algún cliente, refiriendo a su vez que cuando se ejecutan este tipo de hechos no solo se afectan los bienes patrimoniales de los clientes, sino también la funcionalidad informática de los Bancos.

Respecto al **Phishing** García (2018) y Parker y Flowerday (2020), sostienen que se trata de una técnica de ingeniería social que busca obtener información bancaria confidencial a través de la suplantación de páginas web, utilizando las emociones de la víctima para crear confianza y obtener los datos sensibles de cuentas bancarios entre otros, asimismo dentro del contexto de **Phishing** Moncada (2020) sustenta que se trata del robo de datos personales usado por los Hackers que son utilizados para realizar robos y/o estafas, finalmente Koray, Buber, Demir y Diri (2018) se refieren al **Phishing** estructuras anónimas utilizadas por los ciberdelincuentes para recopilar información sensible a través del engaño mediante diseño de sitios web falsos.

Ahora bien, cuando tratamos el tema de **clonación de datos informáticos**, debemos entender que se encuentra asociada a la ciberseguridad, al respecto, Ospina y Sanabria (2020) mencionan que, “la ciberseguridad se enfoca en la protección de la infraestructura computacional y de información circulante en las redes informáticas como son los datos informáticos. En lo que concierne a la presente investigación, cuando hablamos de clonación de datos informáticos nos referimos a la intrusión de mecanismos o software malicioso que altera el normal funcionamiento de los aplicativos móviles bancarios o simplemente a personas quienes valiéndose de diferentes habilidades obtienen los datos necesarios para acceder a un sistema bancario, y en el caso de los fraudes informáticos poder transferir fondos económicos de clientes.

Al referirnos a la **clonación de datos informáticos**, no solo debemos ceñirnos a información almacenada en dispositivos electrónicos, sino más bien a todo tipo de datos personales, que alguna vez se haya compartido o este almacenada en una base de datos a la que personas inescrupulosas puedan acceder con la finalidad de obtener algún tipo de beneficio que para efectos de la presente investigación este determinado por el factor económico. En tal sentido Benussi (2020) respecto a la **clonación de datos informáticos** infiere que, debido al uso de las nuevas tecnologías que realizan un almacenamiento masivo de datos personales se ha demostrado que existe vulneraciones a las medidas de seguridad de los sistemas informáticos, lo que ha ocasionado que se generen perjuicios a los titulares y a los encargados de velar por el cuidado de los datos informáticos. Por lo que, existe la necesidad de aplicar diferentes mecanismos de seguridad en el tratamiento de los datos personales, volviéndose una prioridad para quienes utilizan la economía digital. Por otro lado, Poma y Vargas (2019) se refieren a la ciberseguridad como herramienta utilizada por personas y entidades para evitar ser víctimas de personas inescrupulosas que intentan obtener algún tipo de dato informático. Para efectos de la presente investigación con relación a lo descrito anteriormente es necesario describir como los ciberdelincuentes captan información de los clientes bancarios y **clonan datos informáticos**.

Finalmente, cuando hablamos de datos informáticos o **clonación de datos informáticos** debemos asociar estos términos a la ciberseguridad, que no es más que la protección de los sistemas para evitar su vulneración, en ese sentido, Álvarez y Hevia (2020) reconocen que todo sistema informático es inseguro, por lo que a la fecha, no ha existido un sistema que verdaderamente sea seguro desde su origen, por otro lado, Álvarez (2019) reconoce que existe falta de conocimiento en materia de ciberseguridad por parte de las entidades nacionales y privadas, lo cual genera una falta de idoneidad para la toma de decisiones y aplicación de propuestas concretas en materia de ciberseguridad, asimismo Moreno, Sánchez, Salavarrieta y Vargas (2019) reconocen el cambio en los métodos de pago, los mismos que hoy en día se realizan a través de medios tecnológicos, los cuales desde su punto de vista deben estar más protegidos para evitar fraudes, lo cual se lograra con un adecuado monitoreo de las actividades de los clientes y finalmente Mejía (2019) menciona el nivel de inseguridad que actualmente presentan los Smartphone, debido al uso masivo y transferencia de datos que se generan desde estos dispositivos al estar conectados a internet, lo que hace que sean vulnerables, conforme lo visto anteriormente es necesario que las entidades financieras intensifiquen los procesos de ciberseguridad con la finalidad de proteger los datos informáticos que circulan a través de los dispositivos móviles con los que los usuarios acceden a las plataformas financieras y de esa manera evitar la comisión de delitos informáticos.

Dentro de los enfoques conceptuales para la presente investigación es conveniente describir al i) **Phishing** como la acción mediante el cual una persona con conocimientos en informática, crea una infraestructura web de similares características a una original con la finalidad de obtener y grabar la información introducida en el formulario, por otra parte ii) **Fraude informático** se constituye como la acción por la que utilizando mecanismos informáticos se sustrae fondos económicos de clientes bancarios, dichos mecanismos pueden ser por ejemplo la iii) **Banca Móvil**, considerado como sistema informático que para su funcionamiento es necesario instalar un aplicativo en el dispositivo celular, cuya función financiera es la de realizar pagos, transferencias entre otros. Asimismo,

cabe mencionar que para el funcionamiento de los aplicativos es necesario la introducción de datos informáticos, por lo que para cometer los delitos informáticos contra el patrimonio es necesario la iv) **clonación datos informáticos**, para tal efecto se conoce a estos como información sensible que poseen los clientes bancarios como el número de tarjeta, fecha de vencimiento y código CVV de tarjeta, información indispensable para acceder a sistemas informáticos bancarios. Por lo antes mencionado es necesario identificar a la v) **Ciberseguridad,** como el mecanismo que se utiliza para tratar de evitar vulneraciones a los sistemas informáticos, mecanismo indispensable para las entidades financieras y de conocimientos para los usuarios quienes deben de tomar las medidas de seguridad personal para evitar situaciones de riesgo, finalmente vi) cuando hablamos de **Fintech** debemos entender que se trata de toda aquella tecnología que las entidades financieras utilizan a la fecha para realizar una inclusión de todos clientes para acceder a los servicios financieros basados en uso de las tecnologías, por ejemplo las aplicaciones móviles bancarias.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación.

La presente investigación realizada se ajusta al tipo básica, ello conforme lo descrito por Baena (2014), quien sostiene que la investigación básica "es el estudio de un problema, destinado exclusivamente a la búsqueda de conocimiento" en este sentido la investigación básica busca conocer leyes generales, para posteriormente elaborar teorías para comprenderlas (p. 11), por lo tanto, para la presente investigación se ha optado por el tipo básico, siendo el tema materia de investigación que responde al tema: "El uso de los aplicativos móviles bancarios en los delitos informáticos contra el patrimonio – Arequipa 2020", el cual mediante los instrumentos de recolección de información realizada a los especialistas en materia penal, investigadores de delitos informáticos entre otros, ayudaran a entender el fenómeno actual que se vive con el uso de los aplicativos móviles bancarios y como estos son usados para cometer ilícitos Informáticos Contra el Patrimonio,

procediéndose a realizar un análisis a la jurisprudencia actual vigente y al derecho comparado.

Por otro lado, respecto al diseño de investigación, según Gómez (2006), señala que "el diseño de investigación se refiere al plan o estrategia concebida para obtener la información que se desee, es decir, es el plan de acción a seguir en el trabajo de campo" (p. 85), en tal sentido para la presente investigación cualitativa, se establecerá como plan de investigación el diseño de la teoría fundamentada, la misma que consistirá en obtener información que responda a las categorías y sub categorías que componen la presente investigación, que nos permitirá generar teorías emergentes que expliquen el fenómeno estudiado respecto a los efectos jurídicos de la aplicación normativa y doctrinaria de la institución jurídica banca móvil y delitos informáticos contra el patrimonio en el contexto nacional y derecho comparado.

3.2 Categorías, Sub categorías y matriz de categorización.

Respecto a las categorías y subcategorías, según Herrera, Guevara y Munster (2015) consideran a las categorías como tópicos de investigación que surgen dentro de la investigación o a partir de la formulación de los objetivos generales, considerando a las subcategorías como tópicos que detallan los tópicos de investigación de manera específica, siendo el investigador quien proporciona el significado a las mismas (p. 6). Asimismo, estas han servido para la elaboración de la matriz de categorización, conforme al siguiente recuadro.

Cuadro Nro. 01

El uso de la Banca Móvil en los Delitos Informáticos Contra el Patrimonio Arequipa, 2020	
CATEGORÍAS	**SUBCATEGORÍAS**
Banca Móvil.	Banca por mensajes SMS
	Banca en aplicaciones instaladas en Smartphone.
Delitos Informáticos Contra el Patrimonio.	Fraude informático.
	Clonación de datos informáticos.

(Cuadro Nro. 01 – Fuente: Elaboración propia, 2021. Lima)

3.3 Escenario de estudio.

El escenario para realizar el presente estudio investigación ha sido el Departamento de Investigación de Delitos de Alta Tecnología, dado que en este departamento de investigación se registró un incremento en la recepción de denuncias, en las que se vieron implicados el uso de Banca Móvil o aplicativos móviles bancarios APP, por parte de ciudadanos que a raíz del confinamiento tuvieron la necesidad de que realizar operaciones bancarias desde sus domicilios.

De igual forma para la recolección de datos se ha tomado en cuenta a los especialistas en investigación que laboran en el Departamento de investigación de Delitos de Alta Tecnología – Arequipa quienes han brindado su amplio conocimiento en la materia, asimismo a Fiscales de Fiscalías Penales Corporativas del distrito fiscal Arequipa, quienes con la carga de la prueba han coadyuvado a la recolección de los datos, abogados expertos en materia de delitos informáticos y Perito informático forense.

3.4 Participantes.

Los participantes que se han tomado en cuenta para la presente investigación constan de especialistas en investigación de delitos informáticos pertenecientes al Departamento de investigación de Delitos de Alta Tecnología de la Ciudad de Arequipa, Fiscales Penales del Distrito Fiscal Arequipa, quienes tienen la carga de la prueba, abogados y peritos en materia de delitos informáticos.

Cuadro Nro. 02

Nº	ENTREVISTADO	CARGO QUE DESEMPEÑA	ESPECIALIDAD
1	Jorge Mario VALDIVIA HUAYCOCHEA	Sub Oficial Superior Jefe de Grupo de investigación Nro. 1 DEPINDAT – Arequipa.	PNP
2	Edgar Julio AGUILAR CCAPA	Sub Oficial Superior Jefe de Grupo de investigación Nro. 2 DEPINDAT – Arequipa.	PNP
3	Rogger W. SALDARRIAGA COHAILA	Comandante jefe DEPINDAT – Arequipa.	PNP

4	Gregorio D. CASTILLO MUÑOZ	Sub Oficial de Primera, analista informático – DEPINDAT Arequipa.	PNP
5	Julio Cesar TAPIA CARDENAS	Fiscal Adjunto Superior de la 3ra Fiscalía Superior Penal de Apelaciones Arequipa	Ministerio Público.
6	Elva Teresa BRAVO PALOMINO	Fiscal Adjunto al Provincial de la 1ra Fiscalía Provincial Penal Corporativa de Arequipa	Ministerio Público
7	Lizandro Thomas QUISPE SONCCO	Fiscal Adjunto al Provincial de la 1ra Fiscalía Provincial Penal Corporativa de Mariano Melgar Arequipa	Ministerio Público
8	Anthony Nelson Gustavo LINARES CUELLAR	Abogado defensor público	Ministerio de Justicia y Derechos Humanos
9	Ismael Leonidas SAMOS RIVERA	Magister en ingeniería de seguridad informática- Perito con inscripción REPEJ Nro. IE0001	Corte Superior de Justicia Arequipa
10	Abg. Edgar Luis Condori Quilca	Coordinador del Área de Defensa Penal -	Defensa Corporativa SAC

(Cuadro Nro. 02 – fuente: elaboración propia, 2021. Lima).

3.5 Técnicas e instrumentos de recolección de datos.

En la presente investigación se utilizó como técnica de recolección de datos la entrevista estructurada denominada a su vez entrevista dirigida, la misma que tiene un método preestablecido que responde a una guía de preguntas previamente preparadas, por lo que para la presente investigación se manejó la guía de entrevista, según (Bavaresco, 2001 citado por Useche, Artigas y Queipo, 2019) las técnicas y procedimientos de datos son operaciones que le permiten al investigador comprobar el problema planteado, asimismo determinan que los instrumentos son las herramientas que el investigador utilizara para obtener los datos requeridos para desarrollar su investigación.

Por otro lado, en la presente investigación se utilizó el análisis de fuente documental de resoluciones, convenios internacionales e informes policiales, a través del instrumento de recolección de datos conocida como Guía de Análisis Documental, relacionados al tema de investigación que coadyuvaron a obtener información relevante para el presente trabajo, el mismo que consiste en la observación e interpretación de los datos

obtenidos de los documentos relacionados a los objetivos de la presente investigación en materia de delitos informáticos.

3.6 Procedimiento.

En la presente investigación respecto al procedimiento la doctrina en temas de metodología de investigación científica, nos indica que se trata de un protocolo o el plan de investigación cuyo objetivo es responder lo planteado en el problema planteado, en tal sentido, la presente investigación responde al enfoque cualitativo con diseño en la teoría fundamentada, para tal efecto en aras de obtener información fidedigna referida a la investigación, se coordinará con las autoridades policiales del Departamento de investigación de Delitos de Alta tecnología Arequipa de la Policía Nacional del Perú, fiscales del distrito Fiscal de Arequipa y Jueces para los efectos de tener acceso a la información de los archivos pertinentes respecto a las investigaciones, jurisprudencias inherentes a los procesos judiciales sobre delitos informáticos, Fraude Informático con uso de Banca Móvil, por ende, plasmarlas en la Guía de Análisis Documental.

3.7 Rigor científico.

El rigor científico en una investigación responde a la calidad que se le debe otorgar al estudio de investigación, por tal razón, después de realizar la aplicación de los instrumentos de recolección de datos, se ha requerido que tres expertos en investigación científica realicen la validación de los instrumentos de recolección de datos, que para la presente investigación se trata de la Guía de Entrevista, resultado que se muestra en la tabla respectiva a la presente investigación.

Cuadro Nro. 03

validación de la guía de entrevista			
Validador	Cargo	Porcentaje	Condición
Esaú Vargas Huamán	Docente de la Universidad Cesar Vallejo	93%	Aceptable

Enrique Jordán Laos Jaramillo	Docente de la Universidad Cesar Vallejo	95%	Aceptable
Gerardo F. Ludeña Gonzales	Docente de la Universidad Cesar Vallejo	95%	Aceptable

(Cuadro Nro. 03 – fuente: elaboración propia, 2021. Lima).

3.8 Método de análisis de datos.

Respecto al análisis de datos, según Rodríguez, Lorenzo y Herrera (2005), sostienen que, el análisis de datos cualitativos es el proceso mediante el cual el investigador procede a organizar y manipular la información, ello con la finalidad de buscar relaciones, extraer significados y conclusiones, en tal sentido, la presente investigación estará direccionado a los métodos descriptivo mediante el cual se hará una descripción de resultados recabados mediante la guía de entrevista realizada a nuestros expertos para luego analizarlas, compararlas interpretarlas y obtener los resultados con relación al uso de la Banca Móvil en los delitos informáticos contra el patrimonio, por otro lado, respecto al método hermenéutico se realizara el análisis a textos y fuentes documentales con la finalidad de interpretar la jurisprudencia y normativa vigente sobre delitos informáticos, finalmente con relación al método inductivo en la presente investigación basados en la recolección de datos se formularan las conclusiones a los supuestos descritos en la presente investigación.

3.9 Aspectos éticos.

El presente trabajo de investigación se rige mediante los principios éticos y morales, por lo que su contenido es propio del autor, teniendo como base la recolección de información de diferentes fuentes y casos de realidad actual ocurridos en la ciudad de Arequipa, debiendo mantener el respeto del derecho a la propiedad intelectual, respetado la autoría de trabajos tomados como antecedentes, respetando el correcto citado de las fuentes bibliográficas en las normas internacionales APA.

IV. RESULTADOS Y DISCUSIÓN.

En el presente capítulo se procedió a describir los resultados recogidos mediante el instrumento de recolección de datos de la Guía de entrevista, así como la guía de análisis documental. Para la presente investigación el **Objetivo General:** "Determinar si el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020" se plantearon las siguientes preguntas:

1. ¿De qué manera el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020?
2. En su opinión, ¿por qué los clientes de financieros han optado por el uso de Banca Móvil?
3. Desde su perspectiva, ¿qué factor ha influido para que se incrementen los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020?

Referente a la primera interrogante Aguilar, Saldarriaga, Quispe, Tapia y Bravo (2021) sostiene que la Banca Móvil si promueve los delitos informáticos contra el patrimonio, convirtiéndose esta en un espacio propicio para tales delitos ya que mediante ella introducen datos sensibles. por otro lado, Valdivia (2021), sostiene que existe una falta de comunicación entre las entidades bancarias en cuanto a las medidas de seguridad, finalmente Castillo, Linares, Condori y Samos (2021) sostienen que la banca móvil no promueve los delitos informáticos sin embargo el uso no adecuado de estos si promueve la Comisión de ilícitos informáticos penales. **Referente a la segunda interrogante** Castillo, Aguilar, Quispe y Tapia (2021) sostiene que el uso de la Banca Móvil estuvo representada por el temor a los contagios de la COVID-19 y relacionados a este tema, por otro lado, Valdivia, Saldarriaga, Linares, Condori, Tapia y Samos (2021) sostiene que la banca móvil ofrece facilidad en la realización de operaciones bancarias pudiendo realizar las operaciones desde cualquier lugar, finalmente Bravo (2021) asocia el uso de la banca móvil a una moda sin saber los peligros que trae consigo el mal uso de la banca móvil. **Referente a la tercera interrogante** Valdivia, Aguilar, Saldarriaga, Linares, tapia y Bravo (2021) sostiene que el factor preponderante para el incremento de los ilícitos

informáticos es el desconocimiento, confianza, y la facilidad para realizar los pagos quienes no adoptaron sus medidas de seguridad. Castillo y Samos (2021) consideran como factor a la seguridad informática y la Fentech (tecnologías financieras). Por otro lado, Quispe (2021) asocia al factor de poca asistencia de las entidades bancarias a los clientes. Finalmente, Condori (2021) considera como factor importante la poca persecución que se da a este tipo de ilícitos penales, aunada a la desidia de la población a denunciar este tipo de hechos.

De este modo el **objetivo especifico 1**: Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020, se plantearon las siguientes preguntas:

4. De acuerdo a su experiencia, ¿de qué manera el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020?
5. ¿En qué medida, la Banca Móvil puede considerarse un canal seguro para realizar operaciones bancarias?
6. ¿De qué manera la pandemia ha ocasionado el aumento de los fraudes informáticos?

Referente a la cuarta interrogante Castillo, Valdivia, Aguilar, Saldarriaga, Condori, Quispe, Tapia, Bravo y Samos (2021) consideran que la Banca Móvil si promueve el Fraude Informático ya que los usuarios no toman las medidas de seguridad adecuadas para resguardar datos importantes y sensibles y por el desconocimiento en su uso y manejo. Finalmente, Linares (2021) considera que la banca móvil no promueve el Fraude Informático. **Referente a la quinta interrogante** Castillo, Valdivia, Aguilar, Saldarriaga, Condori, Tapia y Samos (2021) consideran que se trata de un canal seguro siempre y cuando las entidades bancarias utilicen medidas de seguridad pertinentes y los clientes hagan un uso adecuado de la Banca Móvil. para Linares (2021) tiene un 90% de seguridad debido al aprovechamiento que le dan al margen de error los hackers para cometer Delitos Informáticos. Finalmente, Bravo (2021) no considera un canal seguro. **Referente a la sexta interrogante** Castillo, Valdivia, Aguilar, Saldarriaga, Linares, Condori, Quispe, Tapia, Bravo y Samos (2021) consideran que la Pandemia ha ocasionado el aumento de los fraudes informáticos debido

a que los procesos de pago y compra estuvo estrechamente ligado a la no presencia en establecimientos comerciales y nuevas formas de pago asegurando el no desplazamiento físico de las personas.

De este modo el **objetivo específico 2**: Identificar si el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020, se plantearon las siguientes preguntas:

7. ¿Por qué el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020?
8. ¿Qué mecanismos de seguridad se deben implementar para evitar la vulneración a los sistemas de Banca Móvil?
9. ¿Qué medidas de seguridad deben tomar las entidades bancarias y los clientes para evitar la clonación de datos informáticos?

Referente a la séptima interrogante Castillo, Valdivia, Saldarriaga, Linares, Condori, Quispe, Tapia, Bravo y Samos (2021) sostienen que la Banca Móvil si promueve la clonación de datos informáticos porque su uso se ha generalizado y por lo general solo basta una clave de seis dígitos conjuntamente con el número de tarjeta, asimismo al haberse realizado la solicitud de operaciones por banca móvil se puede inferir que los datos informáticos fueron clonados, mientras que para Aguilar (2021) no existe clonación de datos informáticos ya que los ciberdelincuentes acceden a los datos mediante engaño por medio de páginas falsas. **Referente a la octava interrogante** Castillo, Valdivia, Aguilar, Saldarriaga, Linares, Condori, Quispe, Tapia, Bravo y Samos (2021) sostienen que los mecanismos más importantes que se deben de implementar para evitar la vulneración de los sistemas de Banca Móvil están relacionados a la identificación biométrico facial y dactilar, como también el token que puede darse mediante SMS. **Referente a la novena interrogante** Castillo, Valdivia, Aguilar, Saldarriaga, Linares, Condori, Quispe, Tapia, Bravo y Samos (2021) refieren que las medidas de seguridad a implementarse son; contraseñas seguras, notificaciones de operaciones, evitar compartir información personal, huella digital y coordinar con las entidades financieras con la Policía para evitar este tipo de ilícitos penales.

Por otro lado, los resultados obtenidos en la **guía de análisis de fuente documental**, respecto al **Objetivo General** "Determinar si el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020" se ha optado por analizar la **Resolución Nro. 5570-2019** de la **Superintendencia de Banca, Seguro y AFP** y el **Informe Policial Nro. 209-2021- DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv**, para la resolución Nro. 5570-2019 de la Superintendencia de Banca, Seguro y AFP como ente rector en materia bancaria en el Perú contempla la autorización y regulación de las aplicaciones móviles (**Banca Móvil**), instrumento utilizado por los Bancos y clientes quienes durante el año 2020 han masificado el uso de esta herramienta, siendo de este modo utilizado también por los ciberdelincuentes, quienes aprovechando los descuidos y malas prácticas por parte de los usuarios vulneraron sus accesos para cometer ilícitos de transferencia de fondos económicos, por otro lado, en el contenido del Informe Policial se puede evidenciar que la transferencia de dinero se realizó utilizando la Banca Móvil del Banco Interbank pare ellos los delincuentes solicitaron la reposición de la tarjeta SIM del agraviado par posteriormente instalar el aplicativo y realizar las transferencias. Ante ello, **podemos concluir que**, Debido a la masificación en el uso de aplicativos móviles bancarios (**Banca Móvil**) por la situación de la pandemia durante el año 2020, el uso de banca móvil ha promovido los Delitos Informáticos Contra el Patrimonio, debido a que haciendo uso de esta herramienta tecnológica durante el periodo de estudio se han denunciado un número significativo de operaciones bancarias fraudulentas que se realizaron desde aplicativos móviles bancarios (**Banca Móvil**) creados con datos personales de los agraviados, desde donde se realizaron transferencias, compras y pagos con destinos desconocidos por los agraviados.

Por otro lado, conforme al informe analizado para la presente investigación, se logra inferir que, el agraviado después de perder el servicio de su línea telefónica durante el lapso de 12 horas aproximadamente fue alertado de las transferencias fraudulentas que se registraron haciendo uso de su aplicativo móvil bancario (**Banca Móvil**), lo cual significa que su Banca Móvil fue instalado en otro dispositivo móvil haciendo uso de su línea telefónica que fue obtenida mediante reposición de tarjeta SIM por parte de los delincuentes quienes realizaron

transferencias de dinero a cuentas bancarias del exterior, en tal sentido podemos concluir que el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio, debido a su fácil acceso mediante artimañas utilizadas por los delincuentes y las pocas medidas de seguridad establecidas por los Bancos para controlar las operaciones, por otro lado, al estar las cuentas bancarias protegidas por ley en un proceso de investigación demandará de tiempo para solicitar a la autoridad competente el levantamiento del secreto bancario para determinar a los titulares de las cuentas e individualizar a los autores.

Asimismo, con relación al **Objetivo Específico** 1: "Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020" se ha optado por analizar el Convenio sobre la ciberdelincuencia o "**Convenio de Budapest**", del cual Perú forma parte desde el 12 de febrero del 2019 mediante Decreto Supremo Nro. 010-2019-RE y vigente desde el 01 de diciembre del 2019, el cual busca establecer pautas y/o reglas de cooperación internacional entre sus miembros para la identificación específica de conductas delictivas asociadas al uso de las tecnologías de la información, para tal efecto en nuestra normatividad vigente para delitos informáticos la Ley Nro. 30096 y su modificatoria Ley Nro. 30171 han copia el artículo 8 del presente convenio creando el Art. 8 que a la letra dice: El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social" y el **Informe Policial Nro**. **179-2021-DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv.** Ante ello, **podemos concluir**, la Banca Móvil si bien fue creada con el fin de facilitar las operaciones entre los usuarios quienes realizan sus transacciones bancarias desde cualquier lugar, promueve el Fraude Informático, debido a su fácil acceso con datos mínimos para su creación, situación que es aprovechada por los ciberdelincuentes quienes valiéndose de diferentes artimañas obtienen datos

personales de los clientes bancarios, por otro lado con relación al Informe Policial podemos concluir que, Analizado el Informe Policial se logra inferir que las operaciones fraudulentas registradas mediante aplicativo móvil YAPE se realizaron desde un dispositivo móvil distinto al del titular de la cuenta bancaria, dispositivo en el que se instaló la aplicación móvil para realizar catorce operaciones de transferencia monetaria, aplicativo que el agraviado nunca instalo en su dispositivo móvil, desconociendo su uso, llegando a la conclusión que efectivamente el uso de Banca Móvil promueve el fraude informático, ya que los ciberdelincuentes aprovechan los aplicativos bancarios para obtener provecho económico ilícito personal o para terceros.

Finalmente, para el **Objetivo Especifico 2**: "Identificar si el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020" se ha optado por analizar el **Recurso de Nulidad Nro. 2932-2019** emitida por la Primera Sala Penal Transitoria Lima y el **Informe Policial Nro. 191-2021-DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv**, documentos que contemplan cual es el fin de la clonación de datos informáticos. Ante ello, **podemos concluir que**, para efectos de la presente investigación, podemos concluir que la Banca Móvil promueve la clonación de dados informáticos, como lo evidenciado en la fuente documental fue necesario obtener los datos bancarios sensibles de acceso a la cuenta del agraviado mediante Phishing para realizar las operaciones bancarias fraudulentas, en tal sentido queda demostrado en el presente recurso de nulidad que existió clonación de datos informáticos porque una vez copiados fueron utilizados por otra persona ocasionando el Fraude Informático, mientras que para los informes policiales Conforme lo narrado por la agraviada y lo plasmado en el análisis de los hechos del Informe Policial formulado por el Instructor a cargo de la investigación del Departamento de Investigación de Delitos de Alta Tecnología -Arequipa, podemos concluir que la cliente bancaria testifico nunca haber instalado ni utilizado el aplicativo móvil bancario (YAPE) sin embargo manifestó haber recibido un correo indicando que su cuenta Débito del Banco de Crédito se fue afiliada a la banca móvil (YAPE), por lo que se presume que sus datos bancarios fueron clonados para realizar el registro en el aplicativo móvil YAPE desde donde se realizaron transferencias de dinero de la agraviada.

En el presente apartado relacionado a la **discusión de resultados** se procederá a redactar el resultado de la aplicación del método de triangulación, respecto a los hallazgos encontrados en los instrumentos de recolección de datos de la guía de entrevista y la guía de análisis documental con los hallazgos encontrados en los antecedentes de investigación y las corrientes doctrinarias, en el siguiente contexto:

Por un lado, de los resultados obtenidos de los instrumentos de recolección de datos de la guía de entrevista con relación al objetivo general la mitad de los expertos entrevistados sostienen que el uso de la Banca Móvil si promueve los Delitos Informáticos Contra el Patrimonio, mientras que una minoría sostuvo que el uso de la Banca Móvil no promueve los Delitos Informáticos Contra el Patrimonio, pero sin embargo sostienen que un mal uso de estos aplicativos si promueve la comisión de ilícitos informáticos penales, finalmente uno de los expertos sostuvo que existe una falta de comunicación entre las entidades bancarias en cuanto a las medidas de seguridad.

De la misma manera, de los resultados obtenidos de la guía de análisis documental, en la **Resolución Nro. 5570-2019** de la **Superintendencia de Banca, Seguro y AFP,** dicha institución como ente rector en materia bancaria en el Perú autoriza el uso de los aplicativos móviles bancarios como complemento a los servicios ofrecidos por las entidades bancarias, lo cual por el uso masificado por los clientes durante la pandemia ha sido aprovechado por los ciberdelincuentes quienes usando la **Banca Móvil** transfirieron dinero, compraron y pagaron bienes y servicios con dinero de los clientes afectados promoviendo de este modo la **Banca Móvil** los Delitos Informáticos Contra el Patrimonio. Del mismo modo del **Informe Policial Nro. 209-2021- DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv,** se desprende que la **Banca móvil** propiedad del Agraviado Jorge Luis CERVANTES ARTEAGA, fue instalada en otro dispositivo celular, poco después de solicitar con documentos falsos la reposición de la tarjeta SIM y reinstalar el aplicativo móvil desde donde realizaron las transferencias bancarias fraudulentas, siendo esta una modalidad nueva para tomar el control de los aplicativos móviles bancarios de clientes financieros, con

lo que se demuestra que la banca móvil si promovería los Delitos Informáticos Contra el Patrimonio.

Respecto de los hallazgos obtenidos en los antecedentes de investigación, Blossiers (2018), en su investigación respecto al delito informático y su incidencia en la empresa bancaria, sostuvo que a raíz de la comisión de los Delitos Informáticos la empresa como tal y los clientes han sufrido un impacto muy importante en lo económico por la sustracción fondos.

Asimismo, de los resultados obtenidos en la doctrina, Nuñez y Carhuancho (2020) identifican una nueva modalidad de Delitos Informáticos relacionados a la **Banca Móvil** al cual lo denominan Sim Swapping, cuya traducción al español significa "cambio de sim" dispositivo conocido como CHIP telefónico por los usuarios, herramienta que es recabada mediante artimañas por los ciberdelincuentes para obtener provecho económico ilícito.

Finalmente, teniendo en consideración la opinión mayoritaria de los entrevistados y la información obtenida de los diferentes instrumentos y documentos analizados para la presente investigación, el uso de la banca móvil promueve los Delitos Informáticos Contra el Patrimonio, teniendo en consideración a su vez que para cometer este tipo de ilícitos es necesaria la presencia de dos o más personas desde la obtención de datos confidenciales de los clientes bancario, creación de cuentas en los aplicativos bancarios y cobro de los fondos fraudulentos transferidos, razón por la cual podemos dar a conocer que para la presente investigación en la discusión interna y externa damos respuesta al supuesto general que para la presente investigación fue "el uso de banca móvil promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020".

Respecto al **primer objetivo específico** de la investigación: "Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020".

Por un lado, de los resultados obtenidos en los instrumentos de recolección de daos de la guía de entrevista, los expertos que dieron respuesta a las preguntas relacionas al primer objetivo específico en su mayoría sostuvieron que la Banca Móvil si promueve el fraude informático, considerando a este la mayoría de los

entrevistados como un canal seguro para realizar operaciones bancarias, para lo cual los usuarios deberán tomar las medidas de seguridad necesarias para evitar vulneraciones, por último la mayoría coincidió en que la pandemia ocasiono el aumento de los fraudes informáticos debido a la actividades económicas no presenciales lo que ocasiono el uso masivo de la Banca Móvil para satisfacer necesidades esenciales.

De la misma manera, con relación a los resultados obtenidos de la guía de análisis documental respecto al Convenio sobre la ciberdelincuencia o "**Convenio de Budapest**" identifica en su artículo octavo al Fraude Informático, doctrina que fue adoptada por la legislación nacional en la Ley Nro. 30096 y su modificatoria Ley Nro. 30171 "Ley de delitos informáticos" en tal sentido se busca sancionar todo acto que cause perjuicio económico haciendo uso de las tecnologías, en la presente investigación referida al uso de la **Banca Móvil** como medio para obtener provecho económico,. Asimismo, con relación al **Informe Policial Nro**. **179-2021-DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv,** una vez analizado podemos deducir que las operaciones registradas mediante **Banca Móvil** (YAPE) se realizaron desde un dispositivo celular distinto al del titular de la cuenta bancaria, quien desconocía el registro de su cuenta en la mencionada aplicación, demostrándose de esta forma que el uso de la banca móvil si promueve el fraude informático.

Respecto de los hallazgos obtenidos en los antecedentes de investigación, Carreño y Hurtado (2019) en su investigación respecto a los factores que influyen en la adopción de Banca Móvil en los Millennials en Lima urbana, sostuvieron como principal factor para el uso de la Banca Móvil a la habitualidad en el uso de los aplicativos, conforme los descrito por los expertos esta habitualidad y su mal uso respecto a las medidas de seguridad hace que los aplicativos sean vulnerables y promuevan los fraudes informáticos.

Asimismo, de los resultados obtenidos en la doctrina, Mayer (2020) identifica dentro de los delitos informáticos al Fraude Informático, al cual lo define como el perjuicio patrimonial que para producir efectos tiene actos preparatorios que se dan a través de alteración o manipulación de datos informáticos relacionados al Phishing, al respecto Koray, Buber, Demir y Diri (2018) se refieren al Phishing

como el diseño de estructuras anónimas utilizadas por los ciberdelincuentes para recopilar información sensible a través del engaño mediante diseño de sitios web falsos.

Finalmente para concluir respecto al primer objetivo específico conforme lo detallado por los expertos, analizadas las fuentes documentales, antecedentes de investigación, y doctrina respecto a los fraudes informáticos, se ha logrado establecer que el uso de la Banca Móvil promueve los Fraude Informáticos debido básicamente a la clandestinidad con la que operan los ciberdelincuentes en el uso y manejo de las aplicaciones móviles bancarias (**Banca Móvil**), quienes para cometer este tipo de ilícitos se agencian de líneas telefónicas ilícitas y cuantas bancarias de terceros quienes bajo la entrega de un monto dinerario otorgan sus cuentas para ser las receptoras del dinero transferido fraudulentamente, por lo que para la presente investigación, consideramos necesario que, para aperturar aplicaciones móviles bancarias sea de manera presencial en las agencias bancarias proveedoras de este tipo de servicios para evitar sincronizaciones no autorizadas de cuentas bancarias.

Finalmente, respecto al **segundo objetivo específico** de la investigación: “El uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020”.

Por un lado, de los resultados obtenidos en los instrumentos de recolección de datos de la guía de entrevista, los expertos que dieron respuesta a las preguntas relacionas al segundo objetivo específico en su mayoría sostuvieron que la banca móvil si promueve la clonación de datos informáticos, por lo que es necesario implementar mecanismos de seguridad para evitar la vulneración de los sistemas de banca móvil, finalmente advierten que es de vital importancia la implementación de sistemas de seguridad para el acceso a los aplicativos móviles bancarios como son la identificación biométrico facial, dactilar y la activación de los token de seguridad para los confirmatorios de las operaciones por parte de los clientes bancarios, de esta manera queda demostrado el uso de la banca móvil promueve la clonación de datos informáticos, porque son estos los indispensables para acceder a las aplicaciones para cometer los ilícitos penales relacionados con la banca móvil y los fraudes informáticos.

De la misma manera, con relación a los resultados obtenidos de la guía de análisis documental respecto al **Recurso de Nulidad Nro. 2932-2019** emitida por la Primera Sala Penal Transitoria Lima declaró improcedente el recurso materia de revisión, esto debido a que los datos informáticos clonados mediante una página falsa utilizando la técnica del Phishing, fueron indispensables para realizar el fraude informático, ocasionando el perjuicio económico al cliente bancario. Asimismo, con relación al **Informe Policial Nro**. **191-2021-DIRINCRI PNP/DIVINDAT-DEPINDAT AQP-Inv,** después de analizar los hechos materia de la investigación, se logró inferir que la agraviada por el presunto Delito Informático Contra el Patrimonio en la Modalidad Fraude Informático Transferencias Bancarias, nunca instalo en su dispositivo celular la aplicación YAPE desde donde se registraron las transferencias bancarias fraudulentas, por lo que fue necesario clonar los datos informáticos de su cuenta y tarjeta para la afiliación de su cuenta al aplicativo YAPE, el mismo que fue instalado en otro dispositivo, con lo que se demuestra que la Banca Móvil promueve la clonación de datos informáticos, los mismos que son en muchas ocasiones vendidos a terceros con el fin de obtener provecho económico para sí mismo o para terceros.

Respecto de los hallazgos obtenidos en los antecedentes de investigación, Rojas (2016) en su investigación sobre la evaluación de la seguridad de aplicaciones móviles bancarias, encontró en las aplicaciones estudiadas que estas no cuentan con enlaces para reportar ingresos no autorizados, desconociendo los operadores las medidas a tomar en casos de intrusión.

Asimismo, de los resultados obtenidos en la doctrina, García (2018), Parker y Flowerday (2020) se refieren al Phishing como la técnica de ingeniería social utilizada por los ciberdelincuentes con la finalidad de obtener información personal bancaria que tiene un aspecto confidencial propio de una persona, datos que son indispensables para el registro de una cuenta a la **Banca Móvil**.

Finalmente podemos concluir diciendo que para el segundo objetivo específico conforme los detallado por los expertos quienes dieron respuesta a la guía de entrevista, las fuentes documentales, antecedentes de investigación, y doctrina respecto a la clonación de datos informáticos y seguridad de aplicaciones bancarias, se ha logrado establecer que el uso de la banca móvil promueve la

clonación de datos informáticos, porque son estos datos los necesarios e indispensables para acceder a la Banca Móvil o crear una Banca Móvil de un usuario desde un dispositivo celular diferente al del titular o en su defecto como lo visto en el análisis del Informe Policial crear una cuenta en un aplicativo móvil sin el conocimiento del titular de la cuenta, es por eso que los expertos sugirieron la implementación de nuevas medidas de seguridad para el acceso a la banca móvil como la identificación biométrica facial, dactilar y la implementación de los token confirmatorios para las transacciones realizadas desde los aplicativos móviles bancarios, de esta manera damos respuesta al segundo supuesto especifico “El uso de banca móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020”.

V. CONCLUSIONES.

En la presente investigación se ha llegado a las siguientes conclusiones:

PRIMERO: La Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa; según lo establecido por los expertos y los hallazgos encontrados en la presente investigación, debido al uso masificado de la (**Banca Móvil**) durante el año 2020 por la pandemia, instrumento que fue utilizado por los ciberdelincuentes quienes con experiencia en el manejo de tecnologías de la información TIC, lograron sustraer fondos monetarios de clientes financieros y bancarios, no pudiendo en muchas veces identificar a los autores del ilícito informático contra el patrimonio, por la pluralidad de personas necesarias para cometer este tipo de delitos y las funciones que estos desempeñan, situación que la legislación vigente no ha tomado en cuenta .

SEGUNDO: El uso de la Banca Móvil, promueve el fraude informático en la ciudad de Arequipa, 2020; toda vez que, conforme lo descrito por los expertos y los hallazgos encontrados, las aplicaciones móviles bancarias son de fácil acceso, lo cual es aprovechado por los ciberdelincuentes, quienes con la obtención de datos informáticos lograron el ingreso a la Banca Móvil de clientes bancarios quienes en muchas ocasiones no poseían las aplicaciones instaladas en sus dispositivos, siendo afiliados con total desconocimiento y con la autorización de quienes administran las mencionadas aplicaciones y los Bancos quienes poseen la información bancaria de los clientes.

TERCERO: El uso de la Banca Móvil, promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020; en razón que para realizar la afiliación a las diferentes aplicaciones móviles bancarias (Banca móvil) es necesario contar con algún dato informáticos como; número de cuenta, número de tarjeta, código CVV y fecha de vencimiento de tarjetas, información que una vez obtenida es utilizada simultáneamente por los usuarios y por los ciberdelincuentes, quienes con la información obtenida logran en segundos dejar sin fondos una cuenta bancaria.

VI. RECOMENDACIONES.

En la presente investigación se ha llegado a las siguientes recomendaciones:

PRIMERO: Conforme lo establecido en las conclusiones, para la ejecución de los Delitos Informáticos Contra el Patrimonio, es necesario la participación de dos o más personas, quienes cumplen diferentes roles para la comisión del delito, desde el acopio de datos hasta el retiro de fondos monetarios, motivo por el cual considero indispensable que el Congreso de la República emita una Ley que integre al artículo 3 de la Ley Nro. 30077 “Ley contra el crimen organizado” este tipo de delitos teniendo aún más en consideración que las penas conforme Ley de Delitos Informáticos para la modalidad tiene una pena reducida, llegando muchas veces los autores con el simple hecho de confesar el delito estar en libertad de acuerdo a los beneficios otorgados por ley.

SEGUNDO: Conforme sus atribuciones la Superintendencia de Banca, Seguros y Administración de Fondos de Pensiones, como ente rector en materia financiera y bancaria, debe regular el uso y manejo de las aplicaciones móviles bancarias, emitiendo disposiciones específicas para evitar la vulneración y asegurar un correcto manejo por parte de los clientes y seguridad por parte de los bancos.

TERCERO: Conforme los descrito por los expertos y conforme los documentos analizados, como última recomendación respecto al presente trabajo de investigación, se recomienda que las entidades Financieras y Bancarias que ofrecen dentro de sus productos las aplicaciones móviles bancarias (Banca Móvil) utilicen la identificación biométrica facial y/o dactilar como primer escalón en la seguridad para el uso y activación de los mencionados aplicativos, asimismo como como segundo escalón de seguridad usar el token digital para realizar el confirmatorio de las operaciones.

REFERENCIAS.

Alvarez, D. (2019). La paz y la seguridad internacionales en el ciberespacio. *Revista Chilena de Derecho y Tecnología*, *8*, 1–4. https://doi.org/10.5354/0719-2584.2019.55827

Alvarez, D., & Hevia, A. (2020). Protección legal para la búsqueda y la notificación de vulnerabilidades de ciberseguridad en Chile. *Revista Chilena de Derecho y Tecnología*, *9*, 1–5. https://doi.org/10.5354/0719-2584.2020.60658

Arias, J., & Valdivia, I. (2021). Satisfacción de los clientes con los canales de atencion en una entidad financiera de Arequipa. Estidio en los tiempos de covid-19. *Revista Orinoco Pensamiento y Praxis*. https://doi.org/10.6084/m9.figshare.9119978.v7

Avendaño, O. (2018). *Los retos de la banca digital en México * The challenges of electronic banking in*. *12*(41), 87–108. https://doi.org/10.17163/ret.n13.2017.02.

Baena, G. (2014). *Metodología de la Investigación*. https://books.google.com.pe/books?id=6aCEBgAAQBAJ&printsec=frontcover&dq=tipos+de+investigacion.pdf&hl=es&sa=X&ved=2ahUKEwjF-qfE6JrvAhVhH7kGHaxRBJYQ6AEwAHoECAIQAg#v=onepage&q&f=false

Benussi, C. (2020). *Obligaciones de seguridad en el tratamiento de datos personales en Chile : Escenario actual y desafíos regulatorios pendientes*. *9*, 227–280. https://doi.org/10.5354/0719-2584.2020.56660

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://dx.doi.org/10.22395//seec.v22n53a4

Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria*. http://repositorio.unfv.edu.pe/handle/UNFV/2608

Calzada, N., & Calzada, M. (2020). *Epidemiología del COVID-19 en América Latina Covid-19 epidemiology in Latin America*. *2*(2), 102–108. https://doi.org/10.37711/rpcs.2020.2.2.126

Carreño, A., & Hurtado, G. (2019). *Factores que influyen en la adopción de banca móvil en los Millennials en Lima urbana*. http://hdl.handle.net/10757/628187

Celli, S. (2019). *Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388 Modificación del Código Penal argentino*. https://repositorio.uesiglo21.edu.ar/handle/ues21/16861

Gamez, A., Mantilla, Y., & Romero, L. (2018). *DESCRIPCION DEL DESARROLLO DE LA BANCA VIRTUAL EN COLOMBIA PERIODO 2013-2017*. https://hdl.handle.net/10983/22499

García, A. (2019). *Artículos originales Las Fintech y la inclusión financiera en la era digital : El impacto en la reducción de la pobreza y la informalidad en el Perú*. *22*(2005), 67–75.

Garcia, D. (2018). *El Phishing como delito de estafa informática. Comantario a la SAP de Va,encia 37/2017*. *25*, 650–659. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025&lng=es&tlng=es

Garcia, J. (2017). las nuevas invaciones bárbaras. *Review of Global Management*, 2016–

2017. https://doi.org/10.19083/rgm.v3i2.765

Gómez, M. (2006). *Introducción a la Metodología de la investigacion cientifica*. https://books.google.com.pe/books?id=9UDXPe4U7aMC&pg=PA85&dq=DISEÑO+DE+INVESTIGACION&hl=es&sa=X&ved=2ahUKEwil8sGP58_vAhV6HbkGHeDDDo0Q6AEwBHoECAEQAg#v=onepage&q=DISEÑO DE INVESTIGACION&f=false

Herrera, J., Guevara, G., & Munster, H. (2015). Los diseños y estrategias para los estudios cualitativos. Un acercamiento teórico-metodológico. *Gac. Méd. Espirit*, *17*(2), 120–134. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S1608-89212015000200013&lng=es&nrm=iso

Kapoor, A., & Vij, M. (2020). *How to Boost your App Store Rating ? An Empirical Assessment of Ratings for Mobile Banking Apps*. *15*(1), 99–115. https://doi.org/10.4067/S0718-18762020000100108

Koray, Buber, Demir, & Diri. (2018). *Detección de Phishing basada en el aprendizaje automático a partir de URL*. https://doi.org/10.1016/j.eswa.2018.09.029

Lamas, L., & Lamas, G. (2018). *Derecho Penal Sustantivo y Adjetivo* (Instituto).

Leão, F., Brantes, J., Sabino, A., & Wernck, J. (2018). 1. introdução. *Brazilian Business Review*, *15*, 176/190. https://doi.org/10.15728/bbr.2018.15.2.5.

Leon, J. (2018). *Vacios legales que impiden la aplicacion de sanciones por Delitos Informáticos por la ley N° 30096 y modificatori en el distrito Cercado de Lima 2017*. https://repositorio.utelesup.edu.pe/handle/UTELESUP/812

Louw, C., & Nieuwenhuizen, C. (2019). *Digitalisation strategies in a South African banking context : A consumer services analysis*. 1–8. https://dx.doi.org/10.4102/sajim.v22i1.1153

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. *44*(2003), 235–260. https://dx.doi.org/10.4067/S0718-34372017000100011

Mayer, L. (2018). de los delitos informáticos *. *Ius et Praxis*, 159–206. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122018000100159&lng=es&nrm=iso%3E. ISSN 0718-0012

Mayer, L., & Oliver, G. (2020). El delito de fraude informático : Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*, 151–185. https://doi.org/10.5354/0719-2584.2020.53447

Mejía, J. (2019). Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación. *Revista Iberica de Sistemas e Tecnologias de Información*, 82–93. https://doi.org/10.17013/risti.31.82

Moncada, E. (2020). *Comparación de técnicas de machine learning para detección de sitios web de phishing*. 77–103. https://dx.doi.org/10.4102/sajim.v22i1.1176

Moreno, J., Sanchez, C., Salavarrieta, J., & Vargas, L. (2019). Technological Solutions for Fraud Prevention and design of a Transactional Risk Prevention Model for the Payment Button. *Entre Ciencia y Tecnologia*, *13*(26), 36–42. https://doi.org/10.31908/19098367.1154

Nuñez B y Carhuancho C. (2020). *COVID-19 : ¿ LA VULNERACIÓN A DERECHOS CYBER CRIME IN TIMES OF COVID-19 : VIOLATION*. *1*, 93–100.

https://doi.org/10.33539/lumen.2020.v16n1.2287

Ospina, M., & Sanabria, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global : un análisis para Colombia **. 199–217. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=es.

Palomino, G., Velasquez, K., Marcos, K., & Seclen, J. (2019). Una aproximación a partir de un estudio de casos múltiple How do Peruvian fintech innovate ? An approach from a multiple case study . *Revista de Ciencias de La Gestion*, *4*, 38–66.

Parker, H., & Flowerday, S. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal Oj Information Management*, 1–10. https://dx.doi.org/10.4102/sajim.v22i1.1176

Pérez, F., Benito, R., & Ramos, J. (2020). *Factores de crecimiento en las fintech peruanas : una caracterización en un estudio de caso múltiple Growth factors in peruvian fintech : a characterization in a multiple case study*. *5*, 118–151. https://doi.org/10.18800/360gestion.202005.005

Poma, A., & Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *Sciendo*, *22*(4), 275–282. https://revistas.unitru.edu.pe/index.php/SCIENDO/article/view/2692

Rodriguez, C., Lorenzo, O., & Herrera, L. (2005). Teoría y práctica del análisis de datos cualitativos. Proceso general y criterios de calidad. *Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM*. https://www.redalyc.org/pdf/654/65415209.pdf

Rojas, C. (2016). *EVALUACIÓN DE LA SEGURIDAD DE APLICACIONES MÓVILES BANCARIAS*. http://repositorio.uchile.cl/handle/2250/144529

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Analisis conceptual del delito informático en Ecuador. *Revista Conrado*, *17(78)*, 343–351. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122018000100159&lng=es&nrm=iso%3E. ISSN 0718-0012

Santacruz, H., & Hermoza, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. *Revista Iberica de Sistemas e Tecnologias de Información*, 391–401. https://www.proquest.com/scholarly-journals/los-delitos-informáticos-y-su-tipificación-en-la/docview/2318538897/se-2?accountid=201395

Torres, A., & Marin, P. (2017). *Gamificación en aplicaciones móviles para servicios bancarios de España*. *VII*, 27–41. https://doi.org/10.19083/rgm.v3i2.765

Useche, M., Artigas, W., & Queipo, B. (2020). Técnicas e instrumentos de recolección de datos. In *Boletín Científico de las Ciencias Económico Administrativas del ICEA* (Vol. 9, Issue 17). https://doi.org/10.29057/icea.v9i17.6019

ANEXOS

Título: “El uso de Banca Móvil en los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020”.

PROBLEMAS DE INVESTIGACIÓN	OBJETIVOS DE INVESTIGACIÓN	CATEGORÍAS	CONCEPTUALIZACIÓN	SUB CATEGORÍAS	FUENTES	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS
Problema general: ¿De qué manera el uso de banca móvil promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020? **Problemas específicos:** 1.- ¿De qué manera el uso de banca móvil promueve el fraude informático en la ciudad de Arequipa, 2020? 2.- ¿Por qué el uso de banca móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020?	**Objetivo general:** Determinar si el uso de banca móvil promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020. **Objetivos específicos:** 1.- Establecer si el uso de banca móvil promueve el fraude informático en la ciudad de Arequipa, 2020. 2.- Identificar si el uso de banca móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020.	Banca móvil Delitos informáticos contra el patrimonio	La banca móvil, es el medio por el cual se realizan operaciones bancarias a través de dispositivos celulares. Permite a los usuarios realizar operaciones desde cualquier logar cuyo requisito indispensable es la conexión a internet. Delitos cuya característica principal es el uso de herramientas tecnológicas, que recae sobre elementos incorporales e intangibles, actuando sobre máquinas y no en personas, siendo el fin la transferencia de fondos económicos de personas naturales y/o jurídicas.	Banca por mensajes SMS. Banca en aplicaciones instaladas en Smartphone. Fraude informático. Clonación de datos informáticos	Documento de trabajo 13/24, BBVA RESEARCH, 2013. Ley Nro. 30096 y su modificatoria Ley Nro. 30171 Departamento de investigación de delitos de alta tecnología - Arequipa	**TECNICAS**: - Entrevistas. - Análisis documental. **INSTRUMENTOS**: - Guía de Entrevista. - Guía de análisis documental.

GUÍA DE ENTREVISTA

Título: "**El uso de Banca Móvil en los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020".**

Entrevistado/a:……

Cargo/profesión/grado académico:……

Institución:……

Objetivo general

Determinar si el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020.

1. **¿De qué manera el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020?**

   ……
   ……
   ……..

2. **En su opinión, ¿por qué los clientes de financieros han optado por el uso de Banca Móvil?**

   ……
   ……
   ……..

3. **Desde su perspectiva, ¿qué factor ha influido para que se incrementen los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020?**

   ……
   ……
   ……..

Objetivo específico 1

Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020.

4. **De acuerdo a su experiencia, ¿de qué manera el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020?**

   ……

   ……

   ……

5. **¿En qué medida, la Banca Móvil puede considerarse un canal seguro para realizar operaciones bancarias?**

   ……

   ……

   ……

6. **¿De qué manera la pandemia ha ocasionado el aumento de los fraudes informáticos?**

   ……

   ……

   ……

Objetivo específico 2

Identificar si el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020.

7. **¿por qué el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020?**

……

……

……

8. **¿Qué mecanismos de seguridad se deben implementar para evitar la vulneración a los sistemas de Banca Móvil?**

……

……

……

9. **¿Qué medidas de seguridad deben tomar las entidades bancarias y los clientes para evitar la clonación de datos informáticos?**

……

……

……

FIRMA Y

Arequipa,……. de…….…. 2021.

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: El uso de Banca Móvil en los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020.

Autor(a): Alexandr Arturo ZAMBRANO GOMEZ.

Fecha: 17/04/2021.

Objetivo General: Determinar si el uso de Banca Móvil promueve los Delitos Informáticos Contra el Patrimonio en la ciudad de Arequipa, 2020.

Objetivo Específico N° 1: Establecer si el uso de Banca Móvil promueve el Fraude Informático en la ciudad de Arequipa, 2020.

Objetivo Específico N° 2: Identificar si el uso de Banca Móvil promueve la clonación de datos informáticos en la ciudad de Arequipa, 2020.

FUENTE DOCUMENTAL	
CONTENIDO DE LA FUENTE DOCUMENTAL	
ANÁLISIS DEL CONTENIDO DE LA FUENTE DOCUMENTAL	
CONCLUSIÓN	

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Dr Enrique Jordán Laos Jaramillo.

1.2. Cargo e institución donde labora: Docente universitario a nivel de pregrado y posgrado universidad cesar vallejo.

1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista.

1.4. Autor de Instrumento: Alexander Arturo Zambrano Gomez.

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación

- El Instrumento no cumple con Los requisitos para su aplicación

SI

IV. PROMEDIO DE VALORACIÓN :

95 %

Lima, 19 de Marzo del 2021

Enrique Jordán Laos Jaramillo
ABOGADO DE LIMA
Registro CAL 45000
Dr. en Derecho

FIRMA DEL EXPERTO INFORMANTE
DNI N°09911151Telf.: 997201314

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Ludeña Gonzales, Gerardo

1.2. Cargo e institución donde labora: Universidad Cesar vallejo

1.3. Nombre del instrumento motivo de evaluación:

1.4. Autor de Instrumento: Zamorano Gómez, Alexandr Arturo

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN :

95 %

ABOGADO
CAL 58283 CAA 347

FIRMA DEL EXPERTO INFORMANTE
DNI Nº 28223419
ORCID: 0000-0003-4433-9471
RENACYT: P0103573 – Carlos Monge Medrano – Nivel IV

UNIVERSIDAD César Vallejo

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: VARGAS HUAMÁN, Esaú

1.2. Cargo e institución donde labora: Docente y Asesor de Tesis de la Universidad César Vallejo-Filial Lima.

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

1.4. Autor de Instrumento: Zambrano Gomez, Alexandr Arturo

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN : 93 %

Lima, 13 de marzo del 2021.

FIRMA DEL EXPERTO INFORMANTE

DNI No 31042328 Telf.: 963415453