Universidad Nacional
Federico Villarreal

Vicerrectorado de
INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

"SOFTWARE OPELECT EN MÁQUINA VIRTUAL Y LA PREVENCIÓN DEL RIESGO DE FRAUDE ELECTRÓNICO EN OPERACIONES BANCARIAS DE LOS CLIENTES DE LIMA METROPOLITANA"

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN GERENCIA DE PROYECTOS DE INGENIERÍA

AUTOR
MELÉNDEZ MELÉNDEZ, JHON RIGNER

ASESOR
MG. BAZÁN BRICEÑO. JOSÉ LUIS

JURADOS
DR. MARTEL JAVIER EDWIN ANTONIO

DR. LEZAMA GONZALES PEDRO MARTIN

MG. SAL Y ROSAS JULCA MARIANO ANDRÉS

LIMA – PERÚ
2020

TESIS

“SOFTWARE OPELECT EN MÁQUINA VIRTUAL Y LA PREVENCIÓN DEL RIESGO DE FRAUDE ELECTRÓNICO EN OPERACIONES BANCARIAS DE LOS CLIENTES DE LIMA METROPOLITANA”

DEDICATORIA

A mis padres, quienes son mi motivación y fuerza motriz para lograr mis éxitos y mi competencia profesional.

RECONOCIMIENTO

Mi especial reconocimiento para los distinguidos Miembros del Jurado:

Dr. Martel Javier, Edwin Antonio

Dr. Lezama Gonzales, Pedro Martin

Mg. Sal y Rosas Julca, Mariano Andrés

Por su criterio objetivo en la evaluación de este trabajo de investigación.

Así mismo mi reconocimiento para mi asesor:

Mg. Bazán Briceño, José Luis

Por las sugerencias recibidas para el mejoramiento de este trabajo.

Muchas gracias para todos.

ÍNDICE

CÀRATULA i

TÍTULO ii

DEDICATORIA iii

RECONOCIMIENTO iv

INDICE v

RESUMEN ix

ABSTRACT x

I. INTRODUCCIÓN 11

1.1. Planteamiento del Problema 12

1.2. Descripción del Problema 12

1.3. Formulación del Problema 13

1.3.1. Problema General 13

1.3.2. Problemas Específicos 14

1.4. Antecedentes 14

1.4.1. Antecedentes Nacionales 14

1.4.2. Antecedentes Internacionales 18

1.5. Justificación de la investigación 21

1.6. Limitaciones de la investigación 24

1.7. Objetivos 24

1.7.1. Objetivo General 24

1.7.2. Objetivos Específicos 25

1.8.Hipótesis 25

1.8.1. Hipótesis General 25

1.8.2. Hipótesis Específicas 25

II. MARCO TEÓRICO 26

2.1.Marco conceptual 26

III. MÉTODO 40

3.1.Tipo de investigación 40

3.2.Población y Muestra. 41

3.3.Operacionalización de las variables 43

3.4.Instrumentos 43

3.5.Procedimientos 44

3.6.Análisis de datos 45

3.7.Consideraciones éticas 45

IV. RESULTADOS 46

V. DISCUSIÓN DE RESULTADOS 57

VI. CONCLUSIONES 64

VII. RECOMENDACIONES 65

VIII. REFERENCIAS 66

IX. ANEXOS 71

Anexo 1: Matriz de Consistencia 72

Anexo 2: Instrumento de Recolección de Datos 73

Índice de Tablas

Tabla 1. Operacionalizacion de las variables 43

Tabla 2. Confiabilidad del instrumento 45

Tabla 3. Correlaciones entre el software Opelect en máquina virtual y el riesgo de fraude electrónico en operaciones bancarias 46

Tabla 4. Correlaciones entre el software Opelect en máquina virtual y La detección de fraudes electrónicos en operaciones bancarias. 48

Tabla 5. Correlaciones entre el software Opelect en máquina virtual y el Nivel de fraude electrónico en operaciones bancarias 49

Tabla 6. En qué entidad financiera tiene cuentas bancarias 50

Tabla 7. Desde donde realiza sus transacciones bancarias 51

Tabla 8. Con qué frecuencia realiza operaciones electrónicas bancarias 52

Tabla 9. Tiene conocimiento las medidas de seguridad en las operaciones electrónicas bancarias 53

Tabla 10. Ha sido víctima de fraude en operaciones electrónicas bancarias 54

Tabla 11. Conoce usted la modalidad fraudulenta empleada 55

Tabla 12. Utilizaría un software Oplelect para reducir el peligro de fraude electrónico 56

Índice de Figuras

Figura 1. Diagrama de procesos del Software Opelect. 27

Figura 2. En qué entidad financiera tiene cuentas bancarias 50

Figura 3. Desde donde realiza sus transacciones bancarias..... 51

Figura 4. Con qué frecuencia realiza operaciones electrónicas bancarias..... 52

Figura 5. Tiene conocimiento las medidas de seguridad en las operaciones electrónicas bancarias 53

Figura 6. Ha sido víctima de fraude en operaciones electrónicas bancarias 54

Figura 7. Conoce usted la modalidad fraudulenta empleada..... 55

Figura 8. Utilizaría un software Oplelect para reducir el peligro de fraude electrónico 56

RESUMEN

El objetivo del presente trabajo de investigación, fue determinar si el software Opelect en máquina virtual ayudara a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana. Bajo la metodología que se empleó para la recolección de datos, que fue la entrevista a 246 personas que viven en Lima metropolitana y utilizan el sistema electrónico bancario de los bancos BCP, BBVA, Interbank, Scotiabank, Banco de la Nación, cuyo cuestionario, se realizó bajo la escala de Likert. El modelo aplicado para la investigación es no experimental con un tipo descriptivo - correlacional. Como resultado se determinó que el software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana, esto debido a que se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825 y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05.

Palabras clave: Software, Operación Bancaria, Máquina Virtual, Fraude, Entidad bancaria.

ABSTRACT

The objective of this research work was to determine if Opelect software in virtual machine would help to prevent the risk of electronic fraud in banking operations of Lima Metropolitan customers. Under the methodology used for data collection, which was the interview to 246 people living in metropolitan Lima and use the banking electronic system of banks BCP, BBVA, Interbank, Scotiabank, Banco de la Nación, whose questionnaire is performed under the Likert scale. The applied model for the investigation is non experimental with a descriptive - correlational type. As a result, it was determined that Opelect software in a virtual machine would significantly help to prevent the risk of electronic fraud in banking operations of customers in Metropolitan Lima, due to the fact that a Spearman's Rho correlation coefficient was obtained, which has the value of 0.825 and the sigma (bilateral) is 0.002, which is less than the theoretical parameter of 0.05.

Key words: Software, Bank Operation, Virtual Machine, Fraud, Bank Entity.

I. INTRODUCCIÓN

Actualmente el sistema financiero peruano está siendo impactado por eventos relacionados a fraudes, a pesar de ser uno de los sistemas más antiguos y con mayor evolución en el país, desde su nacimiento en el XIX en los tiempos de bonanza del guano, donde los problemas surgían por la facilidad de falsificación de billetes, debido a que solo se contaba con herramientas rudimentarias para su elaboración. En el presente con la automatización de los procesos financieros y la virtualización de sus productos y servicios que se iniciaron aproximadamente el año 1993 en adelante, surgieron fraudes cibernéticos.

El desarrollo integral de la investigación consta de nueve capítulos, los cuales se escriben a continuación:

Se conformada por el planteamiento del problema, la descripción del problema, los antecedentes, justificación, limitaciones, objetivos e hipótesis que comprendió la elaboración de la presente tesis. Comprende al marco teórico el cual abarca el desarrollo de la temática correspondiente al tema y la definición conceptual de la terminología.

El método que corresponde al análisis de la hipótesis del trabajo, se muestran los resultados. Se observarán las discusiones, las conclusiones y recomendaciones. Además, las referencias bibliográficas empleadas que contemplen la investigación y que han facilitado el desarrollo de la tesis, como también la recolección de datos y los anexos.

1.1. Planteamiento del Problema

El crecimiento y desarrollo de la globalización a nivel mundial permitió la intervención de la tecnología en todos los aspectos de las operaciones electrónicas que cada empresa ha optado como mecanismos de atención para sus clientes y que permiten que se consoliden dentro del sistema financiero global pero que los han convertido en un sistema vulnerable para diversos actos delictivos. Algunos de estos mecanismos es el intercambio comercial electrónico y el servicio de banca por internet que fue implementado por las entidades financieras, sin embargo, este avance fue también aprovechado por organizaciones criminales para cometer, lo que se conoce como Fraude Electrónico en Operaciones Bancarias a través de las modalidades delictivas conocidas como: Phishing y Pharming.

El desarrollo de la banca electrónica y el manejo del dinero electrónico ya poseen un lugar indispensable en cada banco existente y con estos se pretenden contribuir a mejorar la eficiencia del sistema bancario, permitiendo que se eleve la productividad y el bienestar de sus clientes ya que se podrían incrementar la eficiencia con la que realizan y reciben pagos.

1.2. Descripción del Problema

En los últimos años el fraude bancario a través de operaciones electrónicas se ha incrementado hasta en un 90%, según las estadísticas obtenidas de la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI PNP, se supo que en el año 2013 de las236 denuncias reportadas el 97% fueron a través de la modalidad de Pharming y el 3% a través de la modalidad de phishing, generando un perjuicio económico de S/. 2.025.183,00 soles; para el año 2014 se reportaron 210 denuncias

de los cuales el 85% fueron a través de la modalidad de Pharming y el 15% a través de la modalidad de phishing, generando un perjuicio económico de S/. 4.620.340,00 soles; para el 2015 de las 156 denuncias el 80% fueron a través de la modalidad de Pharming y el 20% a través de la modalidad de phishing, generando un perjuicio económico de S/. 1.315.165,00 soles; en el año 2016 de 1004 denuncias 8% fueron por modalidad de Pharming y el 92% a través de la modalidad de phishing, generando un perjuicio económico de S/. 22.602.419,14 soles y finalmente en el año 2017 se han reportado 1231 denuncias siendo el 100% por medio modalidad de phishing, lo cual ha generado un perjuicio económico de S/. 8.865.143,3 soles.

De acuerdo a lo expuesto, esto se debe al incremento de operaciones que los clientes realizan a través de la banca por internet, el cual es aprovechado por los ciber delincuentes quienes a través de Pharming y phishing obtienen información de las cuentas bancarias de sus víctimas para ser utilizadas indebidamente. Además, cabe resaltar que según el Decreto Ley N° 25868- (Ley de Protección del Consumidor) y el Decreto Legislativo 6915, se deben establecer diversas normas referidas a la defensa de los derechos del consumidor sino las entidades bancarias se verían envueltas en problemas legales justamente impuestas por sus clientes o usuarios.

1.3. Formulación del Problema

1.3.1. Problema General

¿El software Opelect en máquina virtual ayudara a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana?

1.3.2. Problemas Específicos

¿El software Opelect en máquina virtual ayudara a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana?

¿El software Opelect en máquina virtual ayudara a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana?

1.4. Antecedentes

1.4.1. Antecedentes Nacionales

García y Enero (2018) elaboraron una investigación titulada "*Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú"* en la ciudad de Lima, Perú.

La presente investigación tuvo por objetivo principal brindar una herramienta informática a las organizaciones financieras, específicamente a la red de tiendas, agencias u oficinas de estas entidades; de este modo, poder controlar los fraudes en la ejecución de los procedimientos bancarios, así como también permite gestionar y dar seguimientos mediante la generación de logaritmos en las transacciones que serán derivados al área de riesgos. Para realizar este control y prevención de fraude, se desarrollaron mecanismos informáticos por medio de los cuales se realizará el bloqueo de operaciones para los colaboradores (cajeros) en las transacciones, en las que implique el uso de sus propias cuentas o su documento de identidad. Como conclusión se obtuvo que el sistema de información que se implementó ayudo a mitigar el fraude en la red de tiendas de la entidad bancaria, a su vez, el modelo sistema de información propuesto es viable, factible y deseable para su implementación.

Balcázar (2017) elaboró una investigación titulada "*Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito*" en la ciudad de Trujillo, Perú.

La presente investigación tuvo como objetivo principal Determinar qué medidas de seguridad deben incorporarse en la Resolución Nº 6523-2013-SBS, para evitar las operaciones no reconocidas en tarjetas de crédito y débito, a fin de proteger adecuadamente al consumidor financiero. Si bien, estos productos financieros al ser utilizados a través de sus diferentes plataformas físicas o virtuales generan ventajas y beneficios a los usuarios de las entidades bancarias y financieras; las presentes tarjetas también traen consigo desventajas; puesto que, con el transcurso de los años al avanzar la tecnología, existen los terceros inescrupulosos que se encargan a través de métodos fraudulentos de obtener los datos de las tarjetas de crédito o de las tarjetas de débito de los usuarios. Como conclusión se obtuvo que las medidas de seguridad a incorporarse en la resolución 6523-2013 "Reglamento de tarjetas de crédito y débito", es el uso del sistema biométrico; ya que, con ello se evitaría las operaciones no reconocidas de las tarjetas de crédito y débito, de tal manera se brindaría una adecuada protección al consumidor financiero; asimismo, se debe priorizar el reforzamiento de las áreas de monitoreo de las entidades bancarias y financieras.

Ñaupas (2016) elaboró una investigación titulada *"Minería de datos aplicada a la detección de fraude electrónico en entidades bancarias"* en la ciudad de Lima, Perú.

La presente investigación tuvo por objetivo principal Implementar un modelo basado en técnicas de Minería de Datos que permitirá clasificar las transacciones

realizadas en los canales de banca por internet o banca móvil como fraudulentas o integras, por medio de la aplicación de un proceso de descubrimiento de conocimientos en bases de datos, mediante la aplicación de algoritmos arboles de clasificación. El desarrollo de las nuevas tecnologías hace que las entidades financieras avancen a la par con ellas y ofrezcan a sus clientes diversos medios y aplicaciones que les faciliten realizar sus transacciones financieras, sin embargo, esto es atractivo no solo para los clientes sino también para los defraudadores pues hace que cada vez existan más maneras de cometer fraudes. De esta manera se concluyó que las técnicas predictivas resultan eficientes para descubrir conocimientos y permiten inferir como una variable o atributo puede incidir en otros.

Rojas (2013) elaboró una investigación titulada *"La Seguridad de la banca electrónica y la defensa efectiva del consumidor financiero en la legislación peruana y colombiana"* en la ciudad de Lima, Perú.

La presente investigación tuvo como objetivo principal establecer si existe una debida protección del derecho a la idoneidad del servicio financiero y un tercero acceder a la banca electrónica y ocasionar un daño al consumidor financiero establecido en INDECOPI. El avance de la banca electrónica está progresando hoy en día dado que la penetración de Internet es un hecho ineludible pero la tecnología, así como otorga las ventajas también tiene que hacer frente a una serie de riesgos. En las transferencias electrónicas bancarias. Como conclusión se obtuvo que efectivamente no existe una debida protección del derecho a la Identificación del servicio financiero en INDECOPI si un tercero (hacker) accede a la Banca Electrónica y ocasiona un daño al consumidor financiero. Esto se debe a la principal razón de ser sólo para ser útil en el despliegue informativo y los usuarios deben ser

responsables de una conducta diligente en la prestación de servicios de banca electrónica.

Martínez (2017) elaboró un artículo titulado *"Medidas de seguridad que evitan fraudes en el comercio electrónico*" en el distrito de Ate, Perú.

El presente artículo tuvo como objetivo informar las medidas de seguridad pertinentes que toda empresa con presencia comercial en Internet debe implementar en sus servidores web reduciendo considerablemente los intentos de robo de información bancaria haciendo uso de sistemas anti fraude basados en criptografía de altos niveles de cifrado. Los elevados índices de fraudes a nivel internacional demuestran que existe una baja inversión por parte de las empresas en la seguridad de sus tiendas online, alertando así a que los avances de las tecnologías ofrezcan cada vez soluciones más sólidas frente a la futura y alta demanda respecto a sistemas de seguridad antifraude se refiere. Como conclusión se obtuvo que las empresas para evitar fraudes en el comercio electrónico deben recibir información sobre las medidas de seguridad que deben optar, haciendo uso de las diferentes capas de seguridad que se pueden ir implementando progresivamente de acuerdo al crecimiento y necesidad de la empresa.

1.4.2. Antecedentes Internacionales

Bravo y Pico (2016) elaboraron una investigación titulada *"Evaluación de manuales de procedimientos para prevenir riesgos, errores y fraudes contables*" en la ciudad de Guayaquil, Ecuador.

La presente investigación tuvo como objetivo general determinar la importancia de los diferentes manuales de aplicación a ser estudiados cumplan con las normas internacionales de información financiera además de los procedimientos establecidos para las empresas de servicios en el área contable. El desarrollo económico que tenga una empresa no solo depende de un buen manejo administrativo, sino también de las estrategias para aplicar estos procedimientos que ayuden al desarrollo de cada una de las actividades del área contable sin el cometimiento de errores o fraudes contables, cada empresa debe contar con métodos, procedimientos y programas de revisión constante, estableciendo procesos y controles que ayuden al usuario a lograr un mejor desenvolvimiento y manejo de sus tareas logrando así un trabajo eficiente y disminuyendo la ocurrencia de errores que pueden volver vulnerable el área contable de la empresa. Como conclusión se obtuvo que la mayoría de empresas de servicios en la ciudad de Guayaquil no cuenta con un manual de procedimientos antifraudes. Con la ayuda de los mecanismos y procedimientos diseñados, será posible minimizar el impacto de los riesgos errores y fraudes en la información presentada en los estados financieros.

Paredes (2014) elaboró una investigación titulada *"El fraude en cajeros automáticos mediante clonación de tarjetas débito y crédito"* en la ciudad de Bogotá, Colombia.

La presente investigación tuvo como objetivo principal dar a conocer la problemática que se presenta día a día, del fraude en cajeros automáticos en el sistema financiero colombiano, mediante clonación de tarjetas debido y crédito. El análisis realizado comprende desde la implementación del primer cajero en la historia mundial hasta la influencia de los mal llamados delitos financieros y en las operaciones transaccionales de tarjetahabientes. Identificaron las principales recomendaciones de seguridad tanto en el momento de recibir el plástico, como en el que es utilizado en los cajeros automáticos, principalmente en gasolineras y restaurantes, sitios de mayor preferencia del actuar delincuencial, después de los propios cajeros automáticos. Como conclusión se obtuvo que a lo largo de la historia y desde el invento de los cajeros automáticos, se ha visto cómo estos han evolucionado en seguridad, en seguridad integral, tanto en elementos físicos como tecnológicos y de software, siempre tratando de brindar y ofrecer tranquilidad a los clientes, quienes al final de la cadena son los directos consumidores de este tipo de servicio.

Rodríguez (2013) elaboró una investigación titulada "*Guía general de aplicación de las medidas mínimas de seguridad exigidas a las entidades financieras y de transporte de valores en el Ecuador*" en la ciudad de Sangolqui, Ecuador.

La presente investigación tuvo como objetivo principal elaborar una guía general de la aplicación de las medidas mínimas de seguridad exigidas a las entidades bancarias y de transportes de valores del Ecuador, a través de la integración ordenada y sintetizada de los conceptos más importantes y necesarios, considerando la legislación vigente sobre seguridad bancaria y transporte de valores a disposición

de los consultores, para establecimiento de medidas de prevención y protección optimas en las actividades del transporte de valores y seguridad bancaria. Como conclusión se obtuvo que La normativa legal exige a todas las entidades que conforman el sistema financiero las mismas medidas mínimas de seguridad sin hacer distinción alguna entre los distintos tipos de instituciones que conforman el sistema financiero. Así mismo se sabe que ninguna institución financiera transporta sus valores por sus propios medios, estos utilizan el servicio de transporte de valores ofrecido por las empresas de seguridad que brindan este servicio.

Aravena y Cifuentes (2013) elaboraron una investigación titulada *"Políticas de riesgo financiero banco Santander y Retail Falabella*" en la ciudad de Chillan, Chile.

La presente investigación tuvo como objetivo principal Comparar las Políticas y Normas seguidas por Banco Santander y Retail Falabella para el Análisis de Riesgo Financiero de su cartera de crédito. La filosofía de gestión de riesgos debe ser consistente con la estructura del negocio, buscando en todo momento la creación de valor para el accionista a través de la utilización eficiente del capital asignado a las unidades de negocio. Uno de los pilares fundamentales de la gestión de los riesgos estructurales es la correcta atribución y segregación de funciones que permitan garantizar un marco de responsabilidades y de comunicación apropiados. Como conclusión se obtuvo que ambas compañías cuentas con mediciones de los diferentes riesgos financieros por medio de la provisión, las cuales se da mucha importancia a las colocaciones en el mercado y además un control exhaustivo a las cuentas que ingresan a morosidad en los diferentes tramos de vencimiento, a la vez aplicando las mejores herramientas de recuperaciones mes a mes.

Núñez (2013) elaboró una investigación titulada *"Fraude al sistema financiero y a sus clientes"* en la ciudad de Quito, Ecuador.

La presente investigación tuvo como objetivo general Conocer cuáles son actualmente las principales modalidades delictivas que afectan al sistema financiero y a sus clientes, así presentar un plan de mitigación de riesgos las cuales ayuden a disminuir los riesgos que posee el sistema financiero. En el Ecuador los tipos de fraudes han crecido cada año debido a que el país posee una moneda muy valorada en el mundo como lo es el Dólar Americano, así los hackers y/o delincuentes con sus bandas organizadas se han ubicado en nuestro país. Los clientes conocen muy poco sobre los métodos de fraudes que existen en la actualidad y como evitarlos. Como conclusión se obtuvo que los fraudes en los cajeros automáticos o ATMS ha ido creciendo en los últimos años de forma significativa, esto debido a la gran vulnerabilidad en las claves de las tarjetas de los clientes, pero son varios los tipos de fraudes que afectan al sistema financiero cada año, estos son los más utilizados por los antisociales: En año pasado fraudes como ATM's – Duplicación de Tarjetas, causaron el 50% de las pérdidas totales, cheques falsificados microborrado con el 10%, fraudes tarjetas de crédito con el 7%, otros activos/faltantes de caja.

1.5. Justificación de la investigación

La realización de esta investigación radica en proporcionar una orientación para cada autoridad de supervisión relacionada con los métodos de identificación, evaluación, gestión y control de los riesgos asociados con la banca electrónica y el dinero electrónico en las organizaciones bancarias.

1.5.1. Justificación teórica.

La investigación reunirá información acerca de cada variable utilizada para su elaboración desde la implementación e información sobre el software OPELECT hasta la prevención del riesgo de fraude electrónico. Se planteará un caso empresarial al estudio que quedará a disposición de los investigadores. Además, servirá para confirmar la teoría respecto alsoftware OPELECT y su relación con la prevención del riesgo de fraude electrónico.

1.5.2. Justificación metodológica.

El desarrollo de esta investigación tendrá una justificación metodológica importante, se efectuará un estudio de análisis descriptivo y explicativo, donde se buscará proponer una herramienta a través de un software el cual permitirá indagar con mayor profundidad la problemática y podrá ser aplicada en cualquier otro trabajo de investigación que guarde relación con el tema en desarrollo.

1.5.3. Justificación social.

Esta investigación beneficiará a todos los clientes de los bancos que realizan operaciones bancarias a través métodos electrónicos, ya que la implementación del Software OPELECT en Máquina Virtual a Nivel de usuario, generará confianza en las operaciones bancarias a través de internet, permitirá buscar métodos de seguridad para el bienestar de cada uno. Además, ayudará a los mismos bancos a salvaguardar su integridad y confianza con cada cliente o futuro cliente cuyo efecto permitirá el incremento de las operaciones bancarias y reducirá el número de denuncias.

1.5.4. Justificación económica.

El trabajo de investigación se presenta y se justifica debido a que en la actualidad el fraude bancario se ha incrementado en más del 90 % con respecto a los últimos 5 años conforme se puede apreciar en el siguiente cuadro.

ITEM	2013	2014	2015	2016	2017
Denuncias	236	261	356	1004	1231
Soles	2.025.183,00	4.620.340,00	1.315.165,00	22.602.419,14	8.865.143,3
Dólares	341.752,00	685.856,00	297.375,00	992.059,41	4.219.822,80

Fuente: Elaboración Propia

Con la implementación del Software OPELECT Máquina Virtual a Nivel de usuario se busca reducir las pérdidas económicas tanto para clientes como para las mismas entidades bancarias de Lima Metropolitana.

1.5.5. Importancia de la investigación.

La importancia de esta investigación radica en el hecho de analizar la responsabilidad que debe poseer cada entidad financiera en relación a la seguridad de sus clientes que opten por realizar operaciones electrónicas bancarias, ya que conforme a la ley general del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual-INDECOPI está facultado para exigir el cumplimiento de normas relativas a la competencia, la protección del consumidor y los derechos de propiedad intelectual, en todos los sectores e industrias, incluidos los servicios financieros. De las cuales se incluyen la potestad de realizar investigaciones, adoptar medidas correctivas e imponer sanciones.

1.6. Limitaciones de la investigación

Limitaciones bibliográficas

La bibliografía para la presente investigación es escasa en casos nacionales, lo que generó que no se encuentren muchos trabajos que analicen la responsabilidad ciudadana y el medio ambiente en lima metropolitana.

Limitación teórica

La ausencia moderada de trabajos con antecedentes relacionados al tema de investigación tanto en facultades de pre grado y post grado de las principales universidades del país.

Limitación económica

El limitado financiamiento económico para la realización e implementación del estudio, tanto para la adquisición de material de información o la asesoría de especialistas del campo y así realizar la investigación.

1.7. Objetivos

1.7.1. Objetivo General

Determinar si el software Opelect en máquina virtual ayudara a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

1.7.2. Objetivos Específicos

Determinar si el software Opelect en máquina virtual ayudara a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Determinar si el software Opelect en máquina virtual ayudara a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

1.8. Hipótesis

1.8.1. Hipótesis General

El software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

1.8.2. Hipótesis Específicas

El software Opelect en máquina virtual ayudara de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

El software Opelect en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

II. MARCO TEÓRICO

2.1. Marco conceptual

2.1.1. Software Opelect

Es un software desarrollado en el lenguaje de programación Power Builder versión 11 y JavaScript, diseñado de acuerdo a la necesidad del usuario que realiza operaciones electrónicas bancarias a través de internet; el software tiene un diseño de fácil acceso e interacción con el usuario el cual permitirá realizar operaciones electrónicas de manera sencilla, rápida y segura a través de las entidades financieras Banco de Crédito del Perú, Banco Interbank, Banco Scotiabank, BBVA Continental y Banco de la Nación. Para realizar operaciones electrónicas a través de internet, el cliente ingresa al software OPELECT donde elige la entidad financiera y automáticamente el motor de búsqueda del OPELECT establece conexión con el portal web oficial de la entidad financiera elegida; durante el proceso de conexión el software bloquea cualquier acceso no autorizado al portal web oficial, estableciendo una conexión directa y segura con la entidad financiera.

Fuente: Elaboración propia

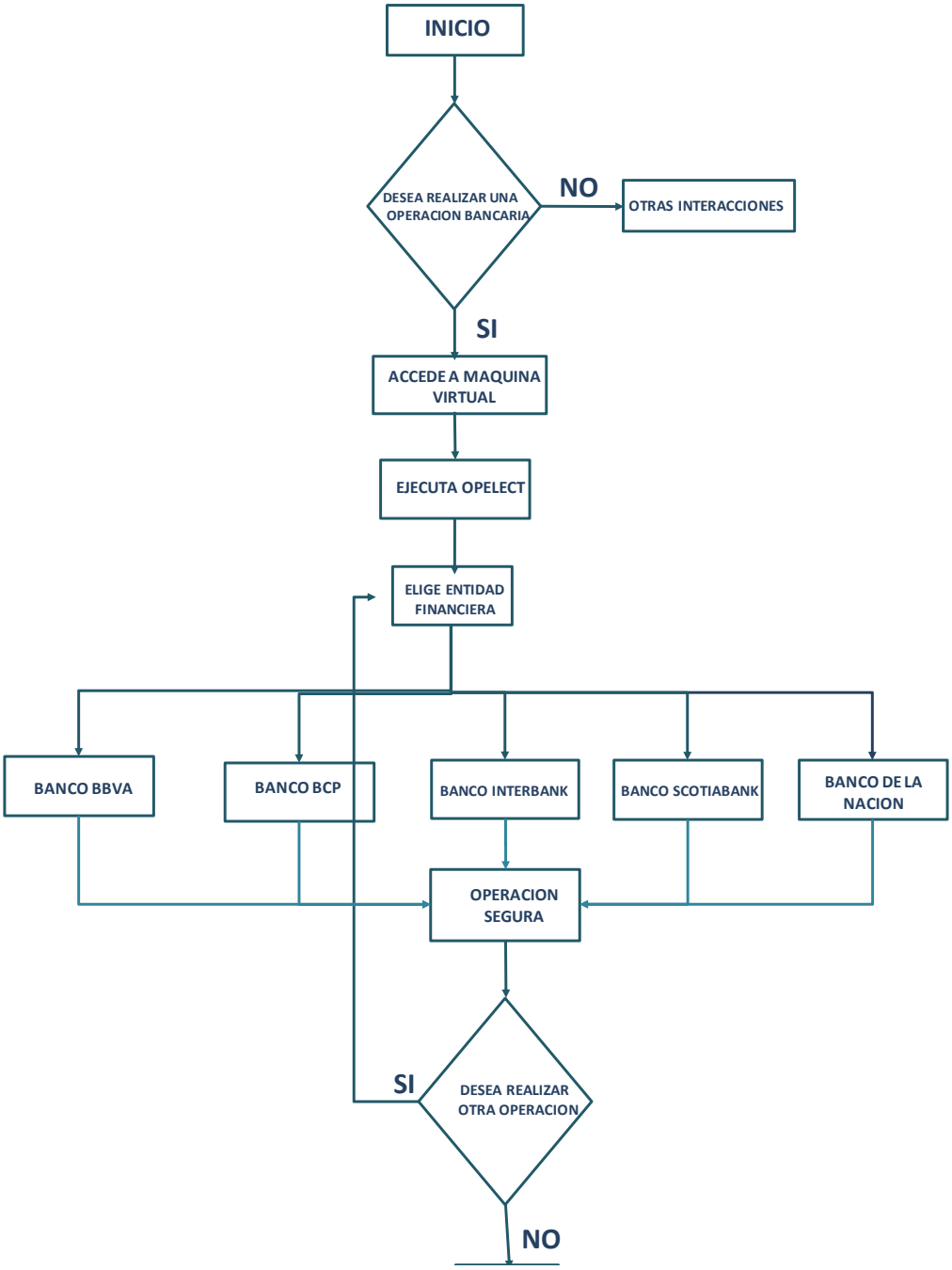


Figura 1. Diagrama de procesos del Software Opelect.

2.1.2. Banca por internet o en línea.

Felicidad (2015)

La banca por Internet es, por consiguiente, un servicio ofrecido por las entidades a sus clientes y comprende las herramientas tecnológicas que ofrece la entidad financiera para que sus usuarios hagan las operaciones bancarias a

través del ordenador, utilizando su conexión a Internet. Situamos pues la banca por Internet como un tipo de banca a distancia que oferta la mayoría de los productos que se encuentran en las oficinas junto a nuevos servicios de valor añadido solo posibles mediante este canal. Son varios los nombres con los que se conoce a la banca por Internet: e-banca, banca directa, banca interactiva. Todos ellos hacen referencia a una banca que utiliza Internet como un canal de comunicación complementario a los tradicionales. Se reserva el nombre de banca virtual para referirnos a la banca que oferta sus servicios bancarios exclusivamente a través de Internet, inicialmente sin sucursales físicas. A veces se hace referencia a este tipo de banca como banca online. En sentido estricto, la banca por Internet se limita al uso de un protocolo de comunicaciones que permite el acceso a la información en tiempo real. En este sentido es similar a los cajeros automáticos implantados con gran éxito desde mediados de los setenta, aunque Internet cuenta con diferencias tecnológicas importantes que afectan a la seguridad de las transacciones y, por tanto, a la percepción que los clientes tienen del servicio, ya que se trata de un sistema abierto basado en aplicaciones de sistemas operativos públicos, más expuestos y menos seguros. Internet representa para la banca comercial tradicional una reconfiguración de los canales convencionales en los que existe una interacción directa cliente-proveedor, y de las estrategias de marketing empleadas. Es una manifestación más de un conjunto de innovaciones que afectan a la organización de las entidades bancarias, la definición de nuevas estrategias de mercado, de nuevos retos competitivos y, sobre todo, la introducción de nuevos productos y servicios bancarios. Además, requiere capacidades tecnológicas, profesionales, financieras y de marketing con las que no cuenta la banca tradicional, todo ello

para alcanzar sus principales retos: conseguir mayor número de clientes, y fidelizar a los ya existentes.

2.1.3. Operaciones bancarias de los diferentes bancos del Perú.

2.1.3.1. BBVA

BBVA Continental (2017)

Según el BBVA Banco Continental Banca por Internet es un canal electrónico que permite realizar tus consultas y operaciones por internet, sin preocupaciones desde cualquier lugar del mundo y sin ir al banco.

2.1.3.2. Banco de Crédito del Perú.

BCP (2017)

Según el Banco de Crédito del Perú, a través de Banca por Internet BCP podrás realizar las mismas operaciones que realizas en sus agencias, pero desde la comodidad de tu casa u oficina de forma rápida y segura.

Con Banca por Internet puedes realizar transferencias, operaciones y revisar los saldos y movimientos de tus cuentas y Tarjetas de Crédito. Para poder acceder a nuestra Banca por Internet necesitas entrar con una clave de internet (clave de 6 dígitos), que te permitirá revisar tus saldos y movimientos. Además, por temas de seguridad tendrás que obtener tu clave digital Token en cualquiera de nuestras agencias para poder concretar tus operaciones.

2.1.3.3. Scotiabank.

Scotiabank (2017)

En tu casa u oficina podrás realizar operaciones bancarias en forma confidencial y segura sin ir al banco. Las operaciones que pueden realizar sus clientes son:

- Afiliación a alertas y avisos sms.
- Transferencia a cuentas propias, de terceros, otros bancos y al exterior,
- Programa tus operaciones frecuentes para que se realicen en la fecha indicada,
- Pago de tarjeta de crédito propias, de terceros, otros bancos y tarjeta única,
- Pago de servicios públicos e instituciones con cargo a cuentas o tarjeta de crédito,
- Recarga Virtual Claro, Movistar, Entel y Bitel.
- Recibe ofertas de préstamos, tarjetas y otros productos,
- Realiza tus operaciones mensuales utilizando nuestro carrito de compras y alertas de pagos.

2.1.3.4. Interbank

Interbank (2017)

El banco Interbank tiene implementado el servicio de Banca por Internet para empresa desde donde sus clientes podrán consultar saldos y movimientos, autorizar operaciones pendientes, revisar autorizaciones anteriores.

2.1.3.5. Banco de la Nación

Banco de la nación (2017)

El banco de la Nación utiliza la denominación de multired virtual que ofrece su servicio de banca por internet desde donde utilizando la Tarjeta Multired Global Debito sus clientes podrán realizar la Consulta de Saldos y Movimientos de Cuentas de Ahorro M.N y M.E; Consulta de saldos y movimientos de cuenta de compensación por tiempo de servicios - CTS M.N y M.E; consulta de código de cuenta interbancario CCI M.N y M.E; Consulta Anual de ITF M.N y M.E; consulta de saldo de préstamo personal; consulta de cronograma de pagos de préstamo personal; Bloqueo de Tarjeta. Con la tarjeta Multired Global Debito, clave de internet de 6 dígitos y clave dinámica con lo cual sus clientes podrán realizar Transferencias al Mismo Banco con cargo a Cuentas de Ahorros M.N. y M.E, transferencias Interbancarias diferidas con cargo a Cuentas de Ahorros M.N. y M.E.

2.1.4. Medidas de seguridad en operaciones electrónicas.

BBVA (2017)

Las entidades financieras más comunes de nuestro país tales como: BBVA Banco Continental, Banco de Crédito del Perú, Banco Scotiabank, Banco Interbank y el Banco de la Nación, como medida de seguridad para sus clientes han lanzado al mercado la clave digital o Token que es un dispositivo creado para prevenir el riesgo de fraude electrónico en operaciones a través de internet.

Asimismo, otra de las medidas de seguridad es la clave SMS que permite a los clientes realizar tus consultas y transacciones de Banca por Internet y App Banca Móvil desde donde te encuentres, a través de una PC, laptop o Smartphone. Solo tienes que ingresar el número de tu celular (Movistar, Claro o Entel) en los cajeros automáticos que se encuentran a nivel nacional a través de la opción Clave SMS.

2.1.5. Fraude bancario.

García & Enero (2018)

Es acción intencional que realizan una o varias personas de la entidad, ya sea los empleados, terceros o hasta la misma gerencia que conlleve a la utilización del fraude con el objetivo de conseguir ventaja injusta o ilegal.

2.1.5.1. Prevención de fraudes.

Merizalde & Zapata (2014)

Mejorar el control administrativo, implementar prácticas y políticas de control, analizar los riesgos que motiven a un fraude, tener la mejor gente posible.

2.1.5.2. Detección de fraudes.

Merizalde & Zapata (2014)

- Observar, probar o revisar los riesgos específicos de control, identificar los más importantes y vigilar constantemente su adecuada administración,
- Simular operaciones,

- Revisar constantemente las conciliaciones de saldos con bancos, clientes, etc.
- Llevar a cabo pruebas de cumplimiento de la eficacia de los controles.

2.1.5.3. Causas y efectos del fraude.

Urbina (2005)

- Autopréstamos mediante empresas de fachada
- Captaciones de dinero sin evaluar su origen y a altas tasas de interés
- Absorción de empresas con créditos obtenidos
- Inversiones a conveniencia con comisiones de por medio y con alto riesgo
- Dilatación de créditos aprobada por juntas directivas con intereses personales y manipuladores de sus órganos de control
- Flexibilidad de controles por parte de los organismos del estado
- Presentación de balances maquillados, sin el cumplimiento de principios básicos de contabilidad relacionados con la provisión, clasificación real de la cartera, patrimonio técnico, etc.
- Auditorías realizadas con procedimientos limitados en cuanto al alcance y a la independencia mental.

2.1.5.4. Tipos de fraudes bancarios.

Nuñez (2013)

Fraudes internos: Son cometidos por los empleados de una empresa, sacan provecho de su conocimiento e información que manejan para su beneficio. Fraudes externos: Son cometidos por personas externas a la empresa que no tienen relación alguna. Fraudes mixtos: Este tipo de fraude es cometido por personas externas con la colaboración de empleados de la empresa.

2.1.5.5. Phishing.

Valle (2013)

El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo". A quien lo practica se le llama phisher. También se dice que el término phishing es la contracción de password harvesting fishing (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que la escritura 'ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua forma de hacking telefónico conocida como phreaking.

El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

2.1.5.5.1. Phishing telefónico.

Gonzales & Peña (2012)

Se pueden recibir llamadas telefónicas donde la persona que habla se identifica como trabajador de un organismo público o privado solicitando datos privados de la víctima.

2.1.5.5.2. Phishing por mensaje de texto.

Leguizamón (s/n)

Esta estafa es menos común. Aquí se utilizan empresas proveedoras de correo y mensajería para efectuar el phishing y así conseguir información privada del usuario. Por ejemplo, la víctima recibe un email de la empresa DHL informándole que ha recibido un paquete y le solicita sus datos.

Gonzales & Peña (2012)

Se recibe un mensaje donde se solicitan datos personales para poder recibir un premio o tiempo aire gratis.

2.1.5.6. Pharming.

Gonzales & Peña (2012)

Consiste en manipular las direcciones del servidor de nombres de dominio o DNS por sus siglas en ingles. Cuando un usuario teclea una dirección en su navegador de internet, ésta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de

nombres, y de ello se encargan los servidores DNS. Sin embargo, utilizando ciertos tipos de malware que modifican el sistema de resolución de nombres local, ubicado en el archivo HOSTS, es capaz de redirigir a una página falsa incluso aun cuando el usuario haya tecleado la dirección en el navegador.

2.1.5.7. Key Logger

Borghello (2006)

Como su nombre lo indica un Keylogger es un programa que registra y graba la pulsación de teclas (y algunos también clicks del mouse). La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas.

2.1.6. Legislación peruana aplicada al fraude bancario.

Ley30171 (2014)

El fraude electrónico se encuentra tipificado en la Ley 30096 Ley de Delitos Informáticos, promulgada el 22 de octubre del 2013, la misma que fue modificada el 10 de marzo del 2014 por la Ley 30171 Ley de Delitos Informáticos. Cabe significar que antes de promulgarse las layes Nro. 30096 y Nro. 30171, Ley de Delitos Informáticos, el delito de fraude bancarios estaba tipificado en el artículo 207 y Articulo 186 del Código Penal Peruano.

2.1.7. Máquinas virtuales.

Camazon (2011)

Una máquina virtual está formada por un BIOS y un conjunto de recursos hardware (memoria, procesador, disco duro virtual, etc.) que se utilizan corno si fuera la maquina física. Dentro de una máquina virtual se puede instalar cualquier sistema operativo, siempre y cuando el programa para virtualizar soporte ese sistema operativo. Desde las máquinas virtuales se puede imprimir, usar los dispositivos USB, navegar por la red, etc.

2.1.8. Software para crear máquinas virtuales.

Pressman (2010)

Es el producto que construyen los programadores profesionales y al que después le dan mantenimiento durante un largo tiempo. Incluye programas que se ejecutan en una computadora de cualquier tamaño y arquitectura, contenido que se presenta a medida que se ejecutan los programas de cómputo e información descriptiva tanto en una copia dura como en formatos virtuales que engloban virtualmente a cualesquiera medios electrónicos. La ingeniería de software está formada por un proceso, un conjunto de métodos (prácticas) y un arreglo de herramientas que permite a los profesionales elaborar software de cómputo de alta calidad.

2.1.8.1. VM ware

Vilca (2016)

VMware Inc., es una filial de EMC Corporation (propiedad a su vez de Dell Inc) que proporciona software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X que corre en procesadores Intel, bajo el nombre de VMware Fusion.

2.1.8.2. Oracle.

Camazon (2011)

Oracle ofrece varias soluciones de alto rendimiento para virtualizar, algunos ejemplos son Oracle VM Server, Oracle Virtual Desktop Infrastructure, Oracle VM. VirtualBox, etc. (Camazon, 2011)

Uno de los principales productos es VirtualBox, un hipervisor de tipo 2 que sirve para virtualizar equipos de sobremesa.

VirtualBox fue desarrollado por Innotek GMI3H que fue adquirido en febrero de 2008 por Sun Microsystems Inc., que a su vez fue comprado por Oracle en junio de 2010. VirtualBox se puede ejecutar en multitud de sistemas operativos como, por ejemplo, Windows, Linux, OS X, Solaris, etc. (Nino Camazon, 2011)

Existen dos versiones de VirtualBox, una contiene el ejecutable (binario) y la otra el código fuente. La versión ejecutable, Oracle VM VirtualBox, es propietaria y gratuita para uso personal, de

evaluación y académico, estando sujeta a la licencia de uso personal y de evaluación VirtualBox (VirtualBox Personal Use and EvaluationLicense o PUEL). La otra versión es software libre (Open Source) y se llama VirtualBox OSE (Open SourceEdition, Edición de código abierto). Tiene licencia GNU General PublicLicense versión 2. La versión libre tiene algunas limitaciones.

Penny Avril, Willie Hardie (2017)

Oracle Database Release fue creado para transformar el acceso y la importancia de los datos de la empresa, el corazón de su negocio. Diseñado para la nube, Oracle Database le permite minimizar los costos de TI, aumentar la agilidad en los servicios de base de datos de aprovisionamiento, escalar y reducir elásticamente los recursos de TI según sea necesario.

2.1.8.3. Microsoft

González Gustavo (2003)

indispensable para el ámbito laboral en la actualidad y hacerse técnicos, productivos y realizar trabajos de mejor calidad por medio de la aplicación de las herramientas de ofimática puede ser usado no sólo en empresas y oficinas, sino que también resulta útil e incluso indispensable en ambientes académicos y caseros, donde puede potenciar y facilitar muchas actividades cotidianas presentación de documentos y trabajos escritos, diseño y presentación de exposiciones mediante diapositivas, administración de correo, entre otros.

III. MÉTODO

3.1. Tipo de investigación

3.1.1. Tipo

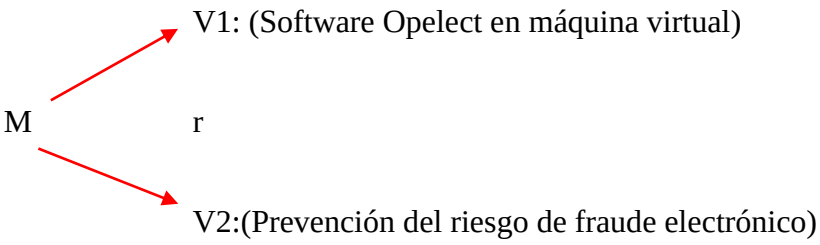
La presente investigación según (Hernández, Fernández y Baptista, 2010) son de tipo descriptivo porque busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice y correlacional porque tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en un contexto en particular. Cabe resaltar que en una misma investigación se puede incluir diferentes alcances todo dependerá de lo que se busca determinar en la investigación.

Además, cuenta con un enfoque cuantitativo según lo mencionado por (Ramírez, Ampa y Ramírez A., 2007) porque considera como objeto y campos de investigación solo los hechos o fenómenos observables, susceptibles de medición y adopta el método hipotético-deductivo cuyos procedimientos son: la observación, la formulación de hipótesis y posteriormente la contrastación o prueba de hipótesis, finalmente la correlación de variables para conseguir el rigor del método científico.

3.1.2. Nivel

De acuerdo a (Morán y Alvarado, 2010) de corte transversal porque recopilan datos en un momento único y Mayurí (2015) indico que el Diseño de investigación es No Experimental, porque no se manipula el factor causal para la determinación posterior en su relación con los efectos y sólo se describen y se analizan su incidencia e interrelación en un momento dado de las variables. Según (Hernández, Fernández y Baptista, 2010) menciona que

son investigación no experimental porque son estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural



Dònde:

m = Muestras tomadas para observaciones

V. 1 = Variable 1

V. 2= Variable 2

r = Correlación

3.2. Población y Muestra.

3.2.1. Población

La población de estudio es el total de personas que se encuentren inscritos en el sistema financiero, según el Banco Mundial 2,837,824 habitantes de lima metropolitana se encuentran inscritos en el sistema financiero e utilizan tarjeta bancaria, ya que estos participan de manera exclusiva y cotidiana en las actividades diarias, y se relacionan con las dimensiones que se pretende medir.

3.2.2. Muestra

La muestra de estudio se determinó en 384 personas que viven en Lima metropolitana y utilizan el sistema electrónico bancario de los bancos BCP,

BBVA, Interbank, Scotiabank, Banco de la Nación.

La muestra fue de tipo aleatoria-simple y su tamaño será calculado usando la siguiente fórmula de población finita con proporciones con un error estimado de 0.05 % y un acierto del 95 %:

$$n = \frac{z^2 Npq}{e^2(N-1) + z^2 pq} \dots (1)$$

n = Tamaño de muestra.
z = Desviación de la curva normal
p = Probabilidad de éxito (0.5)
q = 1 – p = 0.5
N = Población
e = 0.05 máximo error permitido

Reemplazando:

$$n = \frac{(1.96)^2(2837824)(0.5)(0.5)}{(0.1)^2(2837824-1) + (1.96)^2(0.5)(0.5)}$$

$$n = 384$$

Banco	**Número de personas**
Banco de crédito del Perú	77
Banco Continental	77
Scotiabank	77
Interbank	77
Banco de la Nación	76
Total	**384**

3.3. Operacionalización de las variables

Tabla 1.
Operacionalización de las variables

Variable	Dimensiones	Indicadores
Software Opelect en máquina virtual	Instalación del software Opelect	Seguridad en las operaciones bancarias
		Bloqueo de código informático malicioso
	Confiabilidad de los clientes	Accesibilidad
		Nivel de profesionalidad
		Rapidez de respuesta
		Documentación de apoyo
		Seguridad y fiabilidad
Prevención del riesgo de fraude electrónico	Detección de fraudes	Phishing
		Pharming
	Nivel de fraude electrónico	Número de denuncias
		Número de operaciones fraudulentas

Fuente: elaboración propia

3.4. Instrumentos

El instrumento de la recolección de datos que se usó para la presente investigación es la observación activa o directa mediante una encuesta, en donde se ha participado en el proceso investigativo desde el mismo lugar donde acontecen los hechos, ósea recoger la percepción del encuestado.

El instrumento utilizado en el trabajo de investigación es la encuesta que se realizó en forma escrita, mediante un formulario con 20 ítems de los cuales 13 ítems tienen escala de Likert y 7 ítems no tienen escala, con preguntas diseñadas de acuerdo a las

variables definidas para esta investigación; las preguntas son del tipo cerrada las cuales son contestadas por el encuestado y nos permite tener una amplia cobertura del tema de investigación y que posteriormente serán validadas.

La escala está definida de la siguiente manera:

(1) Totalmente en desacuerdo.

(2) En Desacuerdo

(3) Ni de acuerdo ni en desacuerdo

(4) De acuerdo

(5) Totalmente de acuerdo

3.5. Procedimientos

Utilizando la base de datos se aplicó el programa estadístico SSPS 21.0 y Excel 2013 donde se procedió al análisis estadístico para obtener los siguientes resultados:

- Se procedió a describir los datos de cada variable a estudiar calculando el promedio, la varianza, la desviación estándar y el error estándar.
- Luego se calculó el resultado promedio de las dimensiones según los indicadores expuestos en cada ítem.
- Para la correlación entre dos variables se utilizará la correlación r de Spearman, para determinar si existe influencia significativa de las dimensiones con las variables.
- Finalmente se interpretaron los resultados según el sigma obtenido y dichas hipótesis se complementaron con las preguntas que no trabajan con la escala Likert.

3.6. Análisis de datos

El análisis de datos se basó en función a tablas y graficas obtenidos del procesamiento de datos y los resultados son analizados y comparados con otras investigaciones.

Confiabilidad y validez

Se probó la confiabilidad del instrumento de recolección de datos mediante una prueba piloto con una muestra de 5 profesionales expertos en el tema que pasaron a evaluar 13 ítems que poseían una escala de 1-5. Esta prueba piloto arrojó un alfa de Cronbach igual a 0,850 lo cual supone una buena confiabilidad del instrumento.

Tabla 2.

Confiabilidad del instrumento

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
850	865	13

Fuente: Elaboración propia

3.7. Consideraciones éticas

Los aspectos éticos son:

(a) La tesis cumple con el esquema de la Universidad Nacional Federico Villarreal;

(b) El objetivo fundamental de la tesis es generar el nuevo conocimiento; (c) La tesis es original y auténtica por parte del investigador;

(d) Los resultados son reales no hubo manipulación de la misma;

(e) Toda la información es citada respetando la autoría.

IV. RESULTADOS

4.1. Contrastación de hipótesis

4.1.1. Hipótesis general

Ho: El software Opelect en máquina virtual no ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Ha: El software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Se utilizó la regla de decisión, comparando el valor p calculado por la data con el valor p teórico de tabla = 0,05 si el valor p calculado ≥ 0,05, se aceptará Ho, pero, si el valor p calculado < 0,05, se aceptará Ha.

Tabla 3.

Correlaciones entre el software Opelect en máquina virtual y el riesgo de fraude electrónico en operaciones bancarias

			software Opelect en máquina virtual	riesgo de fraude electrónico en operaciones bancarias
Rho de Spearman	software Opelect en máquina virtual	Coeficiente de correlación	1,000	,825**
		Sig. (bilateral)	.	,002
		N	384	384
	riesgo de fraude electrónico en operaciones bancarias	Coeficiente de correlación	,825**	1,000
		Sig. (bilateral)	,002	.
		N	384	384

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación: Según los resultados obtenidos para comprobar la hipótesis general se ha obtenido que el coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825**, se interpreta como una correlación alta y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que la hipótesis alterna se cumple entonces: El software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

4.1.2. Hipótesis especificas

Hipótesis especifica 1

Ho: El software Opelect en máquina virtual no ayudara de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Ha: El software Opelect en máquina virtual ayudara de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Se utilizó la regla de decisión, comparando el valor p calculado por la data con el valor p teórico de tabla = 0,05 si el valor p calculado ≥ 0,05, se aceptará Ho, pero, si el valor p calculado < 0,05, se aceptará Ha.

Tabla 4.

Correlaciones entre el software Opelect en máquina virtual y La detección de fraudes electrónicos en operaciones bancarias.

			software Opelect en máquina virtual	Detección de fraudes electrónicos en operaciones bancarias
Rho de Spearman	software Opelect en máquina virtual	Coeficiente de correlación	1,000	,782**
		Sig. (bilateral)	.	,003
		N	384	384
	Detección de fraudes electrónicos en operaciones bancarias	Coeficiente de correlación	,782**	1,000
		Sig. (bilateral)	,003	.
		N	384	384

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación: Según los resultados obtenidos para comprobar la hipótesis especifica 1 se ha obtenido que el coeficiente de correlación Rho de Spearman, que tiene el valor de 0,782*, se interpreta como una correlación media y el sigma (bilateral) es de 0,003 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que la hipótesis alterna se cumple entonces : El software Opelect en máquina virtual ayudara de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Hipótesis especifica 2

Ho: El software Opelect en máquina virtual no ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Ha: El software Opelect en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Se utilizó la regla de decisión, comparando el valor p calculado por la data con el valor p teórico de tabla = 0,05 si el valor p calculado ≥ 0,05, se aceptará Ho, pero si el valor p calculado < 0,05, se aceptará Ha.

Tabla 5.

Correlaciones entre el software Opelect en máquina virtual y el Nivel de fraude electrónico en operaciones bancarias

			software Opelect en máquina virtual	Nivel de fraude electrónico en operaciones bancarias
Rho de Spearman	software Opelect en máquina virtual	Coeficiente de correlación	1,000	,794**
		Sig. (bilateral)	.	,001
		N	384	384
	Nivel de fraude electrónico en operaciones bancarias	Coeficiente de correlación	,794**	1,000
		Sig. (bilateral)	,001	.
		N	384	384

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

Interpretación: Según los resultados obtenidos para comprobar la hipótesis especifica 2 se ha obtenido que el coeficiente de correlación Rho de Spearman, que tiene el valor de 0,794*, se interpreta como una correlación media y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que la hipótesis alterna se cumple entonces : El software Opelect en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

4.2. Análisis e interpretación.

A partir del análisis de los resultados obtenidos de la encuesta realizada a personas que hacen uso de las entidades financieras en Lima Metropolitano, se obtuvo lo siguiente:

Tabla 6.

En qué entidad financiera tiene cuentas bancarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BCP	72	18,8	18,8	18,8
	BBVA	69	18,0	18,0	36,7
	Interbank	73	19,0	19,0	55,7
	Scotiabank	88	22,9	22,9	78,6
	Banco de la Nación	82	21,4	21,4	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a identificar en qué entidad financiera tiene cuentas bancarias las personas encuestadas, el 22.9% lo tienen en Scotiabank, el 19.0% optaron por Interbank, el 18.0% de encuestados en BBVA, y el 21.4% poseen cuentas en el Banco de la Nación y finalmente el 18.8% decidieron abrir sus cuentas en el Banco de Crédito del Perú (BCP).

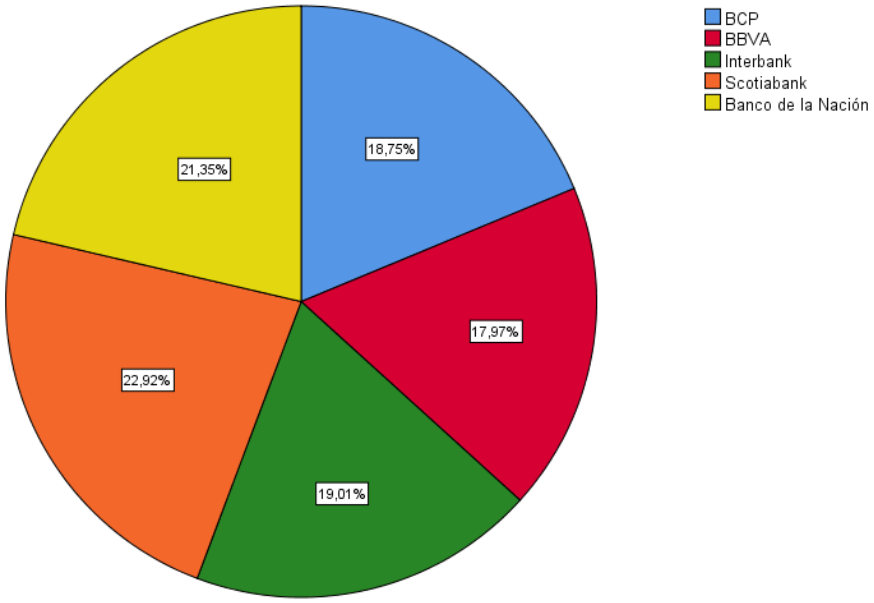


Figura 2. En qué entidad financiera tiene cuentas bancarias

Fuente: Elaboración propia

Tabla 7.

Desde donde realiza sus transacciones bancarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Domicilio	139	36,2	36,2	36,2
	Trabajo	119	31,0	31,0	67,2
	Cabinas Públicas	126	32,8	32,8	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a identificar la realización de transacciones bancarias las personas encuestadas, el 36.2% lo realizan desde su domicilio, el 31.0% desde sus trabajos y finalmente el 32.8% optan por realizar sus transacciones desde cabinas públicas.

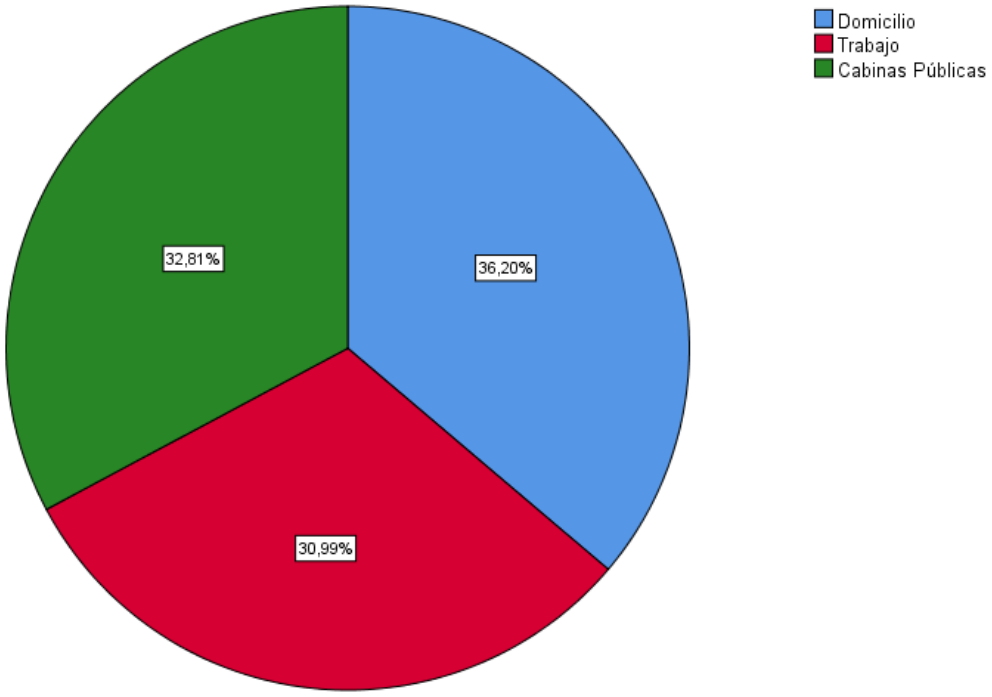


Figura 3. Desde donde realiza sus transacciones bancarias

Fuente: Elaboración propia

Tabla 8.

Con qué frecuencia realiza operaciones electrónicas bancarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Diariamente	97	25,3	25,3	25,3
	2-3 veces por semana	97	25,3	25,3	50,5
	Una vez al mes	104	27,1	27,1	77,6
	Otro	86	22,4	22,4	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a identificar la frecuencia con que se realiza operaciones electrónicas de las personas encuestadas, el 27.1% realizan sus operaciones una vez al mes, el 25.3% lo realizan de 2 a 3 veces cada semana, mientras que el 25.3% realizan operaciones electrónicas diariamente y con otras frecuencias el 22.4%.

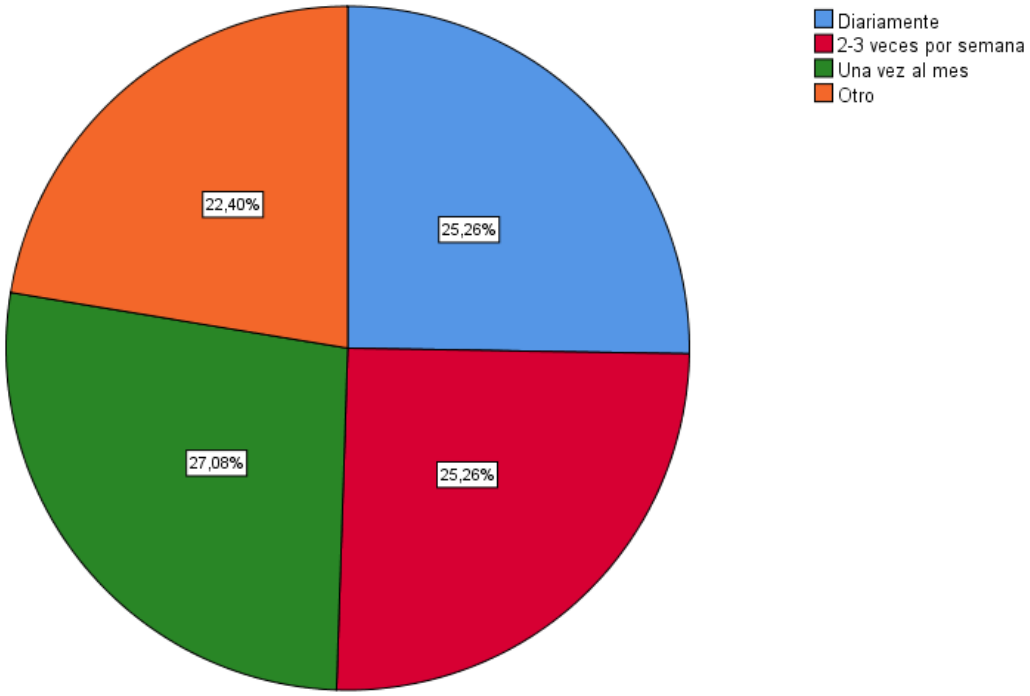


Figura 4. Con qué frecuencia realiza operaciones electrónicas bancarias

Fuente: Elaboración propia

Tabla 9.

Tiene conocimiento las medidas de seguridad en las operaciones electrónicas bancarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	191	49,7	49,7	49,7
	No	193	50,3	50,3	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto al análisis a cerca del conocimiento sobre las medidas de seguridad en las operaciones electrónicas bancarias el 49.7 % de los encuestados respondieron que, si tienen conocimiento de dichas medidas, mientras que el 50.3% de usuarios no lo tienen.

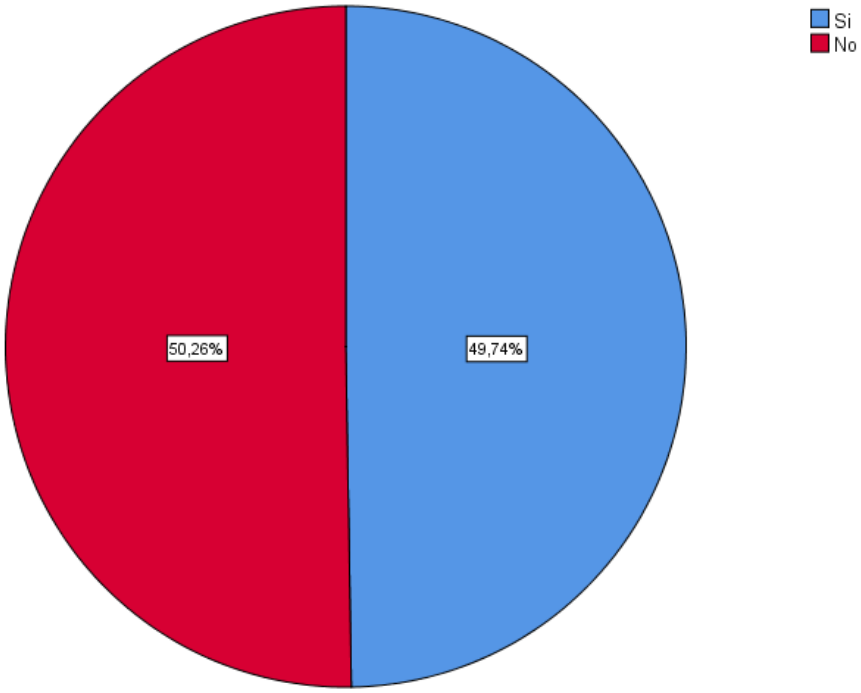


Figura 5. Tiene conocimiento las medidas de seguridad en las operaciones electrónicas bancarias

Fuente: Elaboración propia

Tabla 10.

Ha sido víctima de fraude en operaciones electrónicas bancarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	188	49,0	49,0	49,0
	No	196	51,0	51,0	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a identificar si los clientes han sido víctima de fraude en operaciones electrónicas bancarias el 49.0% de los encuestados respondieron que, si han sufrido de algún tipo de fraude, mientras que el 51.0% aseguran que no fueron víctimas de fraudes electrónicos.

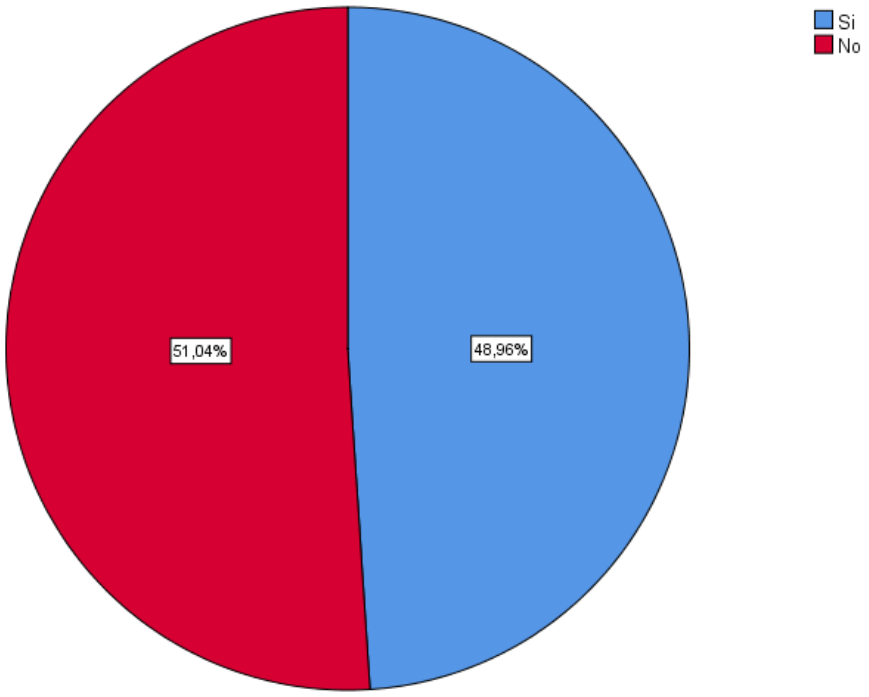


Figura 6. Ha sido víctima de fraude en operaciones electrónicas bancarias

Fuente: Elaboración propia

Tabla 11.

Conoce usted la modalidad fraudulenta empleada

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Pishing	190	49,5	49,5	49,5
	Pharming	194	50,5	50,5	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a si las personas encuestadas conocen la modalidad fraudulenta empleadas se obtuvo que el 49.5% de los usuarios encuestados respondieron que conocen la modalidad Phishing, mientras que el 50.5% conoce la modalidad Pharming.

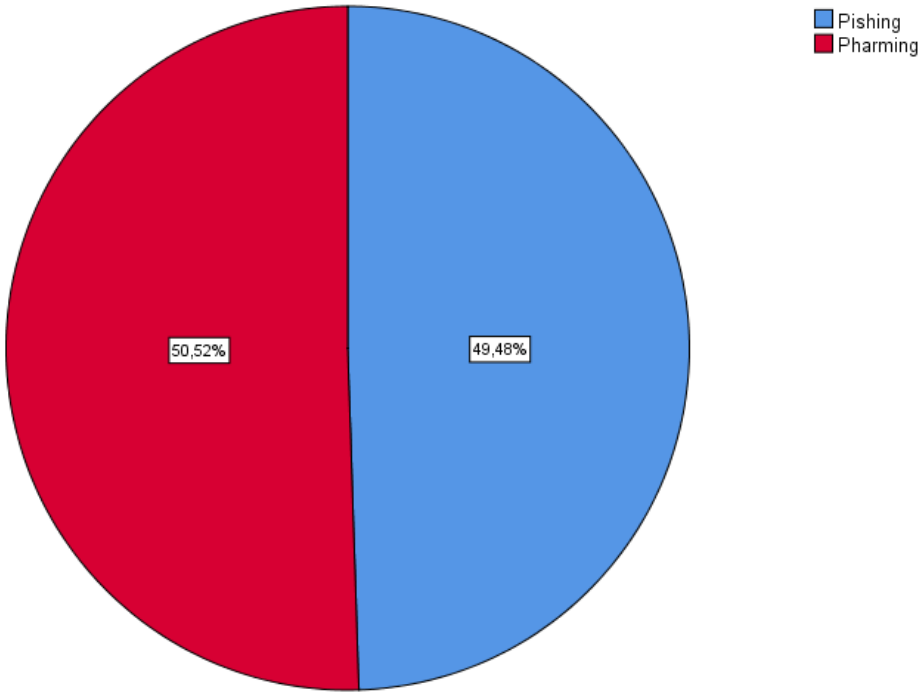


Figura 7. Conoce usted la modalidad fraudulenta empleada

Fuente: Elaboración propia

Tabla 12.

Utilizaría un software Opelect para reducir el peligro de fraude electrónico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	203	52,9	52,9	52,9
	No	181	47,1	47,1	100,0
	Total	384	100,0	100,0	

Fuente: Elaboración propia

Respecto a si los clientes estarían dispuestos a utilizar un software Opelect para reducir el peligro de fraude electrónico, el 52.9% de los encuestados respondieron que, si optarían por usar este software, mientras que el 47.1% de usuarios no lo estarían.

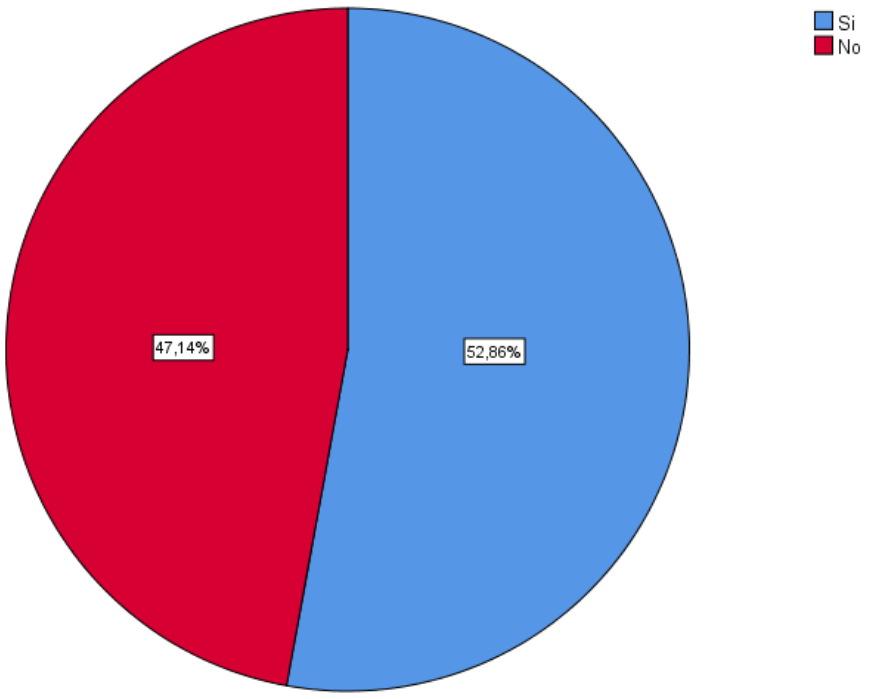


Figura 8. Utilizaría un software Opelect para reducir el peligro de fraude electrónico

Fuente: Elaboración propia

V. DISCUSIÓN DE RESULTADOS

García y Enero (2018) sostuvo que el sistema de información que propone implementar, permitirá generar mayor confianza en la entidad financiera, confianza en el cliente al realizar sus operaciones y un respaldo de seguridad para los colaboradores en las transacciones realizadas, así como también implementar mecanismos de innovación y procesos de mejora continua para prevenir y controlar el fraude financiero. Concluyendo que se obtuvo que el sistema de información que se implementó ayudo a mitigar el fraude en la red de tiendas de la entidad bancaria, a su vez, el modelo sistema de información propuesto es viable, factible y deseable para su implementación. De acuerdo con la presente investigación se obtuvo que el coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825, se interpreta como una correlación alta y la sigma (bilateral) es de ,0002 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudará de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Martínez (2017) Los fraudes en el E-commerce suceden por una baja o nula inversión en sistemas de seguridad que protejan al servidor web de la entidad comercial frente a los ataques cibernéticos y más aún, con el desconocimiento de las medidas pertinentes de seguridad virtual, muchas empresas que tomarían la decisión de ampliar sus canales de atención a la Internet serían considerablemente perjudicados económicamente por fraudes. De acuerdo con esto en la presente investigación se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,794*, se interpreta como una correlación media y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect

en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Balcazar (2017) sostuvo que los principales mecanismos de seguridad en las tarjetas de crédito y tarjetas de débito son las claves secretas; con la que se obtiene total acceso, permitiendo el uso de las mismas; en esta línea, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, al requerir la información de todos los documentos de las transacciones realizadas por el supuesto "titular"; la entidad bancaria o financiera, entrega los reportes Tándem y Journals correspondientes a las operaciones generadas; sin embargo, esta información solo indicará que las operaciones se realizaron de manera habitual porque se digitó la clave secreta correctamente; la misma que, ya no es suficiente para verificar si se trata de operación veraz o de una operación no reconocida. De acuerdo con esto en la presente investigación se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,782*, se interpreta como una correlación media y el sigma (bilateral) es de 0,003 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudará de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Bravo y Pico (2016) establecieron como objetivo determinar la importancia de los diferentes manuales de aplicación a ser estudiados cumplan con las normas internacionales de información financiera además de los procedimientos establecidos para las empresas de servicios en el área contable, bajo el análisis de que el desarrollo económico que tenga una empresa no solo depende de un buen manejo administrativo, sino también de las estrategias para aplicar estos procedimientos que ayuden al desarrollo de cada una de las actividades se afirma que cada empresa debe contar con

métodos, procedimientos y programas de revisión constante, estableciendo procesos y controles que ayuden al usuario a lograr un mejor desenvolvimiento y manejo de sus tareas logrando así un trabajo eficiente y disminuyendo la ocurrencia de errores que pueden volver vulnerable el área contable de la empresa; con lo cual se pudo concluir que la mayoría de empresas de servicios en Guayaquil no cuenta con un manual de procedimientos antifraudes, sin embargo con la ayuda de los mecanismos y procedimientos diseñados, será posible minimizar el impacto de los riesgos errores y fraudes en la información presentada en los estados financieros. De esta manera los resultados son similares en la presente investigación, ya que gracias a la prueba de correlación Rho de Spearman, que tiene el valor de 0,825 y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05 permitiendo afirmar que el software Opelect en máquina virtual ayudará de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Ñaupas (2016) en su investigación se planteó implementar un modelo basado en técnicas de Minería de Datos con el fin de clasificar las transacciones realizadas en los canales de banca por internet o banca móvil como fraudulentas o integras, por medio de la aplicación de un proceso de descubrimiento de conocimientos en bases de datos, esto con la ayuda de la aplicación de algoritmos arboles de clasificación. Una vez realizado el análisis se confirmó que el desarrollo de las nuevas tecnologías permite a las entidades financieras un crecimiento a la par con ellas de manera que ofrezcan a sus clientes diversos medios y aplicaciones que les faciliten realizar sus transacciones financieras, sin embargo esto es atractivo no solo para los clientes sino también para los defraudadores pues hace que cada vez existan más maneras de cometer fraudes, lo que permitió que se concluya en que las técnicas predictivas resultan eficientes para descubrir conocimientos y permiten inferir como una variable o atributo puede incidir

en otros. Con este resultado se puede afirmar el resultado de la presente investigación gracias a la prueba de correlación Rho de Spearman, que tiene el valor de 0,782 y el sigma (bilateral) es de 0,003 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudará de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Paredes (2014) planteo como objetivo principal dar a conocer y describir la problemática que se presenta día a día, del fraude en cajeros automáticos en el sistema financiero colombiano, mediante clonación de tarjetas de débitos y crédito mediante los delitos de clonación de tarjeta. Para lo cual realizo un análisis de los mal llamados delitos financieros, seguido de ello se identificaron las principales recomendaciones de seguridad tanto en el momento de recibir la tarjeta en físico, como en el que es utilizado en los cajeros automáticos de sitios de mayor preferencia del actuar delincuencial, después de los propios cajeros automáticos. Se pudo llegar al final que a lo largo de la historia y desde el invento de los cajeros automáticos, se ha visto cómo estos han evolucionado en seguridad, en seguridad integral, tanto en elementos físicos como tecnológicos y de software, siempre tratando de brindar y ofrecer tranquilidad a los clientes, quienes al final de la cadena son los directos consumidores de este tipo de servicio. De acuerdo con esto en la presente investigación se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,794 media y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Rodríguez (2013) delimito como objetivo principal elaborar una guía general de la aplicación de las medidas mínimas de seguridad exigidas a entidades bancarias y de transportes de valores del Ecuador, en la que se deban considerar la legislación vigente sobre seguridad bancaria y transporte de valores a disposición de los consultores para medidas de prevención y protección optimas en las actividades del transporte de valores y seguridad bancaria. Mediante un Plan de Seguridad de Transporte de Valores que involucra manuales de procedimientos y matrices de supervisión, con la que finalmente se pudo concluir que se obtuvo que la normativa legal exige a todas las entidades que conforman el sistema financiero las mismas medidas mínimas de seguridad sin hacer distinción alguna entre los distintos tipos de instituciones que conforman el sistema financiero. Así mismo se sabe que Ninguna institución financiera transporta sus valores por sus propios medios, estos utilizan el servicio de transporte de valores ofrecido por las empresas de seguridad que brindan este servicio. De acuerdo con esto en la presente investigación se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825 y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Núñez (2013) estableció como objetivo de su investigación conocer cuáles son actualmente las principales modalidades delictivas que afectan al sistema financiero y a sus clientes, así presentar un plan de mitigación de riesgos las cuales ayuden a disminuir los riesgos que posee el sistema financiero. Debido a que en Ecuador los clientes conocen muy poco sobre los métodos de fraudes que existen en la actualidad y como evitarlos, muchos de los tipos de fraudes han crecido cada año debido a que el país posee una moneda muy valorada en el mundo como lo es el Dólar Americano, así los hackers

y/o delincuentes con sus bandas organizadas se han ubicado en nuestro país. De esta manera se pudo concluir que los fraudes en los cajeros automáticos ha sido creciendo en los últimos años de forma significativa, esto debido a la gran vulnerabilidad en las claves de las tarjetas de los clientes, pero son varios los tipos de fraudes que afectan al sistema financiero cada año, con esta afirmación se puede contrastar los resultados de la presente investigación donde, gracias a la prueba de correlación Rho de Spearman, que tiene el valor de 0,794 y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudara de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Rojas (2013) estableció como objetivo principal establecer si existe una debida protección del derecho a la idoneidad del servicio financiero y un tercero acceder a la banca electrónica y ocasionar un daño al consumidor financiero establecido en INDECOPI, esto debido a que el avance de la banca electrónica está progresando hoy en día dado que la penetración de Internet es un hecho ineludible pero la tecnología así como otorga las ventajas también tiene que hacer frente a una serie de riesgo, principalmente en las transferencias electrónicas bancarias. Como conclusión se obtuvo que efectivamente no existe una debida protección del derecho a la Identificación del servicio financiero en INDECOPI si un tercero (hacker) accede a la Banca Electrónica y ocasiona un daño al consumidor financiero. Con este resultado se puede contrastar los resultados de la presente investigación donde, gracias a la prueba de correlación Rho de Spearman, que tiene el valor de 0,825 y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Aravena y Cifuentes (2013) se planteó como objetivo principal buscar comparar las Políticas y Normas seguidas por Banco Santander y Retail Falabella para el Análisis de Riesgo Financiero de su cartera de crédito. Por medio de la filosofía de gestión de riesgos se buscó en todo momento la creación de valor para el accionista a través de la utilización eficiente del capital asignado a las unidades de negocio. Además se identificó que uno de los pilares fundamentales de la gestión de los riesgos estructurales es la correcta atribución y segregación de funciones que permitan garantizar un marco de responsabilidades y de comunicación apropiados, para el cual finalmente se obtuvo que ambas compañías cuentas con mediciones de los diferentes riesgos financieros por medio de la provisión, las cuales se da mucha importancia a las colocaciones en el mercados y además un control exhaustivo a las cuentas que ingresan a morosidad en los diferentes tramos de vencimiento, a la vez aplicando las mejores herramientas de recuperaciones mes a mes. De acuerdo con esto en la presente investigación se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825 y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05 lo que nos permite afirmar que el software Opelect en máquina virtual ayudara de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

VI. CONCLUSIONES

1. El software Opelect en máquina virtual ayudará de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana, esto debido a que se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,825**, se interpreta como una correlación alta y el sigma (bilateral) es de ,002 el mismo que es menor al parámetro teórico de 0,05.
2. El software Opelect en máquina virtual ayudará de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana, esto debido a que se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,782*, se interpreta como una correlación media y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05.
3. El software Opelect en máquina virtual ayudará de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana, esto debido a que se obtuvo un coeficiente de correlación Rho de Spearman, que tiene el valor de 0,794*, se interpreta como una correlación media y el sigma (bilateral) es de 0,001 el mismo que es menor al parámetro teórico de 0,05.

VII. RECOMENDACIONES

1. Esta recomendación discierne de la conclusión 1: Se recomienda implementar el software Opelect en máquina virtual en los principales bancos que estuvieron bajo estudio en la presente investigación y así poder ayudar a disminuir los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana, ya que como se analizó estos bancos se encuentran expuestos a peligros inherentes que cada vez son más y con mejor usa de la tecnología.
2. Esta recomendación discierne de la conclusión 2: Implementar el software Opelect en máquina virtual con el fin de detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana, y de esta manera reducir los problemas que puedan afectar no solo a nuestros usuarios, sino perdiéndolos como clientes de manera que se rompa la confianza que depositan en nosotros, al momento de elegirnos sobre las demás entidades bancarias.
3. Esta recomendación discierne de la conclusión 3: Concientizar a las entidades en que la implementación del software Opelect en máquina virtual ayudará de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana, con la que se pueda perjudicar su prestigio como institución y resaltar por encima de la competencia.

VIII. REFERENCIAS

Aravena, M, y Cifuentes, M. (2013). *Políticas De Riesgo Financiero Banco Santander Y Retail Falabella* (Tesis de Grado) Universidad Del Bio – Bio. Chillan, Chile.

Balcázar, W. (2017). *Medidas de seguridad que deberían incorporarse a fin de evitar operaciones no reconocidas en tarjetas de crédito y débito* (Tesis de Grado). Universidad Privada Antenor Orrego. Trujillo, Perú.

Banco de laNación (2017). *Multired Virtual*. Obtenido de bn.com.pe: http://www.bn.com.pe/clientes/banca-internet/multired-virtual.asp

BBVA (2017). *Clave SMS*. Obtenido de bbvacontinental.pe: https://www.bbvacontinental.pe/meta/seguridad/

BBVA Continental. (2017). *Banca por Internet*. Obtenido de bbvacontinental.pe: https://www.bbvacontinental.pe/personas/canales/banca-por-internet/#ficha-content-0

BCP (2017). *Banca por Internet*. Obtenido de viabcp.com: https://www.viabcp.com/wps/portal/viabcpp/personas/bcp-sin-bcp/banca-por-internet

Bravo, R. y Pico, S. (2016). *Evaluación de manuales de procedimientos para prevenir riesgos, errores y fraudes contables* (Tesis de Grado). Universidad De Guayaquil. Guayaquil, Ecuador.

Camazon, J. (2011). *Sistemas operativos monopuesto.* Madrid: EDITEX.

Elías, J., Hernández, J. y Sánchez, A. (2016). *Desarrollo de un Kit de Seguridad Informática Enfocada para la Protección de la Información Computacional tanto en Hardware*

como en Software para la Universidad Tecnológica de el Salvador (Tesis de Grado). Universidad Tecnológica de El Salvador. San Salvador, El Salvador.

García, E. y Enero, R. (2018). *Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú* (Tesis de Grado). Universidad Tecnológica Del Perú. Lima, Perú.

Hernández, R., Fernández, C. y Baptista P. (2010). *Metodología de la investigación.* México: Editorial Mc. Graw Hill.

Interbank(2017). *Banca por Internet para Empresas*. Obtenido de interbank.com.pe:https://www.interbank.com.pe/banca-internet-empresas

Ley30171 (2014). Delitos Informaticos. *Ley De Delitos Informaticos*. Lima, Lima, Lima: Diarios el Peruano.

Martínez, L. (2017). *Medidas De Seguridad Que Evitan Fraudes*. Lima, Perú: Repositorio Universidad SISE.

Mayurí, J. (2015). El marketing y la ventaja competitividad en los alumnos de FCA-UNMSM, comparada con los alumnos de administración de la Universidad de los Estudios de Bérgamo. *Rev de Investigación de la Fac. De Ciencias Administrativas, 18*, (36): 31-38.

McAfee. (2017). *Security Advice Center*. Obtenido de home.mcafee.com: https://home.mcafee.com/advicecenter/?id=ad_phishing_optpopnp&ctst=1

Merizalde, C. y Zapata, J. (2014). Control interno y métodos utilizados por la auditoría forense para la prevención y detección de fraudes en las estaciones de servicio ubicadas en el distrito metropolitano de quito.

Morán G. y Alvarado, D. (2010). *Métodos de investigación*. México: Primera edición. Pearson educación.

Núñez, R. (2013). *Fraude al sistema financiero y a sus clientes* (Tesis de Grado) Universidad San Francisco De Quito. Quito, Ecuador.

Ñaupas, C. (2016). Minería de datos aplicada a la detección de fraude electrónico en entidades bancarias" (Tesis de Grado). Universidad Nacional Mayor De San Marcos, Lima, Perú.

Paredes, C. (2014). El fraude en cajeros automáticos mediante clonación de tarjetas débito y crédito. Universidad Militar Nueva Granada. Bogotá, Colombia.

Ramírez, A., Ampa, I. y Ramírez, K. (2007). Tecnología *de la investigación.* Primera edición. Editorial Moshera SRL.

Rodríguez, A. (2013). *Guía general de aplicación de las medidas mínimas de seguridad exigidas a las entidades financieras y de transporte de valores en el Ecuador* (Tesis de Grado). Escuela Politécnica Del Ejército, Sangolqui, Ecuador.

Rojas, M. (2013). *La Seguridad De La Banca Electrónica Y La Defensa Efectiva Del Consumidor Financiero En La Legislación Peruana Y Colombiana* (Tesis de Grado). Universidad Cesar Vallejo, Lima, Perú.

SCOTIABANK. (2017). *Scotia en Línea*. Obtenido de scotiabank.com.pe: http://www.scotiabank.com.pe/Acerca-de/servicios-bancarios/scotia-en-linea

Urbina, V (2005). *Auditoria de Fraudes en el Sector Financiero Privado* (Tesis de post Grado). Escuela Superior Politécnica del Litoral. Guayaquil, Ecuador.

Penny Avril, Willie Hardie (2017) Transforming Data Management, Edition 2013 (Vol.I). New York. USA.

García, E. & Enero, R. (2018). *Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú*. (Tesis de Grado). Universidad Tecnológica del Perú, Lima, Perú.

Valle, J. (2013) *El Delito Informático de Phishing (*Tesis de Grado*).* Universidad Regional Autónoma de los Andes. Quevedo. Ecuador.

Leguizamón, M. (s/n). *El Phishing*, (Tesis de Grado). Universitat Jaume, Valencia, España.

Núñez, R. (2013) *Fraude Al Sistema Financiero Y A Sus Clientes* (Tesis de Grado) Universidad San Francisco de Quito. Quito, Ecuador.

Viejo, F. (2015) *Análisis de la banca por Internet entre los usuarios particulares. Un modelo en Dinámica de Sistemas* (Tesis de Maestría). Universidad de Valladolid, Valladolid, España.

Merizalde, C. & Zapata, J. (2014) *Control Interno y métodos Utilizados por la Auditoria Forense para la Prevención y Detección de Fraudes en las Estaciones de Servicio Ubicadas en el distrito Metropolitano de Quito periodo 2012-2013.* (Tesis de grado). Universidad Politécnica salesiana, Quito, Ecuador.

Gonzales, D. & Peña, J. (2012) *Estudio del Impacto de la Ingeniería Social-Phishing* (Tesis de Grado) Universidad Nacional Autónoma de México, Ciudad de México, México.

Borghello, C. (2006) *Keyloggers,* obtenido de https://www.seguinfo.com.ar/articulos/46-keylogger.htm

Pressman, R. (2010) *Ingeniería del Software,* Ciudad de México, México, McGRAW-HILL Interamericana Editores, S.A.

Vilca, A. (2016) *Implementación De Servidores Virtuales En La Corte Superior De Justicia De Puno Sub Sede San Román Utilizando La Herramienta Vmware* (Tesis de Grado) Universidad Andina Néstor Cáceres Velásquez, Juliaca, Perú.

Gonzales, G. (2003) entrevista Internet, http://umeet.uninet.edu/umeet2003/spanish/talks/20031216.2.es.html,extraido el 8 de febrero 2012.

IX. ANEXOS

Anexo 1: Matriz de Consistencia

<table>
<tr>
<th>Problema</th>
<th>objetivo</th>
<th>hipótesis</th>
<th>Variables</th>
<th>Metodología</th>
</tr>
<tr>
<td>

Problema general

¿El software Opelect en máquina virtual ayudará a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana?

Problemas específicos

¿El software Opelect en máquina virtual ayudará a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana?

¿El software Opelect en máquina virtual ayudará a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana?

</td>
<td>

Objetivo general

Determinar si el software Opelect en máquina virtual ayudará a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana

Objetivos específicos

Determinar si el software Opelect en máquina virtual ayudará a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

Determinar si el software Opelect en máquina virtual ayudará a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

</td>
<td>

Hipótesis general

El software Opelect en máquina virtual ayudará de manera significativa a prevenir el riesgo de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

Hipótesis específicas

El software Opelect en máquina virtual ayudará de manera significativa a detectar los fraudes electrónicos en operaciones bancarias de los clientes de Lima Metropolitana.

El software Opelect en máquina virtual ayudará de manera significativa a reducir el nivel de fraude electrónico en operaciones bancarias de los clientes de Lima Metropolitana.

</td>
<td>

Variable independiente: Software Opelect en máquina virtual

Dimensiones	Indicadores
Instalación del software Opelect	Seguridad en las operaciones bancarias
	Bloqueo de código informático malicioso
Confiabilidad de los clientes	Accesibilidad
	Nivel de profesionalidad
	Rapidez de respuesta
	Documentación de apoyo
	Seguridad y fiabilidad

Variable dependiente: Prevención del riesgo de fraude electrónico

Dimensiones	Indicadores
Detección de fraudes	Phishing
	Pharming
Nivel de fraude electrónico	Número de denuncias
	Número de operaciones fraudulentas

</td>
<td>

Tipo de Investigación:
Descriptivo correlacional

Nivel de Investigación:
Correlacional - transversal

Métodos:
Deductivo - cuantitativo

Diseño de investigación:
No experimental

Población:
12 400 000 personas que viven en Lima Metropolitana.

Muestra:
246 personas que viven en Lima metropolitana y utilizan el sistema electrónico bancario de los bancos en estudio.

</td>
</tr>
</table>

Anexo 2: Instrumento de Recolección de Datos

Instrucciones:

Las siguientes preguntas tienen que ver con varios aspectos de su trabajo. Señale con una X dentro del recuadro correspondiente a la pregunta, de acuerdo al cuadro de codificación. Por favor, conteste con su opinión sincera, es su opinión la que cuenta y por favor asegúrese de que no deja ninguna pregunta en blanco.

Puesto que desempeña:……Sexo:…….Edad:……

Codificación				
1	2	3	4	5
nunca	casi nunca	a veces	casi siempre	siempre

		1	2	3	4	5
01	Utiliza usted la banca electrónica de su banco.					
02	Realiza pagos de servicios públicos por medio de la banca por internet.					
03	Realiza transferencias bancarias del mismo banco por medio de la banca por internet.					
04	Realiza transferencias bancarias entre cuentas de diferentes bancos por medio de la banca por internet.					
05	Tiene un cuidado cuando realiza transacciones por internet					
06	Se asegura de que el equipo que utiliza para hacer uso de la banca en línea cuente con dispositivos de seguridad.					
07	Utiliza usted la opcion de recordar contraseña en sus visitas a sitios web.					

08	Ha recibido de su banco algun tipo de capacitación para utilizar el servicio electrónico de manera segura.					
09	Revisa en la página internet de su banco si utiliza alguna consejo o demostración para el uso de forma segura de la banca electrónica.					
10	Utiliza los dispositivos de seguridad que le brinda su banco					
11	Sobre la seguridad en las operaciones bancarias considera que reducen los fraudes bancarios.					
12	La razón por la que no cambia de banco es la seguridad que le brindan para sus cuentas.					
13	Ha sido víctima de algún fraude bancario.					

Marque con una (x) la alternativa que considera la más adecuada para cada pregunta.

14	En qué entidad financiera tiene cuentas bancarias	
	a	BCP
	b	BBVA
	c	Interbank
	d	Scotiabank
	e	Banco de la Nación
15	Desde donde realiza sus transacciones bancarias	
	a	Domicilio
	b	Trabajo
	c	Cabinas públicas
16	Con que frecuencia realiza operaciones electrónicas bancarias	
	a	Diariamente
	b	2-3 veces por semana
	c	Una vez al mes

	d	Otro
17	Tiene conocimiento las medidas de seguridad en las operaciones electrónicas bancarias.	
	a	Si
	b	No
18	Ha sido víctima de fraude en operaciones electrónicas bancarias.	
	a	Si
	b	No
19	Conoce usted la modalidad fraudulenta empleada.	
	a	Phishing
	b	Pharming
20	Utilizaría un software Opelect para reducir el peligro de fraude electrónico.	
	a	Si
	b	No