FACULTAD DE DERECHO Y CIENCIA POLÍTICA

IMPACTO DEL FRAUDE INFORMÁTICO EN EL E-COMMERCE DE LIMA

Línea de investigación:

Procesos jurídicos y resolución de conflictos

Tesis para optar el Título Profesional de Abogado

Autora

Allazo Toribio, Angela Stefanny

Asesor

Navas Rondon, Carlos Vicente

Codigo ORCID 0000-0001-7110-418X

Jurado:

Vigil Farias, Jose

Moscoso Torres, Victor Juber

Alfaro Pamo, Karina Tatiana

Lima - Perú

2024

TESIS ALLAZO TORIBIO.docx

INFORME DE ORIGINALIDAD

27%	24%	5%	17%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	5%
2	hdl.handle.net Fuente de Internet	3%
3	repositorio.unfv.edu.pe Fuente de Internet	1%
4	dspace.unl.edu.ec Fuente de Internet	1%
5	repositorio.ucv.edu.pe Fuente de Internet	1%
6	repositorio.uwiener.edu.pe Fuente de Internet	1%
7	cdn.www.gob.pe Fuente de Internet	1%
8	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

IMPACTO DEL FRAUDE INFORMÁTICO EN EL E-COMMERCE DE LIMA

Línea de Investigación:
Procesos jurídicos y resolución de conflictos
Tesis para optar el Título Profesional de Abogado

Autora:
Allazo Toribio, Angela Stefanny

Asesor:
Navas Rondon, Carlos Vicente
(ORCID: 0000-0001-7110-418X)

Jurado:
Vigil Farias, Jose
Moscoso Torres, Victor Juber
Alfaro Pamo, Karina Tatiana

Lima – Perú
2024

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo general del presente trabajo fue determinar el impacto del fraude informático en el e-commerce de Lima, 2023. El método de esta investigación cuantitativa fue de naturaleza básica y utilizó un enfoque no experimental con alcance correlacional. Los 23 miembros de la Fiscalía Corporativa Especializada en Delitos Cibernéticos de Lima que se desempeñan como auxiliares de la función tributaria y fiscales constituyeron tanto la población como la muestra. Según los resultados el coeficiente de correlación de 0,6 derivado de la prueba de hipótesis Rho de Spearman señala una conexión moderadamente favorable entre las variables de investigación. También hubo un umbral de significancia de 0,002, no alcanza el límite de 0,05. Esto llevó al rechazo de la hipótesis nula y a la confirmación de la alternativa. Se concluyó que el fraude informático influye sustancialmente en el comercio en línea en Lima en el año 2023.

Palabras clave: Fraude Informático, e- commerce, Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima.

ABSTRACT

The overall objective of this study was to determine the impact of computer fraud on e-commerce in Lima, 2023. The method of this quantitative research was basic in nature and used a non-experimental approach with correlational scope. The 23 members of the Specialized Corporate Prosecutor's Office for Cybercrime in Lima who serve as tax function assistants and prosecutors constituted both the population and the sample. According to the results the correlation coefficient of 0.6 derived from Spearman's Rho hypothesis test points to a moderately favorable connection between the research variables. There was also a significance threshold of 0.002, not reaching the 0.05 limit. This led to the rejection of the null hypothesis and confirmation of the alternative. It was concluded that computer fraud substantially influences online commerce in Lima in the year 2023.

Keywords: Computer Fraud, e-commerce, Corporate Prosecutor's Office Specialized in Cybercrime of Lima.

I. INTRODUCCIÓN

1.1. Descripción y formulación del Problema

Las tecnologías de la información y las comunicaciones han facilitado el progreso en varias industrias, agilizando las tareas cotidianas, particularmente en el comercio. El comercio electrónico, a menudo conocido como E-commerce, surgió como un método conveniente para que las empresas, los comercios y los consumidores compren y vendan cosas a través de plataformas tecnológicas. Sin embargo, así como la virtualidad puede resultar beneficiosa para las actividades comerciales, también lo es para cometer delitos, surgiendo de esta manera el cibercrimen o también llamada “ciberdelincuencia” o “ciberdelitos”, el fraude informático, que utiliza tecnología como computadoras y teléfonos móviles, a menudo se considera el tipo de delito cibernético más importante en la sociedad contemporánea.

Según Perez (2019) la explotación de las tecnologías de la información o las comunicaciones para lograr un beneficio ilícito a costa de otra parte es lo que constituye fraude informático. Vinelli (2021) destaca que para perpetrar un fraude informático es necesario utilizar un sistema informático a fin de lograr una ventaja económica. Mayer y Oliver (2020) definen el fraude informático como un fenómeno caracterizado por tres componentes esenciales: comprobar la manipulación de datos o programas de sistemas de tratamiento automatizado de la información, ocasionar un perjucio patrimonial y la presencia de un motivo financiero que impulsa la actividad fraudulenta culpable. Además de este estudio, Zevallos (2020) amplía aún más el alcance al clasificar otras formas de ciberdelitos que están muy extendidas en el ámbito digital. Estos incluyen varios tipos de riesgos cibernéticos, incluido el phishing, las transferencias bancarias fraudulentas, el smishing, el vishing, el ransomware y transacciones fraudulentas en línea realizadas con tarjetas de crédito o débito.

Por otro lado, existe el "E-commerce" o "Comercio Electrónico", el cual es un método para realizar operaciones comerciales que incluyen la compra así como venta de productos y

servicios mediante Internet. Debido a este sistema, es que una persona natural o jurídica, puede adquirir un producto que se encuentre a mucha distancia, o se contrate un servicio ubicado en otro país. Higuerey (2019) destaca el hecho de que la característica fundamental de este tipo de actividad económica es que permite que el comercio se realice mediante plataformas digitales como redes sociales, web site, aplicaciones para teléfonos inteligentes, etc. El comercio electrónico, tal como lo definen Hartley & Rudelius (2018), abarca actividades que incluyen los procesos de almacenamiento, marketing y pago facilitados a través de la comunicación electrónica.

A nivel global, el comercio electrónico ha mostrado un crecimiento significativo, particularmente estimulado por la pandemia de COVID-19. Según informes de la UNCTAD (2021), Corea del Sur registró el mayor aumento en e-commerce durante el año 2020, alcanzando un 25.9%. Este crecimiento fue seguido de cerca por China, con un 24.9%, y el Reino Unido, con un 23.3%. Estos datos resaltan cómo el comercio electrónico se ha transformado en una parte crucial de la economía en las naciones más avanzadas del mundo, adaptándose rápidamente a las nuevas condiciones de mercado impuestas por la pandemia.

A continuación, se muestra el crecimiento del e-commerce en las principales economías del mundo:

Tabla 1

Ventas minoristas en línea (e-commerce), economías seleccionadas, 2018-2020

Economía	Ventas minoristas en línea ($ mil millones)			Ventas minoristas ($ mil millones)			% en línea de las ventas minoristas		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Australia	13,5	14,4	22,9	239	229	242	5,6	6,3	9,4
Canadá	13,9	16,5	28,1	467	462	452	3,0	3,6	6,2
China	1.060,4	1.233,6	1.414,3	5.755	5.957	5.681	18,4	20,7	24,9
Corea (Rep.)	76,8	84,3	104,4	423	406	403	18,2	20,8	25,9
Singapur	1,6	1,9	3,2	34	32	27	4,7	5,9	11,7
Reino Unido	84,0	89,0	130,6	565	564	560	14,9	15,8	23,3
EE. UU.	519,6	598,0	791,7	5.269	5.452	5.638	9,9	11,0	14,0
Economías en la lista	1.770	2.038	2.495	12.752	13.102	13.003	14	16	19

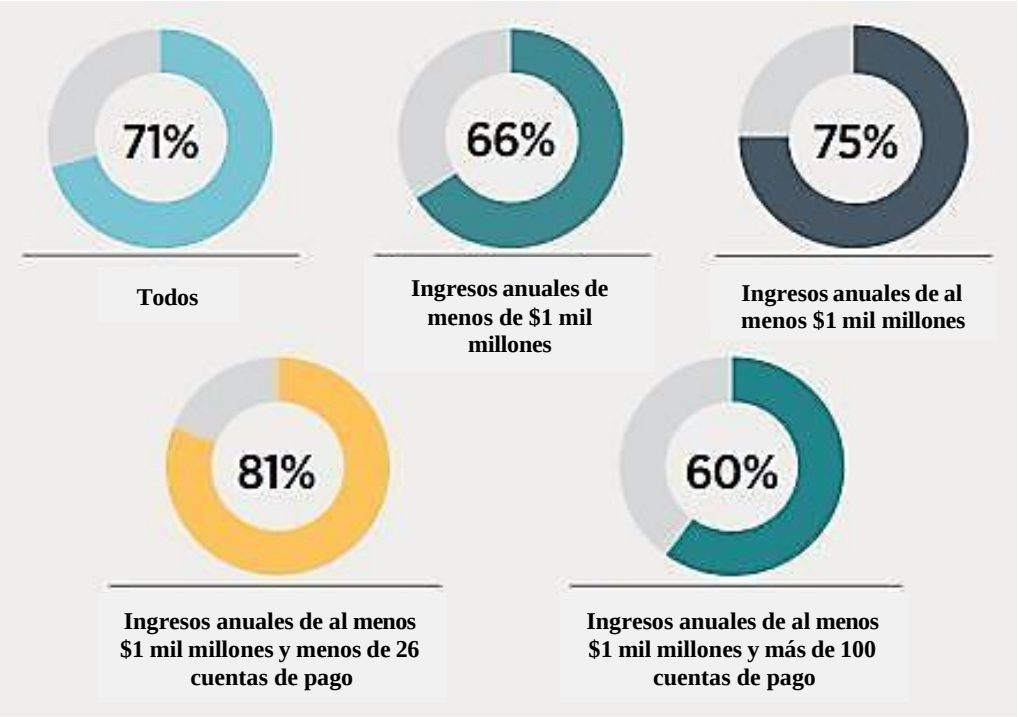
Fuente: Tomado de UNCTAD, a partir de las oficinas nacionales de estadística. Recuperado de https://unctad.org/es/news/el-comercio-electronico-mundial-alcanza-los-267-billones-de-dolares-mientras-covid-19-impulsa

Si bien las compras por Internet han contribuido a la reactivación de las economías nacionales, también han planteado varias preocupaciones sobre la ciberseguridad que persistirán mucho después de que las cosas se calmen. Los procesadores de pagos en línea son vulnerables al fraude. Por ejemplo, según la Encuesta de Control y Fraude de Pagos de Association for Financial Professionals (2022) descubrió que en 2021, un asombroso 71% de las empresas de todo el mundo fueron víctimas de fraude de pagos. Asimismo, de acuerdo con

Deyan (2022), las predicciones indican que para 2023, el fraude con tarjeta no presente (CNP) habrá aumentado un 14%.

Figura 1

Porcentaje de organizaciones que experimentaron intentos y/o Fraude de pagos reales en 2021



Nota: Tomado de Association for Financial Professionals, a partir de la dirección de investigación de encuestas. Recuperado de: *https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud*

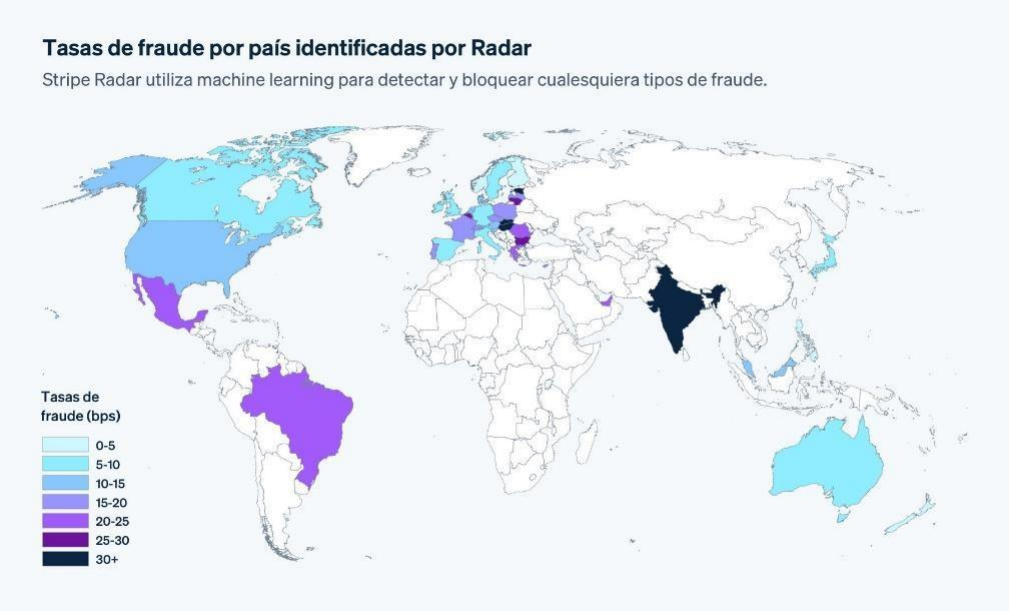
Asimismo, según un nuevo informe de Stripe (2022),se muestra que el fraude varía mucho tanto en número como en habilidad entre los mercados. En comparación con Alemania, la tasa de fraude de Francia es aproximadamente el doble que la del área de Asia y el Pacífico, mientras que la tasa de Singapur es la mitad que la de la región.

A nivel Latinoamericano, Stripe (2022) afirma que la tasa de fraude empresarial de la región es del 97%, superando por un margen sustancial los niveles de América del Norte y Asia-Pacífico. Las razones para esto incluyen una infraestructura de pagos controlada localmente y otras variables únicas de cada ubicación. A medida que se realicen cada vez más

transacciones en línea (un aumento del 518% en las nuevas empresas fundadas en América Latina en 2021), los estafadores tendrán cada vez más oportunidades de aprovecharse de víctimas desprevenidas.

Figura 2

Tasas de Fraude por país



Nota: Tomado de Stripe: *The state of online fraud*, a partir de la dirección de investigación de encuestas. Recuperado de: *https://go.stripe.global/rs/072-MDK-283/images/State_of_online_fraud_report.pdf*

Este problema tampoco es ajeno a personas particulares, según Harán (2020) entre los casos que se reportan en medios de Argentina, México, Perú, Colombia o España, una usuaria afirmó que recibió una botella en vez de una computadora después de realizar una compra en la página web de Internet MercadoLibre. Otro caso ocurrió cuando un consumidor compró un teléfono móvil a través del mismo sitio y luego recibió una piedra. Asimismo, Safatle (2020) de Infobae reporta que vendedores tambien han sido víctimas, toda vez que, un proveedor de teléfonos perdió tanto el equipo como el dinero de la venta.

A nivel nacional en Perú, de acuerdo con Avila (2020) la División de Investigación de Alta Tecnología de la Dirincri ha demostrado que los fraudes patrimoniales e informáticos han

ido en incremento en los últimos años, siendo la mayoría de las denuncias ciudadanas derivadas de compras online y transferencias bancarias, según informó el diario Correo. Según Orlando Mendieta, director de DIVINDAT, al 2 de diciembre de 2020 se recibió 2.600 denuncias por delitos informáticos. De ellas, 1.771 incidentes de fraude informático.

Tabla 2

Denuncias de fraude informático de acuerdo con las estadísticas de la DIVINDAT-DIRINCRI

DENUNCIAS DIVINDAT	2019	2020
CONTRA EL PATRIMONIO - FRAUDE INFORMÁTICO	**1761**	**1771**
Clonación de tarjeta	23	2
Compras fraudulentas por internet	376	187
Operaciones y transferencias electrónicas y/o de fondos no autorizados	1362	1582

Nota: Tomado de Diario Correo, a partir de la dirección de investigación de encuestas. Recuperado de: *https://diariocorreo.pe/edicion/lima/fraude-informatico-1771-personas-han-sido-victimas-de-los ciberdelincuentes-segun-estadisticas-de-la-divindat-nczp-noticia/*

Ademas, Ramírez (como se citó en Bravo T., 2020) aproximadamente el 1,3% de las ventas totales del Perú se obtienen de manera fraudulenta a través de transacciones en línea, afirmó en el programa E-commerce Nights Live.

A nivel local, Lima encabeza la lista de los distritos fiscales con mayores casos de ciberdelitos contra el patrimonio atendidos por el Ministerio Público.

Tabla 3

Casos de ciberdelitos contra el patrimonio atendidos por el Ministerio Publico, según distrito fiscal con mayores casos registrados.

Distrito fiscal	Casos	%
Lima	405	22.7%
Lima Este	326	18.2%
Lima Norte	272	15.2%
Arequipa	177	9.9%
Callao	102	5.7%
Ica	88	4.9%
Lima Sur	64	3.6%
Otros	654	19.8%
Total	**1,788**	**100%**

Nota: Tomado de INDAGA - *Observatorio Nacional de Política Criminal; en base a Sistema de Información de Apoyo al Trabajo Fiscal del Ministerio Publico.* Recuperado de: https://cutt.ly/kNM4lBd

Actualmente los usuarios del e-commerce de Lima enfrentan un gran problema debido al incremento del fraude informático que amenaza su patrimonio económico y el normal desarrollo de sus actividades comerciales a través de medios virtuales.

La mayoría de los internautas aceptan ciegamente los anuncios online, ya sea que aparezcan en páginas web de compra-venta, redes sociales como Facebook o cualquier otro tipo de plataforma online. Esto ha provocado un aumento del delito de fraude informático: mensajes de texto o SMS, Facebook, Instagram, Twitter, entre otros, correos electrónicos y otras plataformas digitales.

Como resultado, los activos de los clientes se verán directamente amenazados. Esto se debe a que cuando los usuarios compran productos y servicios, utilizan sus tarjetas de crédito o débito, transferencias bancarias o datos personales que los ciberdelincuentes podrían explotar con fines ilícitos.

Visto lo anterior, el presente estudio tiene como propósito evaluar el impacto del fraude informático en el comercio electrónico de Lima en el año 2023. Los resultados del estudio permitirán conocer en qué medida este delito ha impactado en el comercio electrónico.

1.1.1. Problema General

¿Cuál es el impacto del fraude informático en el e-commerce de Lima, 2023?

1.1.2. Problemas Específicos

1. ¿Cuál es el impacto de la clonación de tarjetas de crédito en el e-commerce de Lima, 2023?
2. ¿Cuál es el impacto del phishing en el e-commerce de Lima, 2023?
3. ¿Cuál es el impacto del vishing en el e-commerce de Lima, 2023?
4. ¿Cuál es el impacto del Smishing en el e-commerce de Lima, 2023?

1.2. Antecedentes

1.2.1. Antecedentes Nacionales

Verastegui (2022) en el estudio llevado a cabo para lograr el título de abogado en la Universidad César Vallejo que se tituló "El papel del Ministerio Público del centro de Lima en la gestión del delito de fraude informático perpetrado mediante el comercio electrónico" buscó identificar el papel del Ministerio Público en la persecución del fraude informático cometido mediante el comercio electrónico en la lucha contra la ciberdelincuencia. El enfoque fue cualitativo y de diseño de teoría fundamentada. La población estaba compuesta por fiscales del Ministerio Público del centro de Lima, representantes de la Oficina Técnica del Ministerio Público, fuerzas del orden y especialistas en ciberdelincuencia y fraude en el comercio electrónico. Según la investigación, el Ministerio Público de Lima Centro, en la persecución de casos de fraude informático relacionados con el comercio electrónico, ha demostrado que carecía de habilidades, recursos y personal para realizar una investigación y reunir pruebas, peritajes e indicaciones para su trabajo; en consecuencia, sus hallazgos no fueron concluyentes y, peor aún, este delito ha quedado impune.

Tuesta (2022) en el estudio llevado a cabo para lograr el título de abogado en la Universidad Norbert Wiener titulada "El impacto del fraude informático en los derechos fundamentales de las personas en el Cercado de Lima" , buscó identificar el impacto del fraude informático en los derechos fundamentales. El enfoque del estudio fue cualitativo, diseño no experimental y alcance descriptivo – explicativo. La técnica fue el análisis documental. Concluyó que el fraude informático atenta contra derechos básicos y principios esenciales de las personas. Los principios interconectados eran cruciales, pero el principal desafío residía en el plazo limitado para realizar el estudio.

Linares (2022) en el estudio llevado a cabo para lograr el título de abogado en la Universidad Cesar Vallejo titulada "El fraude informático y la protección del patrimonio

durante la pandemia en el distrito fiscal de Lima Este, 2022", buscó determinar cómo el fraude informático afecta la protección del patrimonio durante la pandemia. El estudio utilizó una técnica cuantitativa con un diseño no experimental y alcance descriptivo. Se usó la encuesta para recolectar datos, la población estuvo conformada por 50 personas, entre abogados así como fiscales. Concluyó que el fraude informático tiene un impacto perjudicial en la seguridad de los activos durante una pandemia. Ha habido un notable aumento del 50% en las denuncias de fraude en Internet, concretamente utilizando el método "phishing", lo que afectó el derecho del goce del bien en el distrito fiscal de Lima Este durante la pandemia, en el año 2021.

El phishing es la primera etapa en la manipulación de activos mediante transferencias electrónicas engañosas. El estudio también reveló que el método predominante para adquirir cuentas bancarias es mediante la transmisión de enlaces engañosos por correo electrónico.

1.2.2. Antecedentes Internacionales

Gimenez (2020) en un estudio de grado en Derecho de la Universidad de Alicante títulada "El delito de estafa informática (artículo 249.2.a CP) presenta desafíos en su interpretación e implementación", buscó identificar las principales cuestiones que han sido destacadas por los estudiosos y la práctica jurídica en la interpretación e implementación del artículo, centrándose tanto en la técnica legislativa como en el planteamiento político penal adoptado por el legislador. Concluyó que el fraude informático, tal como lo define el artículo 248.2.a) del Código Penal, es distinto del fraude tal como lo define el artículo 248.1 del Código Penal, a pesar de ser ambos delitos relacionados con el patrimonio. El fraude informático es un tipo de actividad delictiva que realiza de forma independiente y se distingue por los tipos específicos de delitos cometidos.

Preciado & Alvarez (2021) en un estudio de grado en la Universidad Tecnológico de Antioquia que se tituló "Evolución del fraude informático: un problema en las organizaciones

bancarias de Colombia", buscó examinar la progresión del fraude informático entre las empresas de la industria bancaria colombiana. El enfoque de investigación usado en su estudio fue de naturaleza cualitativa, documental así como descriptiva. Concluyó que entre 2014 y 2020, se duplicaron los ataques cibernéticos contra empresas, particularmente aquellas del sector financiero, lo que resultó en un aumento de varios tipos de fraude informático. Los bancos se ven obligados a abordar nuevas técnicas de piratería informática a medida que los ciberdelincuentes han adquirido experiencia en el acceso a los datos de los consumidores. Las TIC permiten la creación de procedimientos de seguridad más sólidos, pero también exponen a los bancos a una mayor vulnerabilidad, ya que los delincuentes están a la vanguardia de la explotación de estas tecnologías.

Mayer & Oliver (2020) en el estudio de la Facultad de Derecho de la Pontifica Universidad Católica de Chile que se tituló "El delito de fraude informático: concepto y delimitación" buscó examinar el delito de fraude informático, centrándose en su concepto y delimitación. Concluyó que todavía falta una comprensión definitiva sobre la definición exacta de fraude informático. Para abordar eficazmente este delito es necesario establecer tres criterios específicos: la manipulación deliberada de datos o programas de sistemas automatizados, la aplicación intencional de perjuicio patrimonial a terceros y la existencia clara de una motivación económica en el responsable de dichos delitos. actividad.

Paguay (2020) en el estudio llevado a cabo para obtener el título profesional abogado en la Universidad Nacional de Ecuador, que se tituló "La perspectiva regulatoria emergente sobre los delitos cibernéticos en las compras en línea", buscó conocer los puntos de vista regulatorios sobre los delitos informáticos en el contexto de las compras en línea. La técnica del estudio utilizó un enfoque mixto, que incluye métodos cualitativos y cuantitativos dentro de un diseño no experimental. La población fueron 53 personas que eran profesionales del derecho. Las estrategias de recolección de datos utilizadas fueron la administración de un

cuestionario y la utilización de una guía de entrevista. Concluyó que un tipo novedoso de actividad delictiva en el comercio por internet surge cuando el comprador incurre en conductas fraudulentas, las cuales no están contempladas explícitamente en el Código Orgánico Integral Penal del Ecuador. Tradicionalmente, los comerciantes a menudo se han enfrentado a sanciones por no entregar cosas, mientras que los consumidores rara vez se han enfrentado a tales consecuencias. Esto pone de relieve la necesidad de un mayor control de los delitos informáticos.

1.3. Objetivos

- ***Objetivo General***

  Determinar el impacto del fraude informático en el e-commerce de Lima, 2023.

- ***Objetivos Específicos***

  OE.1. Determinar cuál es el impacto de la clonación de tarjetas de crédito en el e-commerce de Lima, 2023.

  OE.2. Determinar cuál es el impacto del phishing en el e-commerce de Lima, 2023.

  OE.3. Determinar cuál es el impacto del vishing en el e-commerce de Lima, 2023.

  OE.4. Determinar cuál es el impacto del smishing en el e-commerce de Lima, 2023.

1.4. Justificación

Se requiere justificar o exponer los fundamentos del estudio, ya que toda investigación tiene como objetivo solucionar algún problema. Fernández (2020) destaca el hecho de que existen varias razones posibles para realizar una investigación, incluyendo consideraciones teóricas, prácticas, metodológicas, sociales, económicas, tecnológicas y doctrinales. Asimismo, es preciso señalar que no todas las investigaciones abarcan íntegramente las justificaciones señaladas anteriormente, sino alguna de ellas. Los tipos de justificación a utilizar en una investigación depende de la naturaleza y objetivos del estudio.

El presente estudio abarca tres tipos de justificación que son: teórica, practica y social.

A continuación, explicamos cada una de ellas.

1.4.1 Justificación Teórica

Teóricamente, este estudio tiene mérito ya que pretende enriquecer nuestra comprensión de las ramificaciones técnicas y legales del fraude informático en el E-commerce. También, estudia el impacto de las distintas modalidades de fraude informático en el contexto de las transacciones en línea, así como los mecanismos legales y tecnológicos que pueden implementarse para prevenir y mitigar sus efectos.

1.4.2. Justificación Práctica

Teóricamente, este tipo de justificación existe cuando el desarrollo de la investigación contribuye a resolver un problema o, se proponen estrategias que al ser aplicadas contribuirán a resolverlo (Fernández, 2020). El estudio tiene una justificación práctica, ya que los hallazgos de esta permiten estrategias a los operadores de justicia (Jueces, fiscales y policía nacional) a fin de que se desarrolle una efectiva persecución del delito, así como una debida sanción, ello con el fin de reducir la ciberdelincuencia en nuestro país.

1.4.3. Justificación Social

Esta justificación se encuentra presente cuando la investigación esté orientada a mejorar la sociedad, puesto que debe tener cierta relevancia para la misma, alcanzando trascendencia y alcance o proyección social (Fernández, 2020). El estudio tiene una justificación social ya que los resultados de esta ayudan a proponer cambios normativos que permitan reducir el impacto del fraude informático en el E-commerce beneficiando a los usuarios del comercio electrónico y a la sociedad en general.

1.4.4. Limitaciones

Según Bernal (2016) en el desarrollo de una investigación existen tres tipos de limitaciones que son: las limitaciones de tiempo, de territorio así como de recursos.

1.4.4.1 Limitaciones de tiempo. Según Bernal (2016) las limitaciones de tiempo se relacionan con el marco temporal en la cual se desarrolla el fenómeno a estudiar. Este puede ser retrospectivo o prospectivo. Es retrospectivo si el fenómeno a estudiar ocurrió antes de la planificación y diseño de la investigación. Es posible en el futuro. De manera similar a cómo se pueden recopilar datos de forma longitudinal o transversal. Recopilar datos todos a la vez es lo que los hace transversales. Los datos recopilados en varios momentos lo convierten en un estudio longitudinal. Este estudio es transversal y prospectivo. Es prospectiva porque el fenómeno a estudiar se desarrolla después de la planificación y diseño de la investigación durante el 2023. Es transeccional puesto que la recolección de datos se lleva a cabo en un solo momento durante el 2023.

1.4.4.2. Limitaciones de territorio. Según Bernal (2016) las limitaciones de territorio se relacionan con el ámbito geográfico dentro del cual se desarrolla el fenómeno a estudiar. En la presente tesis el ámbito geográfico en el que se da el fenómeno a estudiar se circunscribe a la ciudad de Lima.

1.4.4.3. Limitaciones de Recursos. Las limitaciones en recursos se relacionan con los recursos necesarios para el desarrollo de una investigación (Bernal, 2016). El estudio se desarrolla con recursos propios y si bien existen algunos limites respecto a los recursos a utilizar estos podrán ser cubiertos por el investigador.

1.5. Hipótesis

- ***Hipótesis General***

  El fraude informático tiene un impacto significativo en el e-commerce de Lima, 2023

- ***Hipótesis Especificas***

  HE.1. La clonación de tarjetas de crédito tiene un impacto significativo en el e-commerce de Lima, 2023.

  HE.2. El phishing tiene un impacto significativo en el e-commerce de Lima, 2023.

HE.4. El vishing tiene un impacto significativo en el e-commerce de Lima, 2023.

HE.5. El Smishing tiene un impacto significativo en el e-commerce de Lima, 2023.

II. MARCO TEÓRICO

2.1. Bases teóricas sobre el tema de Investigación

2.1.1. Bases teóricas respecto al Fraude Informático

El campo de la teoría criminal ha comenzado a prestar más atención al fraude informático en los últimos años. Siendo el protagonista de este campo, su importancia en el cibercrimen es indiscutible. Hace unos treinta años, el fraude informático relacionado con las transferencias financieras electrónicas fue el punto de partida para un estudio exhaustivo del ciberdelito. Hoy en día, el fraude informático continúa como figura central en los ciberdelitos, debido a su impacto económico y su ejecución frecuente, que ha sido impulsada por el uso del comercio electrónico (Mayer y Oliver, 2020).

No obstante, Según Mayer y Oliver (2020) a pesar del interés y relevancia del tema, persiste una falta de claridad en torno a la definición y a los comportamientos constitutivos del fraude informático. Aunque la manipulación de datos o programas de sistemas informáticos para causar perjuicio patrimonial es la noción primaria, la amplitud del término incluye diversas conductas.

Al respecto, Vinelli (2021) sugiere que los casos en los que un agente transfiere ganancias obtenidas ilícitamente a su propia cuenta bancaria o a la de otra parte, o un agente que borra registros financieros en un esfuerzo por cambiar la situación financiera de una persona, constituyen fraude informático, alguien que de manera fraudulenta altere la cantidad de pedidos necesarios en el sistema informático para transferir el exceso de artículos a otra parte. Además, señala que no es necesario el uso de fuerza física o amenazas para que se cometa este delito; por lo tanto, esta conducta es inherentemente engañosa, razón por la cual algunos escritores se refieren a ella como fraude computacional.

2..1.1.1. El fraude Informático y su Vínculo con Delitos Informáticos. El fraude informático está estrechamente relacionado con otras actividades delictivas, incluido el hacking, que a veces se considera sinónimo de delito cibernético. El acceso no permitido a datos o programas es un factor común que conecta ambos comportamientos, lo que puede llevar a que ocurran simultáneamente (Mayer y Oliver, 2020).

2.1.1.2. El fraude Informático y su conexión con el Sabotaje Informático y Estafa. El fraude informático a menudo se asocia con el sabotaje informático debido a la manipulación de datos, mientras que su relación con la estafa también es notable. La distinción entre ambos radica en el medio para provocar perjuicio: manipulación de datos en el fraude informático y engaño en la estafa (Mayer y Oliver, 2020).

2.1.1.3. Características del Fraude Informático. El fraude informático abarca la modificación deliberada de datos en cualquier etapa del ciclo de procesamiento, incluida la entrada, el programa y la salida. El objetivo es adquirir un beneficio financiero a costa de otra persona o grupo mediante el uso de computadoras, ya sea directa o indirectamente. (Cangalaya, 2020).

2.1.1.4. Clasificación del Fraude Informático. En la clasificación de fraudes informáticos, se destacan tres tipos cometidos a través de la manipulación de computadoras. En primer lugar, la manipulación de datos de entrada involucra alterar, omitir o introducir información falsa en un ordenador. Este tipo de fraude es común, sencillo de realizar y difícil de detectar, no exigiendo habilidades técnicas avanzadas (Cangalaya, 2020). El segundo tipo, la manipulación de programas, denominada Caballo de Troya, implica interferir en el procesar información al alterar programas existentes o insertar instrucciones encubiertas en programas para permitir funciones no autorizadas junto con sus operaciones normales (Cangalaya, 2020). En tercer lugar, está la manipulación de los datos de salida, que establece objetivos para el funcionamiento del sistema informático y luego los ejecuta una y otra vez si surge un problema.

Un tipo común de fraude en cajeros automáticos implica la falsificación de instrucciones utilizadas para la recopilación de datos. Hoy en día, se utilizan software y hardware especializados para codificar información fraudulenta en tarjetas financieras. La seguridad de los datos así como los sistemas es complicada y está plagada de obstáculos legales y tecnológicos causados por varios tipos de fraude informático (Cangalaya, 2020).

2.1.1.5. Formas de Control del Fraude Informático. En la prevención y control del fraude informático, se recomienda no aceptar publicidad ni ofertas sospechosas, instalar programas de seguridad en plataformas virtuales y capacitar a usuarios. La adquisición de programas con licencia original y actualizaciones, así como la modificación periódica de contraseñas, fortalecen la seguridad. Utilizar navegadores seguros con "https://" y un candado cerrado en la barra de navegación garantiza autenticidad. Ante el fraude, se deben tomar medidas correctivas: instalar antivirus, firewall y software original. Exigir sistemas de seguridad robustos en plataformas empresariales y protegerse contra spyware también es crucial para prevenir y afrontar amenazas (Cangalaya, 2020).

2.1.2. Bases Teóricas Respecto al E- commerce

2.1.2.1. Orígenes y Evolución del E- Commerce. El comercio electrónico se trata de una novedosa forma de consumir que ha tenido una influencia significativa en las transacciones económicas que se producen entre clientes y empresas a escala global, regional, nacional y local. Este modo de funcionamiento se ha ido generalizando gradualmente en todos los ámbitos económicos. El comercio electrónico permite a los consumidores explorar múltiples opciones de compra a través de medios electrónicos, accediendo a diferentes sitios web para comparar precios, calidad y características de bienes y servicios, así como detalles postventa, fechas de entrega, garantías y plazos de pago (González, 2020).

Su origen se relaciona con el surgimiento de Internet y transacciones anteriores, y se estandarizó con el intercambio de datos electrónicos en los años setenta, facilitando la

comunicación entre grandes empresas. La viabilidad del comercio electrónico se vio reforzada por el soporte de ciclo de vida asistido por computadora y las transferencias electrónicas de fondos, que permiten la transmisión de fondos y pagos en línea. Sin embargo, la llegada de la World Wide Web (WWW) y el cifrado de seguridad SSL 3.0 en la década de 1990, debido a los avances en las TIC, provocó su meteórico ascenso (González, 2020).

Los beneficios del comercio electrónico han llevado al desarrollo de diversas opciones para fomentar su uso, brindando a los consumidores la posibilidad de adquirir bienes tangibles e intangibles con entregas digitales o físicas, aprovechando la comodidad de las transacciones en línea y la expansión de servicios de entrega a domicilio (González, 2020). Además, Verma & Dixit (2023) refieren que, el futuro del comercio electrónico está determinado por tendencias, desafíos y oportunidades clave, así como con los avances tecnológicos, así como las preferencias de los usuarios, los cuales impulsan una mayor expansión. Asimismo, Chao, (2023) señala que, el e-commerce revolucionó el comercio mundial de bienes, reduciendo los costos operativos y ofreciendo una amplia variedad de bienes, sin embargo carece de la experiencia social del comercio minorista tradicional. Aunado a ello, Sharma, Srivastva, & Fatima (2023) coinciden en que el comercio electrónico y la transformación digital han redefinido el comercio moderno, lo que ha llevado a una mayor eficiencia operativa, un mayor alcance en el mercado y experiencias de consumo enriquecidas.

2.1.2.2. Tipos de E-commerce. El comercio electrónico abarca una variedad de tipos de transacciones en línea que involucran a consumidores (C), empresas (B) y gobiernos (G). Estos tipos incluyen el B2B, donde las empresas intercambian bienes y servicios entre sí, el B2C, entre los muchos tipos de interacciones entre empresas y gobiernos (B2G) se encuentran los intercambios entre consumidores y empresas (C2B), en los que los individuos venden productos y servicios a las empresas (Organización para la Cooperación y el Desarrollo Económico) [OCDE], 2020).

2.1.2.3. Ventajas del E-commerce El comercio electrónico ofrece ventajas significativas. En primer lugar, brinda la oportunidad de mejorar la eficiencia y flexibilidad interna al agilizar tanto los procesos productivos como operativos, al tiempo que facilita una comunicación más rápida con proveedores y clientes, lo que permite satisfacer sus necesidades de manera más efectiva. En segundo lugar, posibilita la expansión y penetración en nuevos mercados, ofreciendo la ventaja de llegar a un público más amplio a un costo reducido. Esto implica no solo alcanzar diferentes regiones geográficas, sino también acceder a un mercado global, favoreciendo la comunicación con clientes internacionales de manera similar a la local. Por tanto, resulta esencial establecer una política internacional clara al desarrollar la presencia en línea, considerando que es probable que desde los primeros meses de funcionamiento del sitio web se reciban consultas de mercados internacionales (Malca, 2020).

2.2. Definición de Términos Básicos

2.2.1. Fraude Informático

Vinelli (2021) indica que el fraude informático se define como el uso de medios engañosos o fraudulentos para lograr beneficios económicos mediante la manipulación de sistemas informáticos. Zevallos (2020) identifica varias modalidades de fraude informático, en las cuales se encuentran las transacciones en línea que utilizan datos de tarjetas, la clonación de tarjetas, el phishing, las transferencias fraudulentas, el malware y el vishing. No obstante, en sentido estricto, Mayer y Oliver (2020) implican que el concepto de fraude informático está vinculado a la adquisición de pérdidas económicas mediante la manipulación de datos.

2.2.2. Clonación de tarjetas de crédito o débito

Es un tipo de fraude que consiste en crear una copia exacta de una tarjeta de crédito o débito aprovechándose de información vulnerable obtenida a través de ingeniería social, malware o dispositivos maliciosos; esto permite a los atacantes acceder a los fondos de la cuenta de la víctima para realizar transacciones no autorizadas. (Moreno, 2022). Asimismo, se

define como una conducta delictiva mediante la cual el agente hace uso de dispositivos skimmer, que leen bandas magnéticas en tarjetas de crédito, así como débito, para perpetrar fraudes en locales como restaurantes, gasolineras y otros. El siguiente paso es transferir los datos a una computadora y luego a una segunda tarjeta clonada que tenga la misma información que la original. (Acurio del Pino, 2020).

2.2.3. Phishing

El objetivo de esta conducta delicitiva es usurpar la identidad de la víctima, recopilando información confidencial mediante engaños, incluidos detalles financieros, detalles de cuentas, contraseñas así como números de tarjetas de crédito. Como ejemplo, consideremos el caso de correos electrónicos fraudulentos o ventanas emergentes que engañan a los usuarios para que introduzcan su información personal. Esto facilita que los delincuentes accedan a estos datos. (Zevallos, 2020). Asimismo, Goodrich (2022) lo define como un ataque de ingeniería social que implica el envío de mensajes fraudulentos que parecen proceder de fuentes confiables. El propósito es manipular a la víctima para que revele información confidencial.

2.2.4. Vishing

El vishing o tambien conocido como “pishing por voz” es un ataque cibernetico que utiliza llamadas telefónicas para engañar a las víctimas y para obtener información personal o financiera, utilizando técnicas de persuasión y manipulación para ganar la confianza de la víctima. (Hadnagy, 2020). Por otro lado, se tiene que esta actividad delictiva se lleva a cabo usando el envío de un mensaje de texto, en el cual el perpetrador se hace pasar por una institución bancaria. A través de algún pretexto, solicita que el destinatario se comunique con un número telefónico falso o que responda al mensaje con información confidencial, como el número de tarjeta o la contraseña secreta (Zevallos, 2020).

2.2.5. Smishing

Esta conducta delictiva está basada en el uso de mensajes de texto a través de

dispositivos de telefonía móvil. En estos mensajes, el número de origen se oculta intencionadamente, y con frecuencia, el contenido incluye direcciones de entidades aparentemente legítimas. Sin embargo, al hacer clic en los enlaces proporcionados, en realidad se redirige al usuario a una página de phishing o se introduce un código malicioso en el dispositivo móvil. Un ejemplo ilustrativo es cuando la víctima recibe mensajes de texto que afirman que ha sido agraciada con un premio y, para recibirlo, se le insta a acceder a un enlace presente en el propio mensaje (Zevallos, 2020). Ademas, Goodrich (2022) define el smishing como un tipo de ataque cibernético que utiliza mensajes de texto con el objetivo de obtener información personal o financiera, aprovechándose de la confianza de las víctimas, mediante el engaño y la manipulación.

2.2.6. E- Commerce

Higuerey (2019) afirma que el comercio electrónico, también conocido como comercio electrónico, facilita el intercambio en línea de bienes, así como servicios a través de redes sociales y aplicaciones móviles. De igual forma, como afirma Galeano (2024), se denomina comercio electrónico al acto de comprar y vender productos, así como servicios a través de Internet. Además, Robayo-Botiva, (2020) destaca que la realización de transacciones comerciales utilizando Internet, la World Wide Web (web), motores de búsqueda (navegadores) y aplicaciones móviles (apps) que operan en dispositivos móviles se conoce como comercio electrónico.

2.2.7. Redes Sociales

Son plataformas en línea que combinan características de redes sociales tradicionales con funcionalidades de comercio electrónico. En este tipo de redes sociales, los usuarios no solo pueden interactuar y conectarse entre sí, sino que también pueden explorar, comprar y vender productos o servicios directamente en la plataforma. Estas redes sociales de comercio electrónico permiten a los usuarios crear perfiles de comprador o vendedor, exhibir productos,

realizar transacciones y realizar actividades de compra y venta dentro de la misma plataforma. Además, las redes sociales son herramientas digitales que permiten a los usuarios generar y compartir contenido, interactuar con otros y realizar compras, convirtiéndose en un canal importante para el comercio electrónico. (García Ávila, 2022)

2.2.8. Páginas Web

Las páginas web de comercio electrónico, también conocidas como tiendas en línea o sitios de compras en línea, son plataformas en línea diseñadas para facilitar la compra, así como venta de productos o servicios mediante Internet. Estas páginas web permiten a los usuarios explorar catálogos de productos, comparar opciones, agregar productos al carrito de compras, realizar transacciones y completar compras desde la comodidad de dispositivos electrónicos. Asimismo, las páginas web son plataformas digitales funcionan como tiendas virtuales, donde las empresas pueden vender productos o servicios y os clientes pueden navegar, seleccionar y comprar de manera remota. (Molina Ruiz, 2022)

2.2.9. Aplicaciones Móviles

Las aplicaciones móviles de comercio electrónico, también conocidas como aplicaciones de compras o tiendas móviles, son aplicaciones desarrolladas para dispositivos móviles, que permiten a los usuarios examinar, comprar e intercambiar bienes y servicios fácilmente en estas plataformas. Además, según Jiménez (2022) las aplicaciones móviles funcionan como plataformas de venta en línea que permiten a los clientes realizar compras, acceder a servicios y realizar pagos desde cualquier lugar y en cualquier momento.

2.3. Marco Legal

2.3.1. Convenio sobre delitos cibernéticos, Convenio de Budapest sobre delitos cibernéticos o Convenio de Budapest

El Convenio de Budapest es el primer tratado internacional cuyo objetivo es salvaguardar a la sociedad contra el cibercrimen y los delitos en Internet mediante el

establecimiento de una legislación internacional adecuada, la mejora de los métodos de investigación e incentiva una mayor colaboración entre los estados miembros. (Convenio sobre la Ciberdelincuencia, 2001). Este tratado tiene como objetivos:

- Armonizar los componentes nacionales del derecho penal relativos a infracciones y las normas relacionadas con los delitos informáticos a fin de proporcionar un marco regulatorio uniforme para los delitos cibernéticos.
- Para investigar y procesar estos y otros delitos perpetrados mediante sistemas informáticos o pruebas electrónicas, es fundamental prohibir las capacidades procesales del derecho penal interno.
- La implementación rápida y eficiente de un marco para la colaboración internacional.

En este acuerdo se establecen los tres pilares necesarios para combatir el cibercrimen. El objetivo principal del primer eje es categorizar las diversas formas de ciberdelito. En cuanto al segundo eje, tenemos las normas procesales, mediante la cual se establece procedimientos para salvaguardar la evidencia digital y los instrumentos para manipular esta evidencia. Y como ultimo eje, se tiene las normas para la cooperación internacional; las cuales son reglas de colaboración para la investigación de cualquier tipo de delito utilizando evidencia digital, ya sea informática o convencional. Cubre temas que incluyen la extradición, la recopilación o transmisión de pruebas digitales y la ubicación de los sospechosos.

El Congreso de la República aprobó por abrumadora mayoría la adhesión del Perú a la Convención de Budapest, la primera convención internacional en el Perú para combatir los delitos informáticos en Internet, mediante Resolución Legislativa N° 30913 del 13 de febrero de 2019.

2.3.2. Ley Nº 30096 - Ley de Delitos informáticos

La Ley Nº 30096 - Ley de Delitos Informáticos es un esfuerzo para frenar y penalizar las prácticas comunes que causan daños a los sistemas informáticos, datos y otros activos

legales valiosos cuando se perpetran mediante el uso de las tecnologías de la información o de la comunicación. Su objetivo es garantizar que la batalla contra el ciberdelito tenga éxito (Ley de Delitos informáticos, 2013).

2.3.3. Decreto Legislativo N° 1614, que modifica la Ley N° 30096 – Ley de Delitos Informáticos

El diario gubernamental El Peruano emitió el Decreto Legislativo N° 1614 el 21 de diciembre de 2023, que modifica los numerales 2 y 8 de la Ley N° 30096, también busca combatir y disuadir el cibercrimen elevando el castigo mínimo por el acceso ilegal e identificando y describiendo ciertos comportamientos para delitos como el fraude informático.

Según el artículo 2, que trata del acceso ilegal, un individuo se enfrenta a una pena privativa de la libertad de uno a cuatro años y con treinta a noventa días-multa, por acceder intencional e ilegalmente a todo o parte de un sistema informático, o por ir más allá de lo permitido. Asimismo, señala que, si un agente vulnera de forma dolosa e ilegal las medidas de seguridad dispuestas para impedirle el acceso al sistema informático, total o parcialmente.

El artículo 8 de la ley señala que el fraude informático como el acto deliberado e ilícito de adquirir algo mediante la explotación de datos o sistemas informáticos, en perjuicio de otra parte. Las penas por este delito incluyen multas monetarias que van de sesenta a ciento veinte días y prisión por un período de cuatro a ocho años. Si los bienes en cuestión son propiedad del Estado y están destinados a programas asistenciales, la pena oscila entre ochenta a cien días de multa y una pena de cárcel de 8 a 14 años. Ciertas sanciones también se extienden a quienes participan en la transferencia de activos en determinadas situaciones (Decreto Legislativo N° 1614, 2023).

III. MÉTODO

3.1. Tipo de Investigación

Esteban (2018) señala que existen dos tipos de investigación que son: la investigación aplicada y la investigación básica. La primera busca generar nuevos conocimientos para enriquecer la ciencia o una determinada disciplina y la segunda busca solucionar problemas prácticos relacionados con el campo de los procedimientos de producción, circulación, distribución de bienes.

La presente tesis es de tipo básica porque su desarrollo aporta al conocimiento del fraude informático en el e-commerce. Este nuevo conocimiento permitió realizar recomendaciones para mejorar la legislación nacional que regula este delito.

3.1.1 Enfoque de Investigación

Hernández & Mendoza (2018) señala que existen tres rutas de investigación: cuantitativa, cualitativa y mixta.

El enfoque cuantitativo aplica técnicas de estadística el cual es un enfoque cuantitativo de la investigación que usa datos recopilados para cuantificar las variables del estudio en un esfuerzo por descubrir patrones que confirmen las hipótesis expresadas previamente. (Hernández & Mendoza,2018).

Dado que el desarrollo del estudio se basa en estadística descriptiva e inferencial para evaluar las hipótesis, esta investigación sigue una metodología cuantitativa.

3.1.2 Diseño de investigación

Hernández y Mendoza (2018) refieren que el diseño de investigación es un modelo de cómo se recopilará información para el estudio. El enfoque cuantitativo señala que el diseño experimental y el diseño no experimental son las dos categorías principales de métodos de investigación. Para ver cómo el cambio de una variable afecta a la otra, el diseño experimental

utiliza un experimento controlado. Un diseño no experimental, por otro lado, no incluye realizar experimentos sino estudiar variables tal como ocurren en la naturaleza.

Debido a que el objetivo al realizar esta tesis es observar las variables de estudio en su hábitat natural, inalteradas, se optó por un método no experimental.

3.1.3. Nivel o Alcance de Investigación

Según Hernández y Mendoza (2018) el proceso de investigación consta de cuatro fases diferenciadas. Es importante tener en cuenta los grados de exploración, descripción, correlación y explicación. El nivel exploratorio se centra en cuestiones desconocidas o poco estudiadas. Conocer y definir las características de las variables de investigación es el objetivo del nivel descriptivo. Mientras que el nivel explicativo intenta arrojar luz sobre los orígenes de un fenómeno, el nivel correlacional se esfuerza por cuantificar el grado en que dos o más variables de investigación están relacionadas.

Debido a que medir el vínculo entre las dos variables de estudio es el objetivo del estudio, tiene un nivel correlacional. En otras palabras, se pretende determinar en qué medida el fraude informático impacto en el E-commerce.

3.2. Ámbito Temporal y Espacial

El estudio se llevó a cabo en el año 2023 con respecto al período de tiempo. De manera similar, la ciudad de Lima sirve como límite geográfico o espacial para el estudio.

3.3. Variables

Las variables de estudio son las siguientes:

- Variable X: Fraude informático
- Variable Y: E-commerce

Las dimensiones de la “Variable X: Fraude informático” son las siguientes:

Dimensión 1: Clonación de tarjetas de crédito.

Dimensión 2: Phishing

Dimensión 3: Spear phishing

Dimensión 4: Transferencias electrónicas fraudulentas

Dimensión 5: Compras por internet mediante información robada de tarjetas de crédito o débito.

Dimensión 6: Vishing

Dimensión 7: Ransomware

Dimensión 8: Smishing

Las dimensiones de la “Variable Y: E-commerce” son las siguientes:

Dimensión 1: Redes Sociales

Dimensión 2: Páginas Web

Dimensión 3: Aplicaciones Móviles

A continuación, se presenta la matriz de operacionalización de variables.

3.3.1. Matriz de Operacionalización de Variables.

Tabla 4

Matriz de operacionalización de variables

VARIABLE	DIMENSIONES	INDICADORES	ESCALA
VARIABLE X: FRAUDE INFORMÁTICO	**1. Clonación de tarjetas de crédito.-**	• Casos Investigados • Pérdidas Financieras • Usuarios Afectados	Ordinal
	2. Phishing.-	• Casos Investigados • Pérdidas Financieras • Usuarios Afectados	Ordinal
	3. Vishing.-	• Casos Investigados • Pérdidas Financieras • Usuarios Afectados	Ordinal
	4. Smishing.-	• Casos Investigados • Pérdidas Financieras • Usuarios Afectados	Ordinal
VARIABLE Y: E- COMMERCE	**Redes Sociales.-**	Facebook WhatsApp	Ordinal
	Paginas Web.-	Páginas web	Ordinal
	Aplicaciones Móviles.-	Aplicaciones Móviles	Ordinal

3.4. Población y Muestra

3.4.1. Población

De acuerdo con Hernández & Mendoza (2018) la población la constituyen elementos los cuales poseen en común determinadas características.

La población de 23 personas de esta investigación está compuesta por asistentes en función fiscal y fiscales de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima.

3.4.2. Muestra

Hernández & Mendoza (2018) señalan que la muestra es un subconjunto que es representativo de la población que se estudia y se investiga recopilando datos sobre algunas de las características de la población. Si el investigador realizara una investigación sobre toda la población, entonces estaríamos ante un censo, como afirma el mismo autor.

Por tanto, en esta investigación se utilizará un censo; es decir, 23 personas compuestas entre fiscales y asistentes en función fiscal de la Fiscalía Corporativa Especializada en Delitos Cibernéticos de Lima conformarán la muestra, la cual equivaldrá a la población.

3.5. Instrumentos

3.5.1. Técnicas e Instrumentos de recolección de datos

Según Useche (2019) Se requiere una estrategia de recolección de datos para cuantificar las variables. De manera similar, como se indicó anteriormente, las ciencias sociales utilizan una amplia gama de métodos de recopilación de datos, que incluyen, entre otros, sesiones en profundidad, entrevistas, encuestas, análisis documental y observación. Además, existen herramientas especializadas para recopilar datos para cada uno de estos métodos.

En el estudio se usó la encuesta como técnica de recolección de datos así como el cuestionario de instrumento. En concreto, se utilizaron dos cuestionarios que nos ayudaron a recoger información sobre cada una de las dos variables de estudio. Los cuestionarios que se utilizaron son los siguientes:

Cuestionario 1: Variable X - Fraude Informático

Cuestionario 2: Variable Y – E - commerce

3.5.2. Confiabilidad y Validez de los Cuestionarios

La confiabilidad se determinará utilizando el método Alfa de Cronbach.

Asimismo, el método del juicio de expertos comprobará la validez, por lo que solicitó a tres expertos en la materia que revisaran el cuestionario para asegurar de que fuera legítimo.

3.6. Procedimientos

Para el desarrollo del presente estudio se siguió los procedimientos:

1.- La población de investigación se estudió mediante la herramienta de recolección de datos.

2.- Los datos recogidos fueron sometidos a análisis estadístico utilizando SPSS con fines tanto descriptivos como inferenciales.

3.- La prueba de hipótesis se realizó analizando e interpretando los hallazgos adquiridos.

4.- Se realizó la discusión de hallazgos.

5.- La investigación concluyó con la presentación de sus resultados y sugerencias.

3.7. Análisis de datos

Para el análisis de los datos se usó el software estadístico SPSS V. 25, utilizando tanto estadística descriptiva como inferencial para alcanzar el objetivo.

La estadística descriptiva se utilizó para mostrar los datos recopilados, utilizamos el gráfico de barras y la distribución de frecuencia.

La estadística inferencial tiene como propósito poner a prueba las teorías. Verificar si los datos son normales es el primer paso para elegir la mejor prueba de hipótesis. Dos posibles pruebas para esto son las pruebas de Kolmogorov-Smirnov y Shapiro-Wilk. Cuando en una muestra hay menos de cincuenta elementos se realiza la prueba de Shapiro-Wilk; cuando son más de cincuenta, se emplea la prueba de Kolmogorov-Smirnov. (Flores, 2021).

Dado que el estudio contó con un tamaño de muestra de 23 personas, entre fiscales y asistentes en función fiscal, se utilizó la prueba de Shapiro-Wilk para comprobar si los datos seguían una distribución normal. Seleccionamos la prueba de hipótesis óptima en función de los datos.

3.8. Consideraciones éticas

En el estudio se tuvo cuenta la búsqueda de la verdad, toda vez que la investigación se desarrolló con objetividad para poder alcanzar resultados más próximos a la realidad. También se tuvo en cuenta el respeto a la confidencialidad de los encuestados. Asimismo, se respetó la propiedad intelectual; así como el reconocimiento de la autoría de las obras utilizadas. Para ello, se citaron y referenciaron los trabajos intelectuales que se utilizaron utilizando las Normas APA.

IV. RESULTADOS

4.1. Resultados Relacionados con el Objetivo General

El objetivo general es evaluar el alcance del delito cibernético en el mercado en línea de Lima en el año 2023. Se produjeron los siguientes hallazgos.

4.1.1. Análisis e Interpretación de Resultados

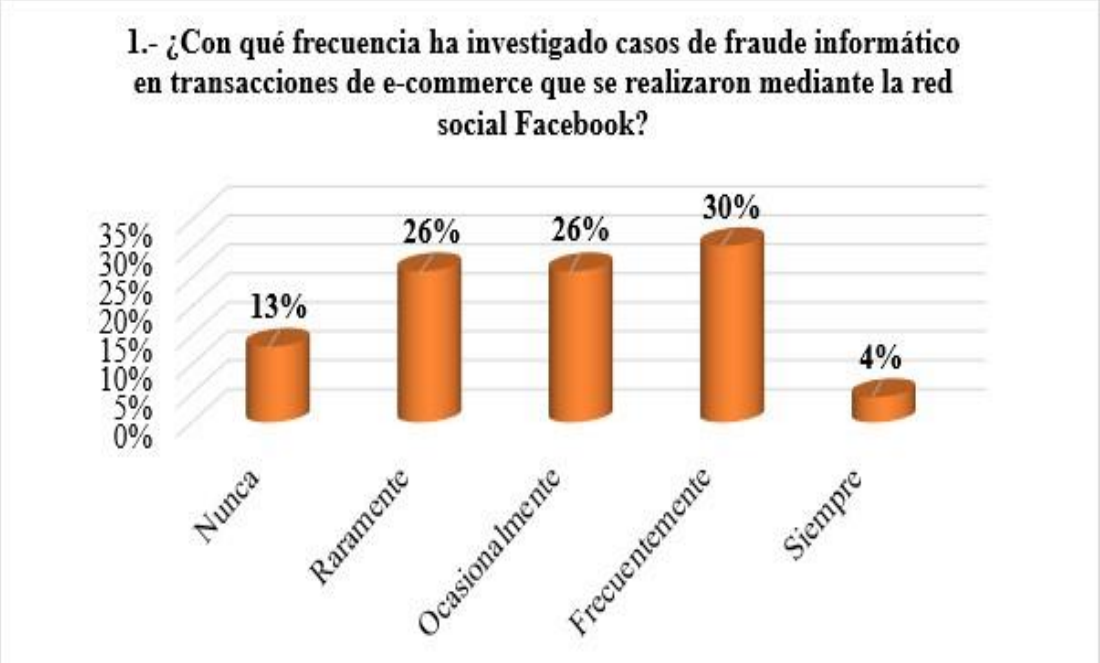
Tabla 5

Fraude informático en transacciones de e-commerce en Facebook

1.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la red social Facebook?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Nunca	3	13%	13%	13%
Raramente	6	26%	26%	39%
Ocasionalmente	6	26%	26%	65%
Frecuentemente	7	30%	30%	96%
Siempre	1	4%	4%	100%
Total	23	100%	100%	

Figura 3

Fraude informático en transacciones de e-commerce en Facebook



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 1 del cuestionario 2: *¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la red social Facebook?* El 13% respondió nunca, el 26% raramente, otro 26% respondió ocasionalmente, el 30% respondió frecuentemente y 4% respondió siempre.

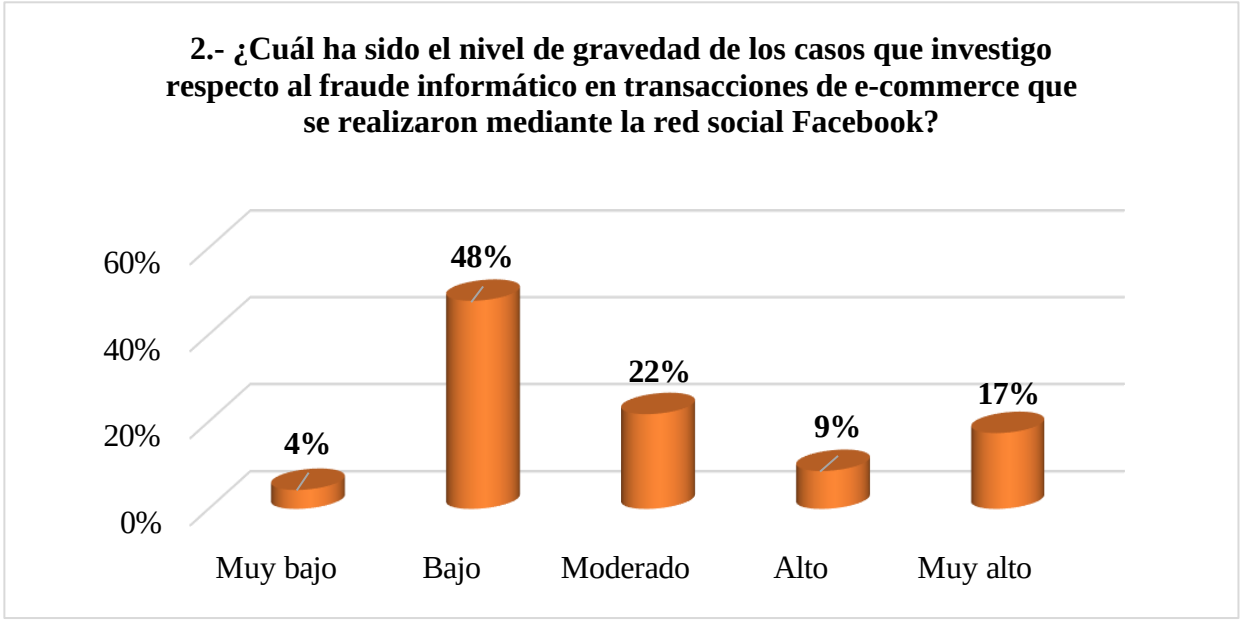
Tabla 6

Nivel de Gravedad – Fraude Informático Facebook

2.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante la red social Facebook?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	1	4%	4%	4%
Bajo	11	48%	48%	52%
Moderado	5	22%	22%	74%
Alto	2	9%	9%	83%
Muy alto	4	17%	17%	100%
Total	23	100%	100%	

Figura 4

Nivel de Gravedad – Fraude Informático Facebook



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 2 del cuestionario 2: *¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante la red social Facebook?* El 4% respondió muy bajo, el 48% bajo, otro 22% respondió moderado, el 9% respondió alto y 17% respondió muy alto.

Tabla 7

Regulación contra Fraude informático en E-commerce en Facebook

3.- ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la red social Facebook?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
En desacuerdo	13	57%	57%	57%
Ni de acuerdo ni en desacuerdo	9	39%	39%	96%
Totalmente de acuerdo	1	4%	4%	100%
Total	23	100%	100%	

Figura 5

Regulación contra Fraude informático en E-commerce en Facebook

Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 3 del cuestionario 2: *¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la red social Facebook?* El 57% respondió en desacuerdo, otro 39% respondió ni de acuerdo ni en desacuerdo, y el 4% respondió totalmente de acuerdo.

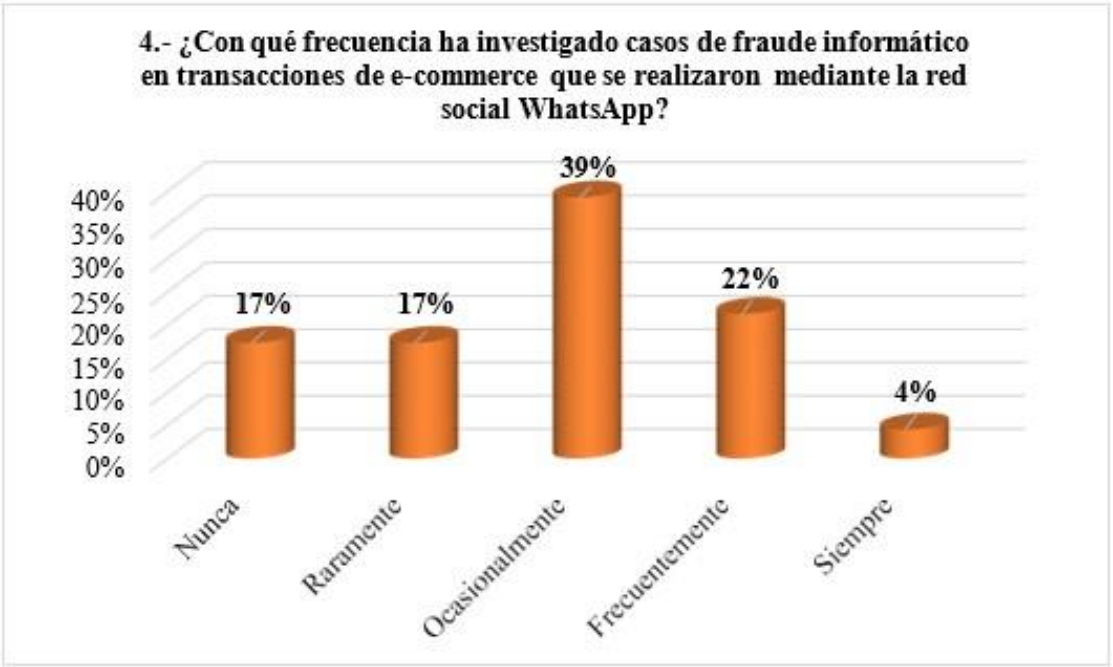
Tabla 8

Fraude informático en transacciones de e-commerce en WhatsApp

4.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la red social WhatsApp?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Nunca	4	17%	17%	17%
Raramente	4	17%	17%	35%
Ocasionalmente	9	39%	39%	74%
Frecuentemente	5	22%	22%	96%
Siempre	1	4%	4%	100%
Total	23	100%	100%	

Figura 6

Fraude informático en transacciones de e-commerce en WhatsApp



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 4 del cuestionario 2: *¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la red social WhatsApp?* El 17% respondió nunca, el 17% raramente, otro 39% respondió ocasionalmente, el 22% respondió frecuentemente y 4% respondió siempre.

Tabla 9

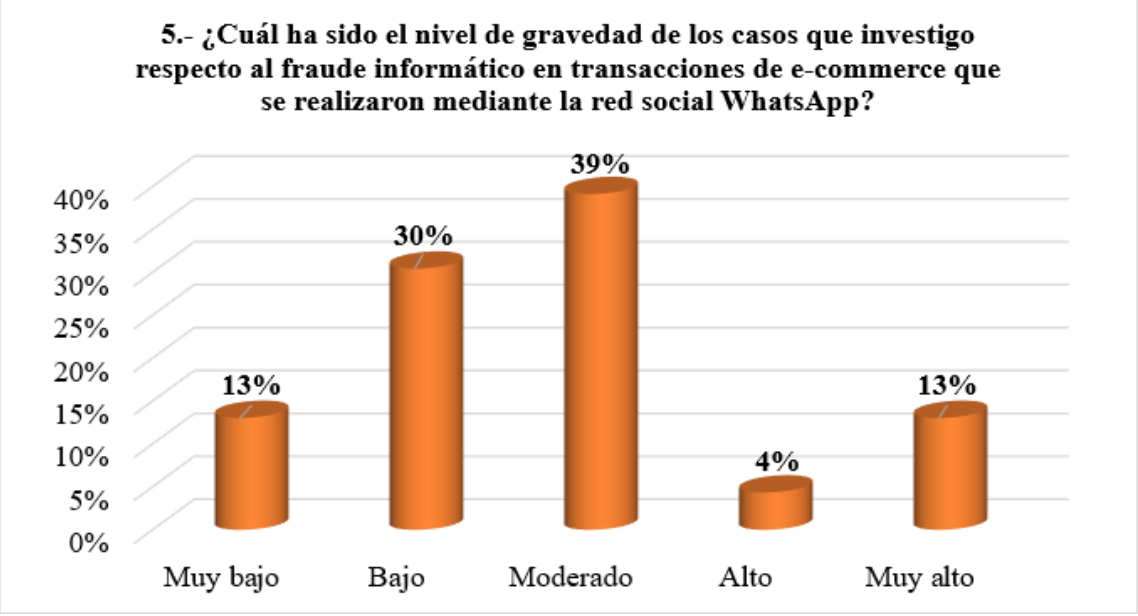
Nivel de gravedad - Fraude informático WhatsApp

5.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante la red social WhatsApp?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy bajo	3	13%	13%	13%
Bajo	7	30%	30%	43%
Moderado	9	39%	39%	83%
Alto	1	4%	4%	87%
Muy alto	3	13%	13%	100%
Total	23	100%	100%	

Figura 7

Nivel de gravedad - Fraude informático WhatsApp



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 5 del cuestionario 2: *¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante la red social WhatsApp?* El 13% respondió muy bajo, el 30% bajo, otro 39% respondió moderado, el 4% respondió alto y 13% respondió muy alto.

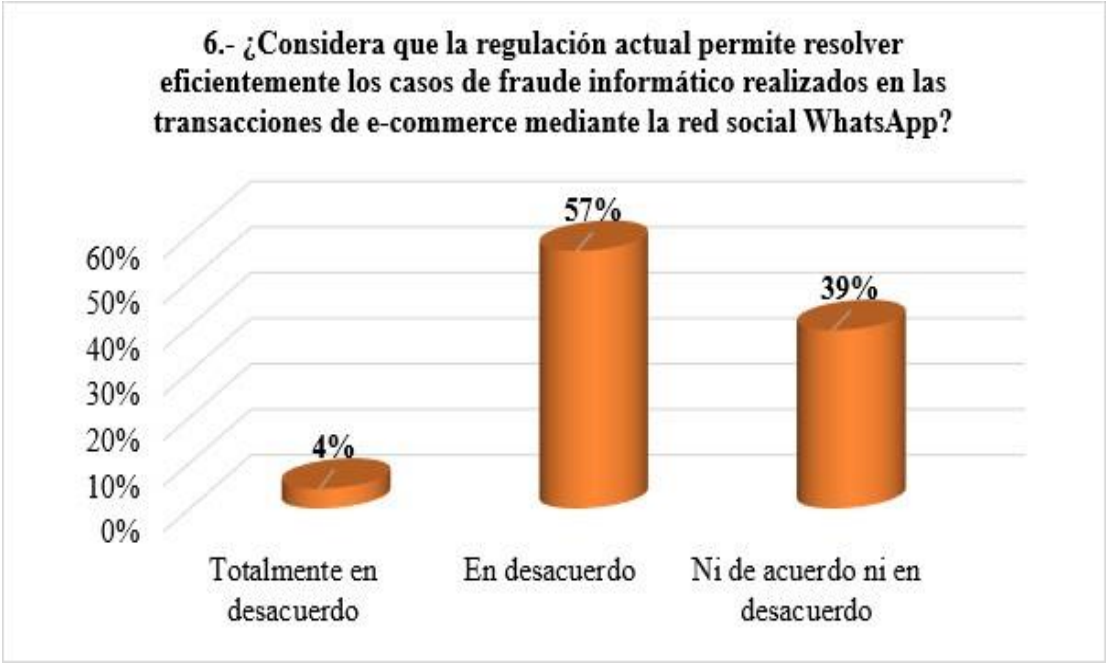
Tabla 10

Regulación contra Fraude informático en E-commerce en WhatsApp

6.- ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la red social WhatsApp?				
Frecuencia		**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Totalmente en desacuerdo	1	4%	4%	4%
En desacuerdo	13	57%	57%	61%
Ni de acuerdo ni en desacuerdo	9	39%	39%	100%
Total	23	100%	100%	

Figura 8

Regulación contra Fraude informático en E-commerce en WhatsApp



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 6 del cuestionario 2: *¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la red social WhatsApp?* El 4% respondió totalmente en desacuerdo, el 57% en desacuerdo, y 39% respondió ni de acuerdo ni en desacuerdo.

Tabla 11

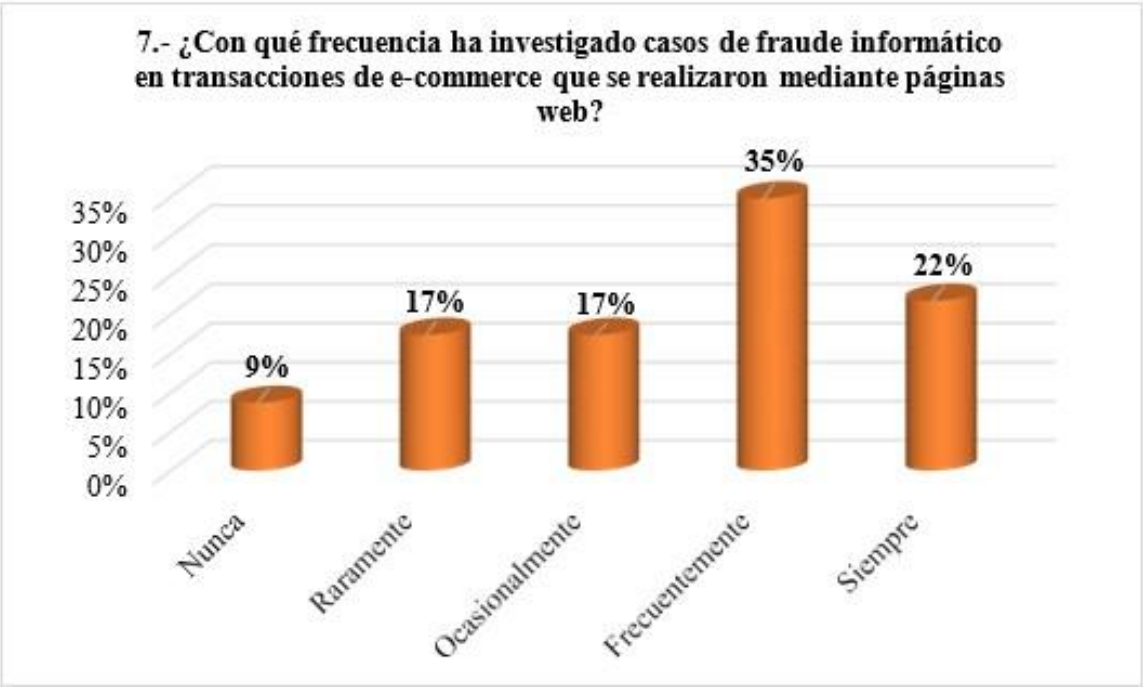
Fraude informático en transacciones de e-commerce en páginas web

7.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante páginas web?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nunca	2	9%	9%	9%
Raramente	4	17%	17%	26%
Ocasionalmente	4	17%	17%	43%
Frecuentemente	8	35%	35%	78%
Siempre	5	22%	22%	100%
Total	23	100%	100%	

Figura 9

Fraude informático en transacciones de e-commerce en páginas web



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 7 del cuestionario 2: *¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante páginas web?* El 9% respondió nunca, el 17% raramente, otro 17% respondió ocasionalmente, el 35% respondió frecuentemente y 22% respondió siempre.

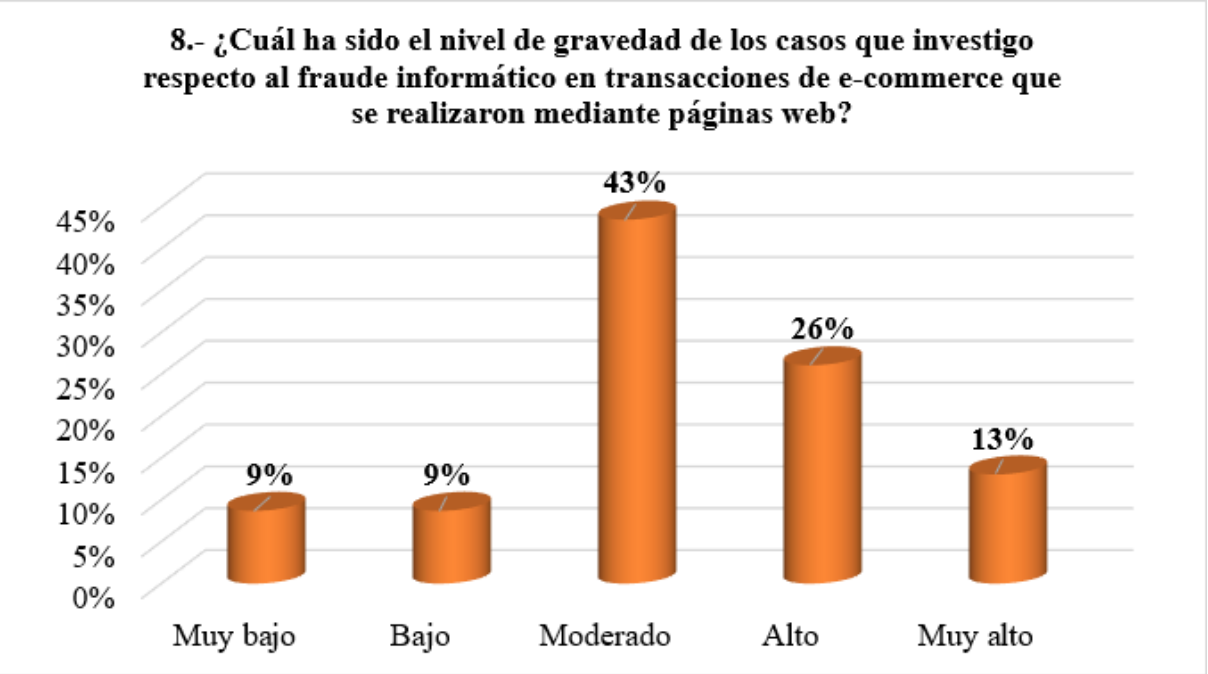
Tabla 12

Nivel de gravedad - Fraude informático en Páginas web

8.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante páginas web?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	2	9%	9%	9%
Bajo	2	9%	9%	17%
Moderado	10	43%	43%	61%
Alto	6	26%	26%	87%
Muy alto	3	13%	13%	100%
Total	23	100%	100%	

Figura 10

Nivel de gravedad - Fraude informático en Páginas web



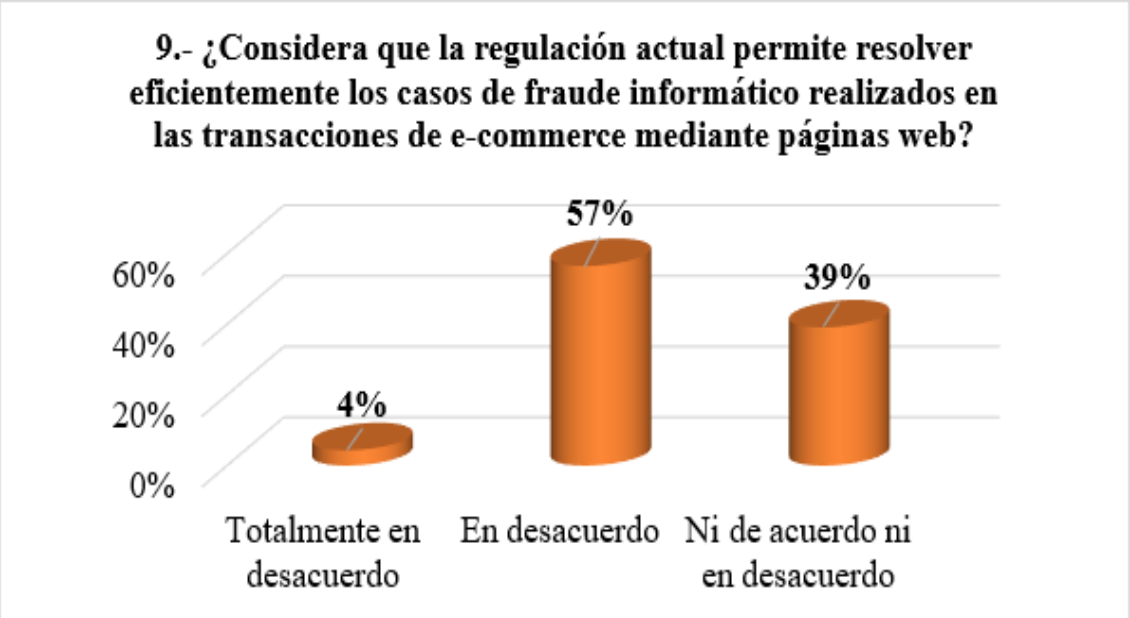
Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 8 del cuestionario 2: *¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante páginas web?* El 9% respondió muy bajo, el 9% bajo, otro 43% respondió moderado, el 26% respondió alto y 13% respondió muy alto.

Tabla 13
Regulación contra Fraude informático *en E-commerce en* Páginas web

9.- ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante páginas web?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Totalmente en desacuerdo	1	4%	4%	4%
En desacuerdo	13	57%	57%	61%
Ni de acuerdo ni en desacuerdo	9	39%	39%	100%
Total	23	100%	100%	

Figura 11
Regulación contra Fraude informático *en E-commerce en* Páginas web



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 9 del cuestionario 2: *¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante páginas web?* El 4% respondió totalmente en desacuerdo, el 57% en desacuerdo, y 39% respondió ni de acuerdo ni en desacuerdo.

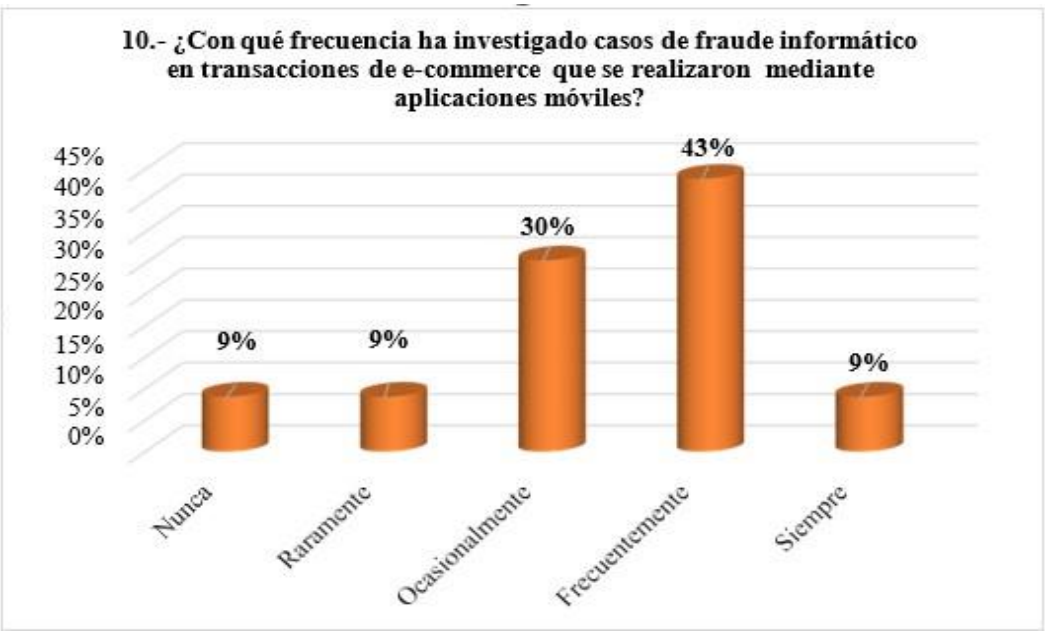
Tabla 14

Fraude informático en transacciones de e-commerce en aplicaciones móviles

10.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante aplicaciones móviles?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Nunca	2	9%	9%	9%
Raramente	2	9%	9%	17%
Ocasionalmente	7	30%	30%	48%
Frecuentemente	10	43%	43%	91%
Siempre	2	9%	9%	100%
Total	23	100%	100%	

Figura 12

Fraude informático en transacciones de e-commerce en aplicaciones móviles



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 10 del cuestionario 2: *¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante aplicaciones móviles?* El 9% respondió nunca, el 9% raramente, otro 30% respondió ocasionalmente, el 43% respondió frecuentemente y 9% respondió siempre.

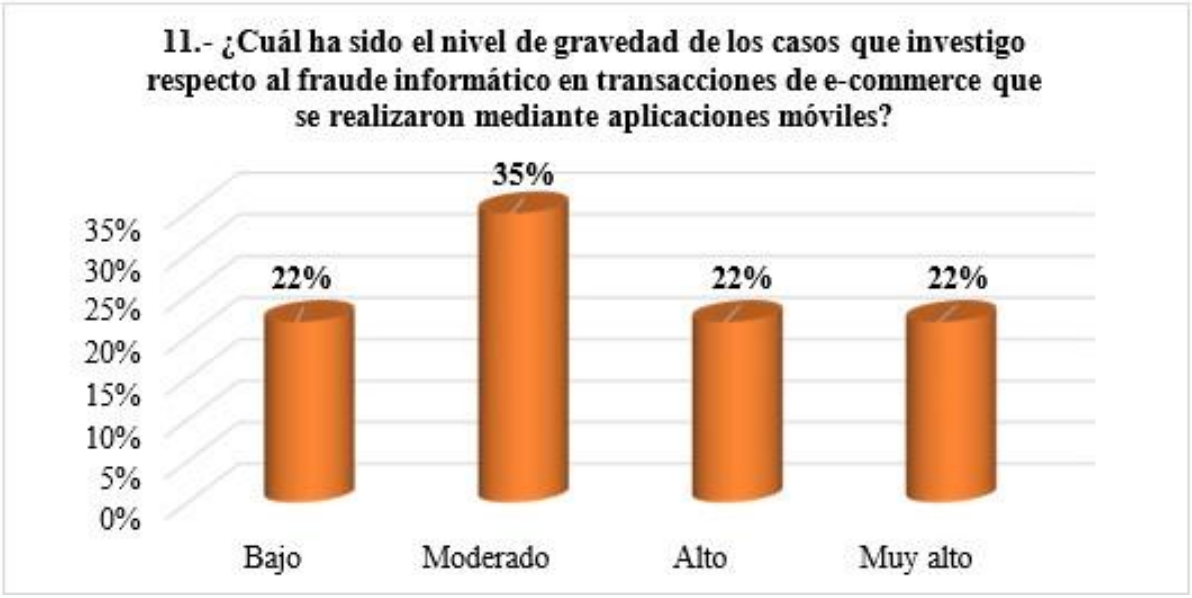
Tabla 15

Nivel de gravedad - Fraude informático en Aplicaciones móviles

11.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante aplicaciones móviles?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Bajo	5	22%	22%	22%
Moderado	8	35%	35%	57%
Alto	5	22%	22%	78%
Muy alto	5	22%	22%	100%
Total	23	100%	100%	

Figura 13

Nivel de gravedad - Fraude informático en Aplicaciones móviles



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 11 del cuestionario 2: *¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante aplicaciones móviles?* El 22% respondió bajo, el 35% moderado, otro 22% respondió alto y 22% respondió muy alto.

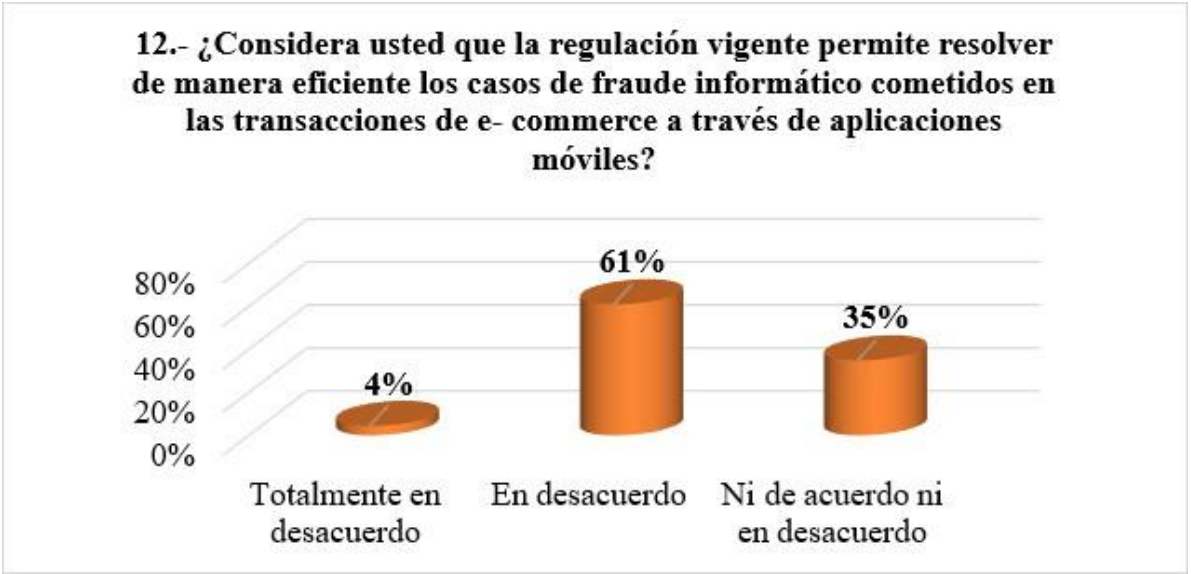
Tabla 16

Regulación contra Fraude informático en E-commerce en Aplicaciones móviles

12.- ¿Considera usted que la regulación vigente permite resolver de manera eficiente los casos de fraude informático cometidos en las transacciones de e- commerce a través de aplicaciones móviles?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Totalmente en desacuerdo	1	4%	4%	4%
En desacuerdo	14	61%	61%	65%
Ni de acuerdo ni en desacuerdo	8	35%	35%	100%
Total	23	100%	100%	

Figura 14

Regulación contra Fraude informático en E-commerce en Aplicaciones móviles



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 12 del cuestionario 2: *¿Considera usted que la regulación vigente permite resolver de manera eficiente los casos de fraude informático cometidos en las transacciones de e- commerce a través de aplicaciones móviles?* El 4% señaló totalmente en desacuerdo, el 61% en desacuerdo, otro 61% respondió en desacuerdo y 35% respondió ni de acuerdo ni en desacuerdo.

4.1.2. Prueba de Hipótesis

Con relación a la hipótesis general establecida en el estudio a continuación, se presenta la hipótesis alterna (H1) y la hipótesis nula (H0) respectivamente:

H1: El fraude informático tiene un impacto significativo en el e-commerce de Lima, 2023.

H0: El fraude informático no tiene un impacto significativo en el e-commerce de Lima, 2023. Los hallazgos obtenidos tras aplicar la prueba de Spearman se presentan a continuación.

Tabla 17

Correlaciones Rho de Spearman

			Variable X: Fraude Informático	Variable Y: E-Commerce
Rho de Spearman	Variable X: Fraude Informático	Coeficiente de correlación	1.000	,600**
		Sig. (bilateral)		0.002
		N	23	23
	Variable Y: E-Commerce	Coeficiente de correlación	,600**	1.000
		Sig. (bilateral)	0.002	
		N	23	23

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

Análisis:

Se tiene un coeficiente de correlación de 0,6, el cual, conforme con los estándares para el coeficiente de Spearman (ver Anexo N° 5), es estadísticamente significativo, sugiere una relación bastante buena. Además, en 0,002, el nivel de significancia es inferior al límite de 0,05. Como resultado, se confirma la hipótesis alterna. Como resultado, se concluye que el fraude informático tiene un impacto significativo en el e-commerce de Lima, 2023.

4.2. Resultados Relacionados con el Objetivo Especifico 1

En el estudio se formuló como objetivo específico 1 determinar cuál es el impacto de la clonación de tarjetas de crédito en el e-commerce de Lima, 2023. Los hallazgos obtenidos fueron los siguientes:

4.2.1. Análisis e Interpretación de Resultados

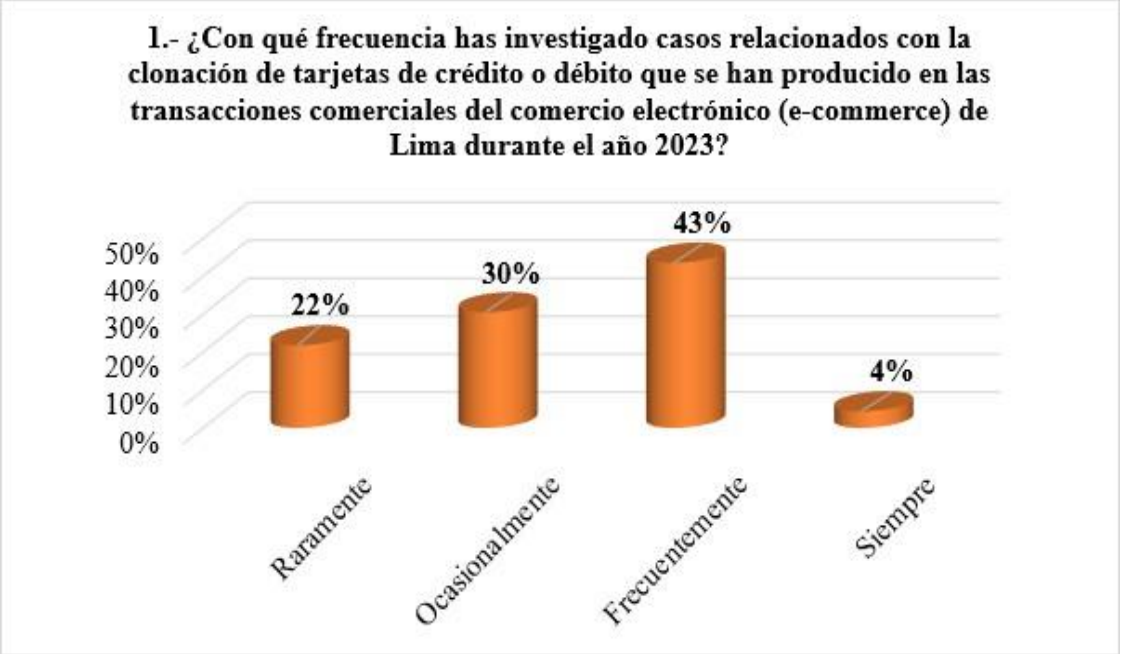
Tabla 18

Clonación de tarjetas de crédito o débito en E-commerce - Lima año 2023

1.- ¿Con qué frecuencia has investigado casos relacionados con la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Raramente	5	22%	22%	22%
Ocasionalmente	7	30%	30%	52%
Frecuentemente	10	43%	43%	96%
Siempre	1	4%	4%	100%
Total	23	100%	100%	

Figura 15

Clonación de tarjetas de crédito o débito en E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 1 del cuestionario 1: *¿Con qué frecuencia has investigado casos relacionados con la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 22% respondió raramente, otro 30% respondió ocasionalmente, el 43% respondió frecuentemente y 4% respondió siempre.

Tabla 19

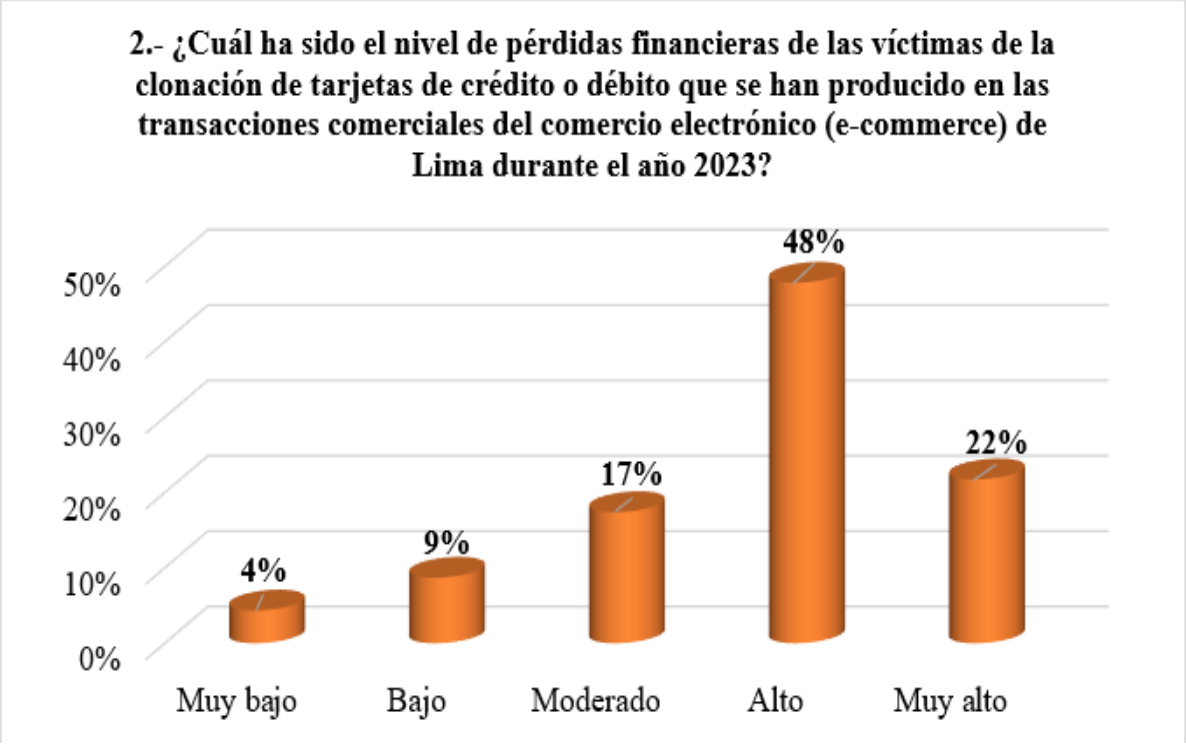
Pérdidas financieras por clonación de tarjetas en E-commerce - Lima año 2023

2.- ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	1	4%	4%	4%
Bajo	2	9%	9%	13%

Moderado	4	17%	17%	30%
Alto	11	48%	48%	78%
Muy alto	5	22%	22%	100%
Total	23	100%	100%	

Figura 16

Pérdidas financieras por clonación de tarjetas en E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 2 del cuestionario 1: *¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 4% respondió muy bajo, el 9% bajo, otro 17% respondió moderado, el 48% respondió alto y 22% respondió muy alto.

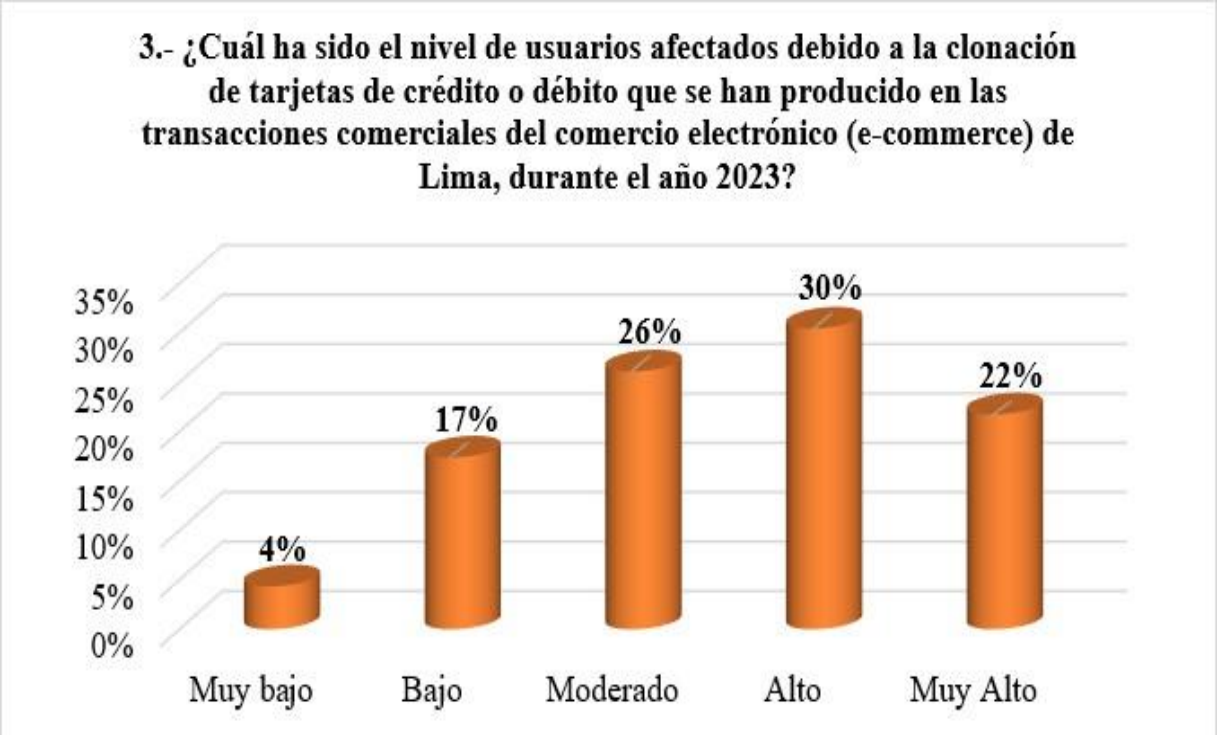
Tabla 20

Usuarios afectados por clonación de tarjetas en E-commerce – Lima año 2023

3.- ¿Cuál ha sido el nivel de usuarios afectados debido a la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	1	4%	4%	4%
Bajo	4	17%	17%	22%
Moderado	6	26%	26%	48%
Alto	7	30%	30%	78%
Muy Alto	5	22%	22%	100%
Total	23	100%	100%	

Figura 17

Usuarios afectados por clonación de tarjetas en E-commerce – Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 3 del cuestionario 1: *¿Cuál ha sido el nivel de usuarios afectados debido a la clonación de tarjetas de crédito o débito que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?* El 4% respondió muy bajo, el 17% bajo, otro 26% respondió moderado, el 30% respondió alto y 22% respondió muy alto.

4.2.2. Prueba de Hipótesis

Con relación a la hipótesis especifica 1 establecida en el estudio a continuación, se presenta la hipótesis alterna (H1) y la hipótesis nula (H0):

H1: La clonación de tarjetas de crédito tiene un impacto significativo en el e-commerce de Lima, 2023.

H0: La clonación de tarjetas de crédito no tiene un impacto significativo en el e-commerce de Lima, 2023.

Luego se presentan los hallazgos luego de usar el Rho de Spearman.

Tabla 21

Correlaciones Rho de Spearman

			Dimensión 1: Clonación de tarjetas de crédito o débito	Variable Y: E-Commerce
Rho de Spearman	Dimensión 1: Clonación de tarjetas de crédito o débito	Coeficiente de correlación	1.000	0.287
		Sig. (bilateral)		0.185
		N	23	23
	Variable Y: E-Commerce	Coeficiente de correlación	0.287	1.000
		Sig. (bilateral)	0.185	
		N	23	23

Análisis:

El valor de correlación observado muestra una correlación positiva de 0,287, lo que concuerda con los criterios del coeficiente de Spearman (ver Anexo No. 5). Además, en 0,185, el nivel de significancia es superior al límite de 0,05. Por lo tanto, se rechaza la hipótesis alterna y se reconoce la hipótesis nula como la explicación correcta. La conclusión que se puede sacar de esto es que, la clonación de tarjetas de crédito no tiene un impacto significativo en el e-commerce de Lima, 2023.

4.3. Resultados Relacionados con el Objetivo Especifico 2

Para efectos de esta investigación se desarrolló el objetivo específico 2 para conocer la influencia que tienen las técnicas de phishing en el comercio en línea en Lima en el año 2023. Los ítems que se enumeran a continuación son los resultados que se lograron.

4.3.1. Análisis e Interpretación de Resultados

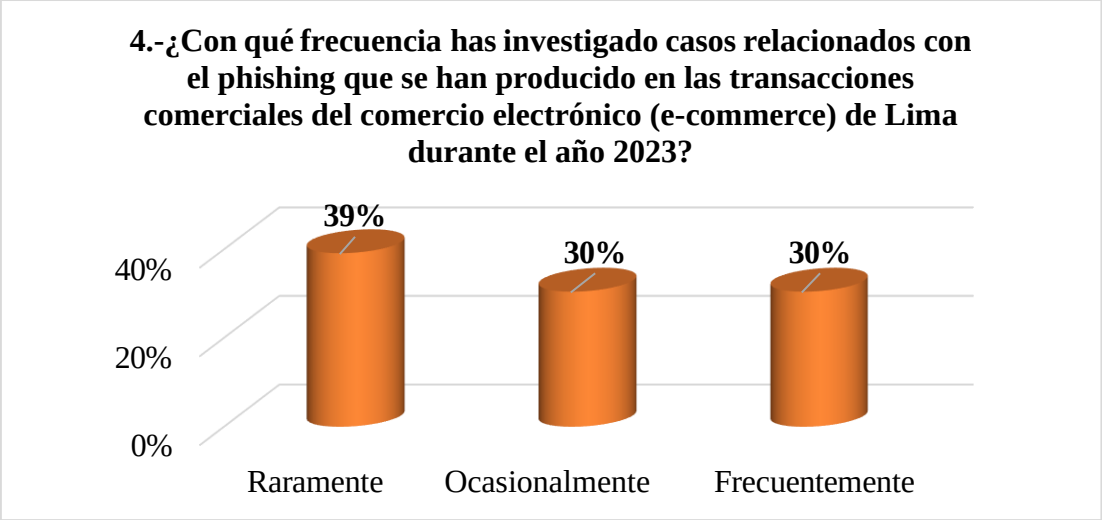
Tabla 22

Casos de phishing en transacciones comerciales del E-commerce - Lima año 2023

4.-¿Con qué frecuencia has investigado casos relacionados con el phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Raramente	9	39%	39%	39%
Ocasionalmente	7	30%	30%	70%
Frecuentemente	7	30%	30%	100%
Total	23	100%	100%	

Figura 18

Casos de phishing en transacciones comerciales del E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 4 del cuestionario 1: *¿Con qué frecuencia has investigado casos relacionados con el phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 39% respondió raramente, el 30% ocasionalmente y otro 30% respondió frecuentemente.

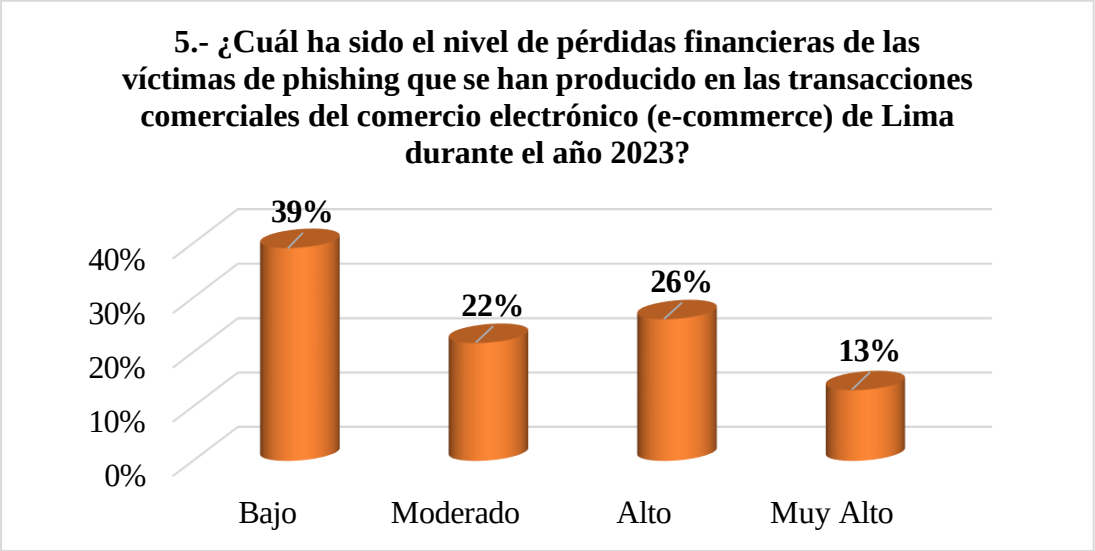
Tabla 23

Pérdidas financieras por phishing en el E-commerce - Lima año 2023

5.- ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Bajo	9	39%	39%	39%
Moderado	5	22%	22%	61%
Alto	6	26%	26%	87%
Muy Alto	3	13%	13%	100%
Total	23	100%	100%	

Figura 19

Pérdidas financieras por phishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 5 del cuestionario 1: *¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 39% respondió bajo, el 22% moderado, otro 26% respondió alto y 13% respondió muy alto.

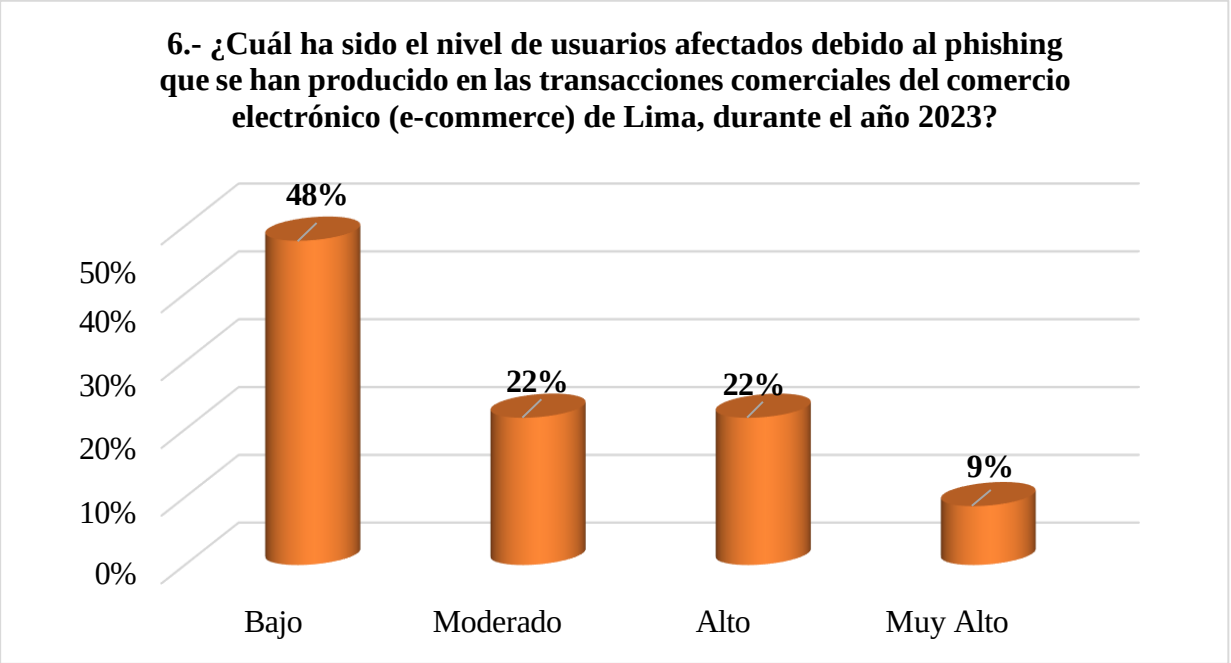
Tabla 24

Usuarios afectados por phishing en el E-commerce - Lima año 2023

6.- ¿Cuál ha sido el nivel de usuarios afectados debido al phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Bajo	11	48%	48%	48%
Moderado	5	22%	22%	70%
Alto	5	22%	22%	91%
Muy Alto	2	9%	9%	100%
Total	23	100%	100%	

Figura 20

Usuarios afectados por phishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 6 del cuestionario 1: *¿Cuál ha sido el nivel de usuarios afectados debido al phishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?* El 48% respondió bajo, el 22% moderado, otro 22% respondió alto y 9% respondió muy alto.

4.3.2. Prueba de Hipótesis

Con relación a la hipótesis especifica 2 establecida en el estudio a continuación, se presenta la hipótesis alterna (H1) y la hipótesis nula (H0) respectivamente:

H1: El phishing tiene un impacto significativo en el e-commerce de Lima, 2023.

H0: El phishing no tiene un impacto significativo en el e-commerce de Lima, 2023.

Los hallazgos obtenidos tras aplicar la prueba de Spearman se presentan a continuación.

Correlaciones Rho de Spearman

			Dimensión 2: Phishing	Variable Y: E-Commerce
Rho de Spearman	Dimensión 2: Phishing	Coeficiente de correlación	1.000	,446*
		Sig. (bilateral)		0.033
		N	23	23
	Variable Y: E-Commerce	Coeficiente de correlación	,446*	1.000
		Sig. (bilateral)	0.033	
		N	23	23

*. La correlación es significativa para el nivel 0,05 (bilateral).

Análisis:

Existe una relación algo positiva entre ambas variables, como lo demuestra el coeficiente de Spearman (ver Anexo No. 5), que arroja un valor de correlación de 0.446. No sólo eso, sino que el nivel de significancia es inferior al requisito de 0,05, llegando a 0,033. Por lo tanto, es aceptada la hipótesis alterna y se descarta la hipótesis nula, concluyendo que el pishing tiene impacto significativo en el E-commerce de Lima, 2023.

4.4. Resultados Relacionados con el Objetivo Especifico 3

El tercer objetivo del estudio es determinar cuál es el impacto del Vishing en el E-commerce de Lima, 2023. Produciéndose los siguientes hallazgos:

4.4.1. Análisis e Interpretación de Resultados

Tabla 25

Casos de vishing en transacciones comerciales del E-commerce - Lima año 2023

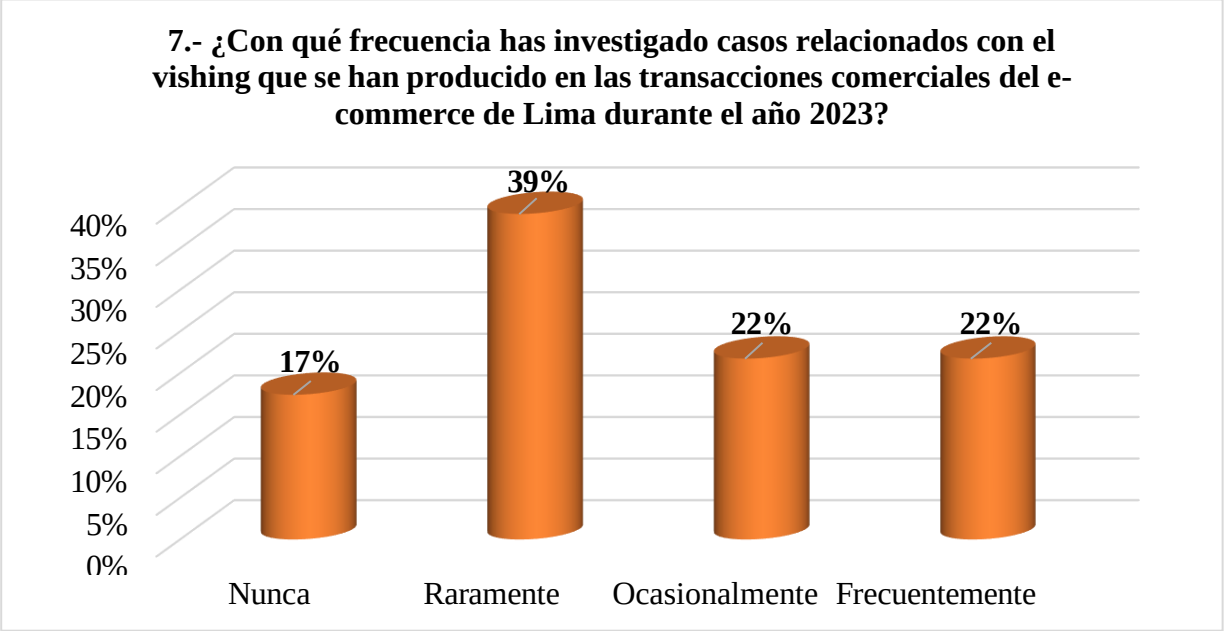
7.- ¿Con qué frecuencia has investigado casos relacionados con el vishing que se han producido en las transacciones comerciales del e-commerce de Lima durante el año 2023?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nunca	4	17%	17%	17%
Raramente	9	39%	39%	57%

Ocasionalmente	5	22%	22%	78%
Frecuentemente	5	22%	22%	100%
Total	23	100%	100%	

Figura 21

Casos de vishing en transacciones comerciales del E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 7 del cuestionario 1: *¿Con qué frecuencia has investigado casos relacionados con el vishing que se han producido en las transacciones comerciales del e-commerce de Lima durante el año 2023?* El 17% respondió nunca, el 39% raramente, otro 22% respondió ocasionalmente y 22% respondió frecuentemente.

Tabla 26

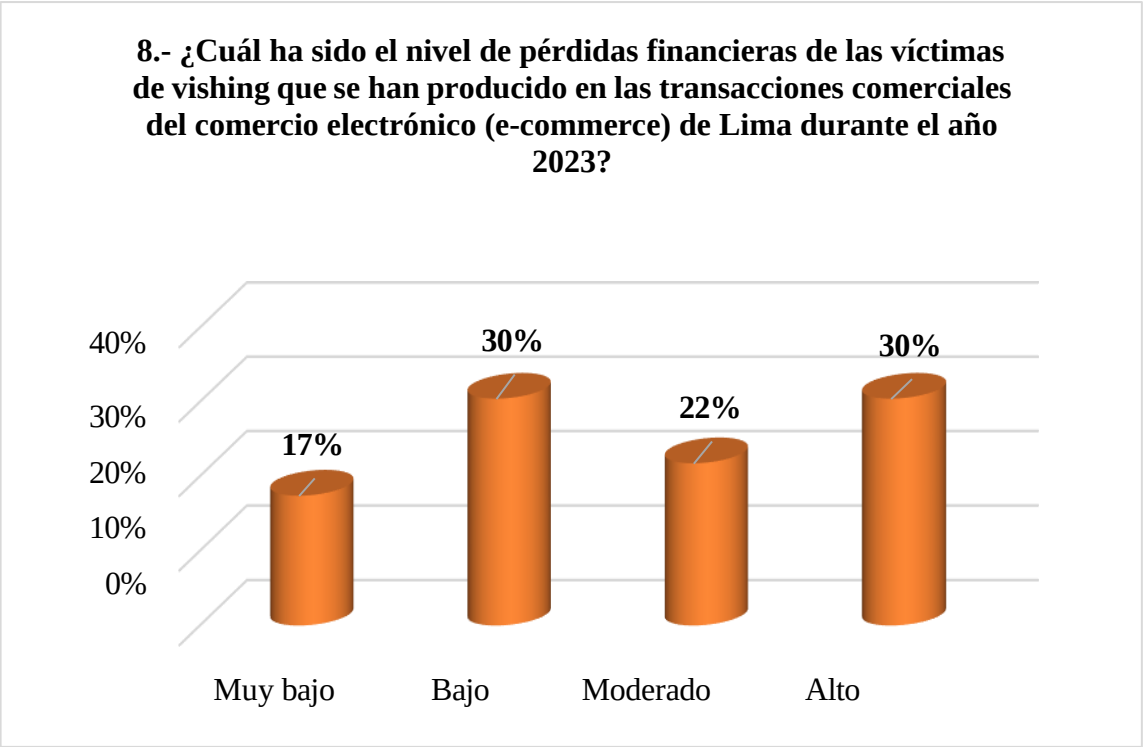
Pérdidas financieras por vishing en el E-commerce - Lima año 2023

8.- ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de vishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	4	17%	17%	17%

Bajo	7	30%	30%	48%
Moderado	5	22%	22%	70%
Alto	7	30%	30%	100%
Total	23	100%	100%	

Figura 22

Pérdidas financieras por vishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 8 del cuestionario 1: *¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de vishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 17% respondió muy bajo, el 30% bajo, otro 22% respondió moderado y 30% respondió alto.

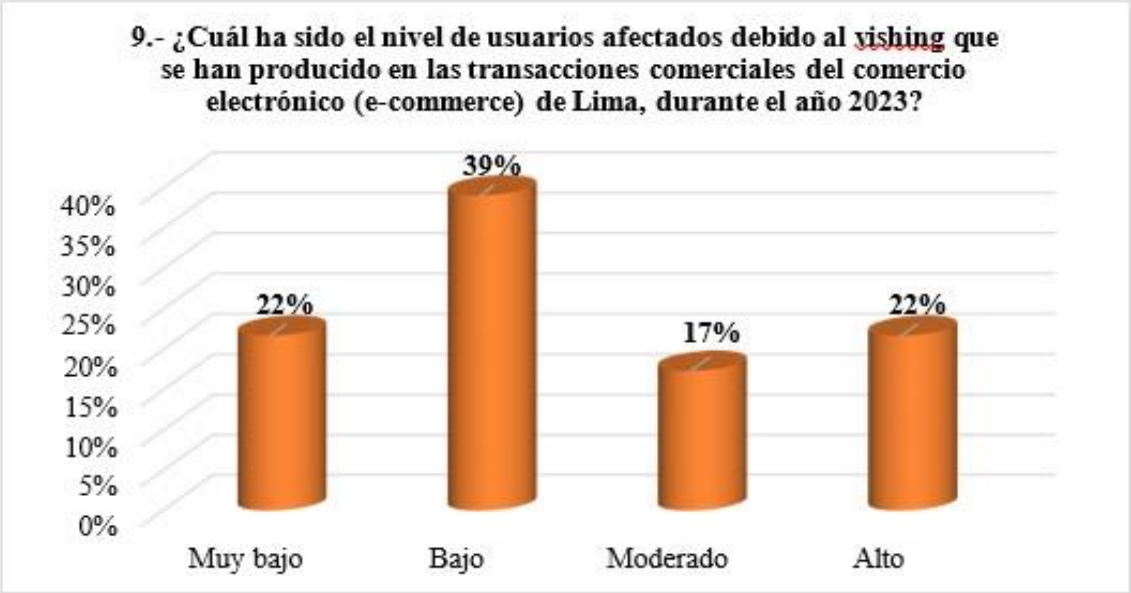
Tabla 27

Usuarios afectados por vishing en el E-commerce - Lima año 2023

9.- ¿Cuál ha sido el nivel de usuarios afectados debido al vishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	5	22%	22%	22%
Bajo	9	39%	39%	61%
Moderado	4	17%	17%	78%
Alto	5	22%	22%	100%
Total	23	100%	100%	

Figura 23

Usuarios afectados por vishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 9 del cuestionario 1: *¿Cuál ha sido el nivel de usuarios afectados debido al vishing que se han producido en las*

transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023? El 22% respondió muy bajo el 39% bajo, otro 17% respondió moderado, y 22% respondió alto.

4.4.2. Prueba de Hipótesis

Con relación a la hipótesis especifica 3 establecida en el estudio a continuación, se presenta la hipótesis alterna (H1) y la hipótesis nula (H0) respectivamente:

H1: El vishing tiene un impacto significativo en el e-commerce de Lima, 2023.

H0: El vishing no tiene un impacto significativo en el e-commerce de Lima, 2023.

Los hallazgos obtenidos tras aplicar la prueba de Spearman se presentan a continuación.

Correlaciones Rho de Spearman

			Dimensión 3: Vishing	Variable Y: E-Commerce
Rho de Spearman	Dimensión 3: Vishing	Coeficiente de correlación	1.000	0.310
		Sig. (bilateral)		0.150
		N	23	23
	Variable Y: E-Commerce	Coeficiente de correlación	0.310	1.000
		Sig. (bilateral)	0.150	
		N	23	23

Análisis:

El valor de correlación observado de 0,310 muestra una correlación positiva leve, de acuerdo con las condiciones para el coeficiente de Spearman (ver Anexo No. 5). Asimismo, el valor p es 0,150, es estadísticamente significativo a un nivel superior a 0,05. Debido a esto, podemos concluir que la hipótesis nula es correcta y rechazar la alternativa. De ello se deduce que el vishing no tiene un impacto significativo en el E-commerce de Lima, 2023.

4.5. Resultados Relacionados con el Objetivo Especifico 4

En el estudio se formuló como objetivo específico 4 determinar cuál es el impacto del

smishing en el e-commerce de Lima, 2023. Los hallazgos obtenidos fueron los siguientes:

4.5.1. Análisis e Interpretación de Resultados

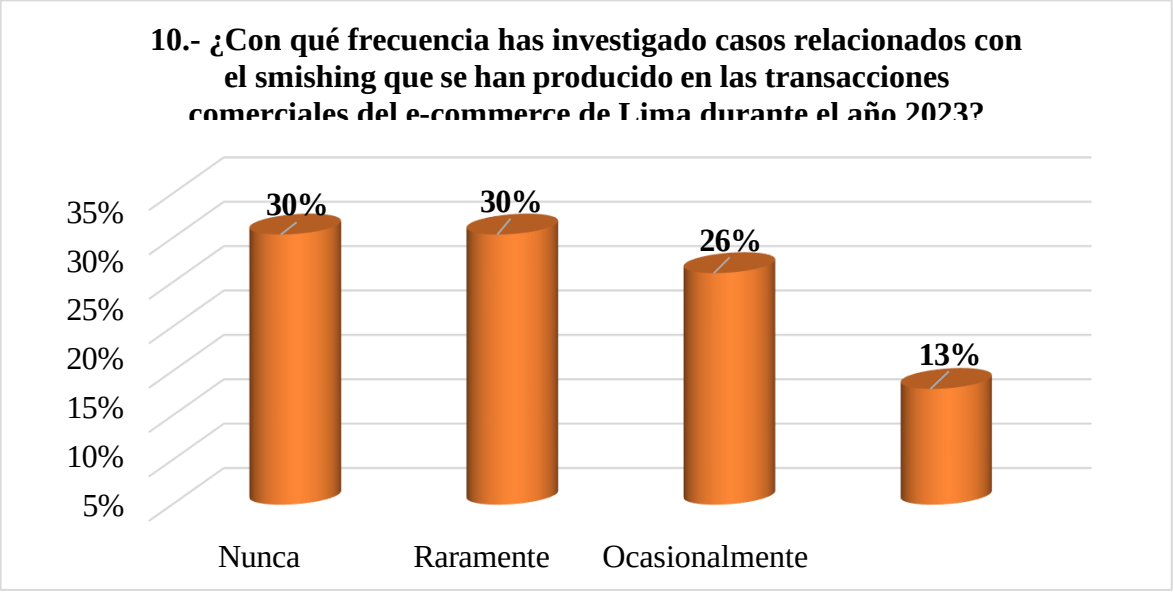
Tabla 28

Casos de smishing en transacciones comerciales del E-commerce - Lima año 2023

10.- ¿Con qué frecuencia has investigado casos relacionados con el smishing que se han producido en las transacciones comerciales del e-commerce de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Nunca	7	30%	30%	30%
Raramente	7	30%	30%	61%
Ocasionalmente	6	26%	26%	87%
Frecuentemente	3	13%	13%	100%
Total	23	100%	100%	

Figura 24

Casos de smishing en transacciones comerciales del E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 10 del cuestionario 1: *¿Con qué frecuencia has investigado casos relacionados con el smishing que se han producido*

en las transacciones comerciales del e-commerce de Lima durante el año 2023? El 30% respondió nunca, el 30% raramente, otro 26% respondió ocasionalmente y el 13% respondió frecuentemente.

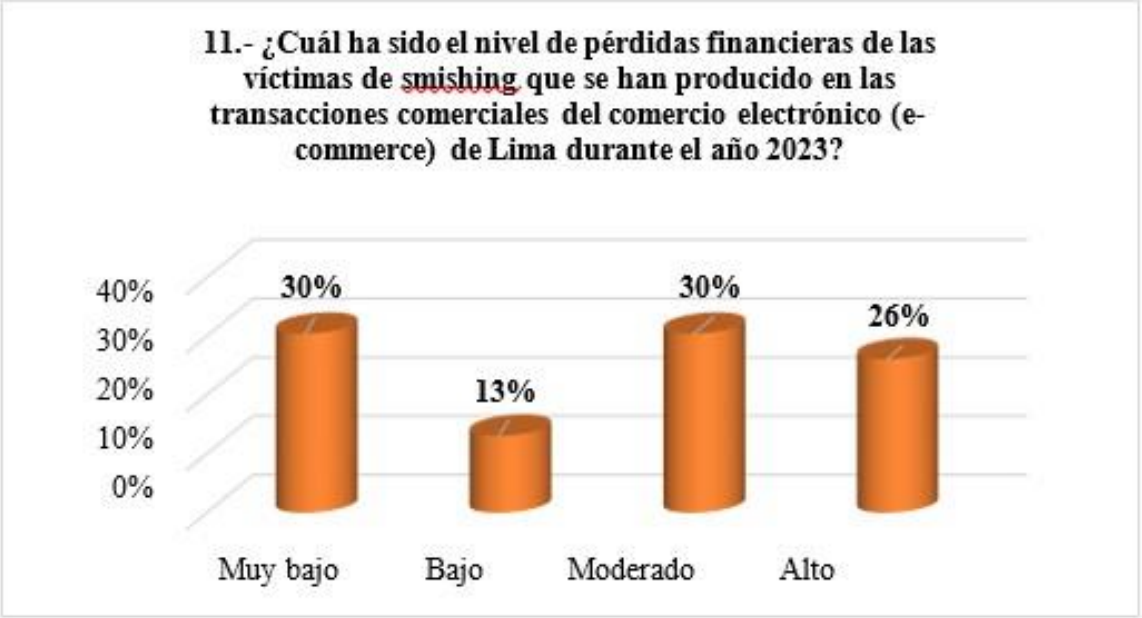
Tabla 29

Pérdidas financieras por smishing en el E-commerce - Lima año 2023

11.- ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de smishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Muy bajo	7	30%	30%	30%
Bajo	3	13%	13%	43%
Moderado	7	30%	30%	74%
Alto	6	26%	26%	100%
Total	23	100%	100%	

Figura 25

Pérdidas financieras por smishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 11 del cuestionario

1: *¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de smishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?* El 30% respondió muy bajo, el 13% bajo, otro 30% respondió moderado y 26% respondió alto.

Tabla 30

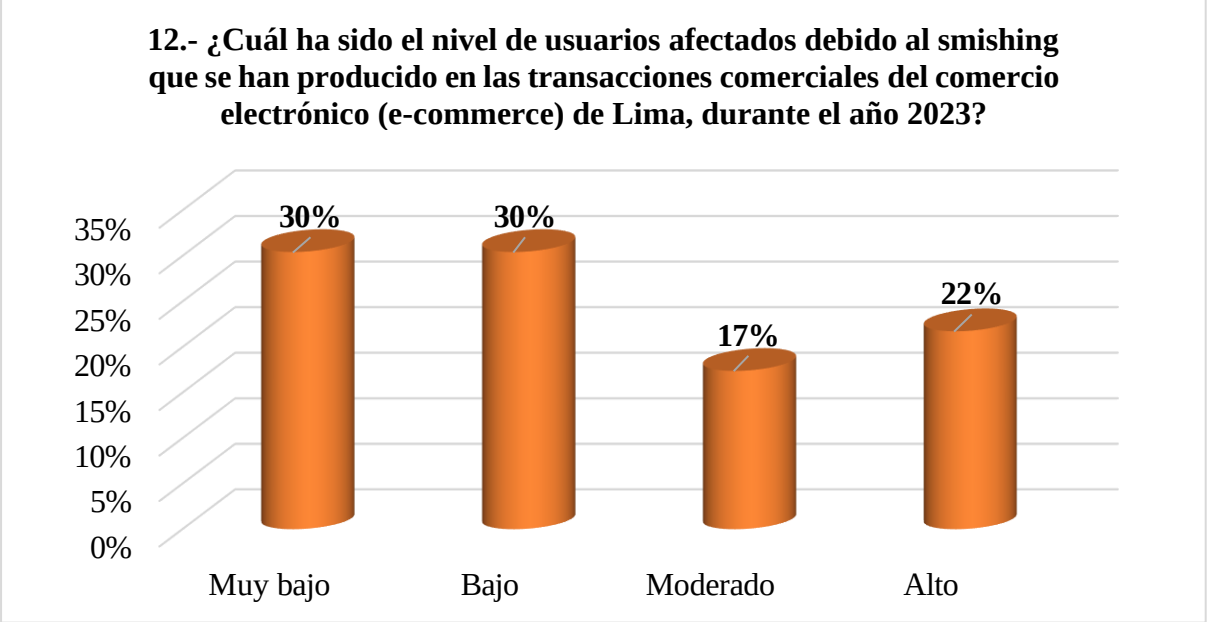
Usuarios afectados por smishing en el E-commerce - Lima año 2023

12.- ¿Cuál ha sido el nivel de usuarios afectados debido al smishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy bajo	7	30%	30%	30%
Bajo	7	30%	30%	61%
Moderado	4	17%	17%	78%
Alto	5	22%	22%	100%
Total	23	100%	100%	

Figura 26

Usuarios afectados por smishing en el E-commerce - Lima año 2023



Análisis:

En base a los datos recolectados, se aprecia que respecto a la pregunta 12 del cuestionario

1: *¿Cuál ha sido el nivel de usuarios afectados debido al smishing que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?* El 30% respondió muy bajo, el 30% bajo, otro 17% respondió moderado y 22% respondió alto.

4.5.2. Prueba de Hipótesis

Con relación a la hipótesis especifica 4 establecida en el estudio a continuación, se presenta la hipótesis alterna (H1) y la hipótesis nula (H0) respectivamente:

H1: El Smishing tiene un impacto significativo en el e-commerce de Lima, 2023.

H0: El Smishing no tiene un impacto significativo en el e-commerce de Lima, 2023.

Los hallazgos obtenidos tras aplicar la prueba de Spearman se presentan a continuación:

Tabla 31

Correlaciones Rho de Spearman

			Dimensión 4: Smishing	Variable Y: E-Commerce
Rho de Spearman	Dimensión 4: Smishing	Coeficiente de correlación	1.000	,449*
		Sig. (bilateral)		0.032
		N	23	23
	Variable Y: E-Commerce	Coeficiente de correlación	,449*	1.000
		Sig. (bilateral)	0.032	
		N	23	23

*. La correlación es significativa para el nivel 0,05 (bilateral).

Análisis:

Un coeficiente de Spearman de 0.449 señala una relación moderadamente favorable, según los criterios establecidos en el Anexo No. 5. También está presente un nivel de significancia inferior al límite de 0,05 (0,032). Una vez aclarado esto, podemos aceptar la hipótesis alterna y rechazar la nula. Por lo tanto, se concluye que el smishing tiene un impacto significativo en el E-commerce de Lima, 2023.

V. DISCUSIÓN DE RESULTADOS

5.1. Discusión de los Resultados Relacionados con el Objetivo General

Se halló un coeficiente de correlación de 0,6 con respecto a los hallazgos de la prueba de hipótesis general; esto corresponde, según los estándares del coeficiente de Spearman (ver Anexo N° 5), denota una correlación positiva moderada. Además, el nivel de significancia fue inferior a 0,05, llegando a 0,002. El hallazgo permitió aceptar la hipótesis alterna. Por lo tanto, se concluye que el fraude informático tiene un impacto significativo en el E-commerce de Lima, 2023.

Estos resultados son similares a los conseguidos por **Tuesta** (2022), cuyos resultados mostraron que, el fraude informático impacta significativamente en los derechos, principios y garantías fundamentales de las personas en el Cercado de Lima.

5.2. Discusión de los Resultados Relacionados con el Objetivo Especifico 1

De acuerdo con el criterio del coeficiente de Spearman (ver Anexo No. 5), esta prueba de hipótesis específica arrojó resultados con una correlación positiva baja de 0,287. Asimismo, el grado de significancia supera el límite de 0,05 con un valor de 0,185. Debido a esto, se puede concluir que la hipótesis nula es correcta y rechazar la alternativa. De ello se concluye que la clonación de tarjetas de crédito no tiene un impacto significativo en el E-commerce, 2023.

Estos hallazgos son contrarios a los conseguidos por **Mayuri, Shingavi, Palarpawar & Nikam** (2023) cuyos resultados revelaron que la aplicación de escáner de tarjetas de crédito impacta en la reducción del fraude con tarjetas de crédito mediante el reconocimiento facial, proporcionando un proceso comercial electrónico más conveniente y eficiente.

5.2. Discusión de los Resultados Relacionados con el Objetivo Especifico 2

Con relación a los hallazgos de la hipótesis especifica 2 se encontró un coeficiente de correlación de 0.446, lo que, de acuerdo con las recomendaciones para el coeficiente de Spearman (ver Anexo No. 5), denota una correlación positiva moderada. El nivel de

significancia es inferior al umbral crucial de 0,05, llegando a 0,033. En consecuencia, el resultado permitió aceptar la hipótesis alterna y descartar la hipótesis nula. Por lo tanto, se concluye que el phishing tiene un impacto significativo en el E-commerce de Lima en el año 2023.

Estos hallazgos son similares a los hallados por **Linares** (2022) quien concluyó en su investigación que el phishing afectó el derecho del goce del bien durante la pandemia en el distrito fiscal de Lima Este, al ser la primera etapa en la afectación del patrimonio, a través de transferencias electrónicas fraudulentas. Asimismo, estos resultados son similares a los obtenidos por **Amira Binti, Razak, Firdau, Ernawan, & Akmar Zulkifli** (2023) quienes en su investigación demostraron que los ataques de phishing pueden provocar pérdidas financieras, uso fraudulento de tarjetas de crédito, filtraciones de datos y una falta general de confianza en las compras en línea entre las víctimas.

5.2. Discusión de los Resultados Relacionados con el Objetivo Especifico 3

De acuerdo a las recomendaciones del coeficiente de Spearman (ver Anexo No. 5), se logró un coeficiente de correlación de 0.310 respecto a los datos hallados en la prueba de la hipótesis particular 3, lo cual denota una correlación positiva baja. Además, el nivel de significancia es de 0,150, siendo superior al límite de 0,05. Entonces, se opta por la hipótesis nula y se descarta la alternativa. Concluyéndose que el vishing no tiene un impacto significativo en el E-commerce de Lima 2023.

Estos resultados son similares a los hallados por **Kuzmin** (2022) quien realizó un estudio cuyos hallazgos revelaron que el vishing se puede prevenir mediante el uso de servicios de búsqueda electrónica, servicios especiales y estrategias de protección de las víctimas, como la autodefensa psicológica y la vigilancia. Asimismo, estos hallazgos son similares a los obtenidos por **Cajigas & Pérez** (2023) quienes, según sus conclusiones, 561 denuncias estuvieron relacionadas con otras modalidades de fraude informático en el año 2022, y solo

181 denuncias estuvieron relacionadas con el vishing.

5.2. Discusión de los Resultados Relacionados con el Objetivo Especifico 4

Se halló un coeficiente de correlación de 0,449 en relación con los hallazgos de la prueba de hipótesis particular 4. Esto, de acuerdo con los criterios del coeficiente de Spearman (ver Anexo N° 5), denota una correlación positiva moderada. Además, a 0,032 (o menos que el nivel de significancia de 0,05), los resultados no se consideran significativos. Como consecuencia de esto, se descartó la hipótesis nula y se aceptó la hipótesis alterna, concluyéndose que el smishing tiene un impacto significativo en el E-commerce de Lima, 2023.

Estos resultados son similares a los hallados por **Rahman, Timko, Wali, & Neupane** (2022) quienes realizaron un estudio que revelaron que los ataques de smishing son efectivos, toda vez que el 16,92 % de los participantes pueden caer en ellos, y una combinación de acciones de respuesta y clic aumenta las probabilidades de que un usuario responda a un mensaje de smishing. Asimismo, estos resultados son similares a los obtenidos por **Ventura** (2021) cuyos hallazgos resaltaron la importancia de las sanciones smishing, ya que los delitos cibernéticos ocupan un papel importante en la sociedad moderna; como consecuencia, deben existir mecanismos legales para proteger a los usuarios durante las transacciones en línea.

VI. CONCLUSIONES

6.1 Se concluye que en el año 2023 el fraude informático tuvo un impacto significativo en el E-commerce de Lima. Este hallazgo está respaldado por un nivel de significancia de 0,002, que es inferior al criterio comúnmente aceptado de 0,05. El hallazgo permitió aceptar la hipótesis alterna. Además, según el criterio del coeficiente de Spearman se encontró un valor de correlación de 0.6, lo que denota una correlación positiva moderada entre el fraude informático y el E-commerce de Lima, 2023 (ver Anexo E).

6.2 Se concluye que las compras online en Lima no se vieron afectados por la clonación de tarjetas de crédito en el año 2023. Con un nivel de significancia de 0.185, que es mayor al corte de 0.05, se puede sacar esta conclusión. Por lo cual, es aceptada la hipótesis nula. Se detectó un valor de correlación de 0,287, lo que indica que existe una correlación positiva baja entre ambas variables. Esto se determinó utilizando los lineamientos para el coeficiente de Spearman, que se encuentran en el Anexo E.

6.3 Según los hallazgos, el phishing tuvo un impacto significativo en el E-commerce de Lima en el año 2023. Este resultado se obtiene sobre la base de un nivel de significancia de 0,033, que es menor al criterio generalmente aceptado de 0,05. En consecuencia, se aceptó la hipótesis alterna y se descaró la hipótesis nula, mientras que se demostró que la hipótesis nula era incorrecta. También hubo una correlación positiva moderada, al obtenerse como coeficiente de correlación de 0,446, que concuerda con los estándares para el coeficiente de Spearman (ver Anexo E).

6.4 Se ha determinado que el fenómeno vishing no tuvo un impacto significativo en el E- commerce de Lima en el año 2023. Esta conclusión se basa en un nivel de significancia de 0.150, el cual es superior al umbral típico de 0.05 empleado. Por lo cual, es aceptada la hipótesis

nula. Además, se obtuvo un valor de correlación de 0.310, lo que indica una correlación positiva baja entre ambas variables, tal como lo señalan los lineamientos para el coeficiente de Spearman (ver Anexo E).

6.5 Se ha determinado que el smishing tuvo un impacto significativo en el E-commerce en Lima en el año 2023. Utilizando un nivel de significancia de 0,032, que es inferior a 0,05, permite llegar a la conclusión. El hallazgo permitió aceptar la hipótesis alterna. Además, se observó un valor de correlación de 0,449, que es consistente con los criterios para el coeficiente de Spearman (ver Anexo E), lo que indica una correlación positiva moderada.

VII. RECOMENDACIONES

7.1 Se recomienda mejorar la regulación existente respecto a fraude informático dado que más del 50% de los participantes expresaron su desacuerdo con la eficacia de la regulación actual para resolver casos de fraude informático en transacciones de e-commerce mediante aplicaciones móviles y páginas web, se sugiere investigar las deficiencias percibidas en estas áreas y proponer medidas de mejora en la regulación, así como aplicación de la ley. Además, considerando que una proporción considerable de encuestados investiga casos de fraude informático en transacciones de e-commerce a través de redes sociales, como Facebook, con frecuencia u ocasionalmente, es imperativo profundizar en el análisis del impacto del fraude informático en estas plataformas específicas y desarrollar estrategias de prevención y regulación adaptadas a sus características únicas. Estas recomendaciones se fundamentan en los resultados que reflejan las mayores preocupaciones y áreas de interés de los encuestados, con el objetivo de abordar eficazmente los desafíos relacionados con el fraude informático en el e-commerce de Lima en el año 2023.

7.2 Se recomienda dirigir futuras investigaciones hacia el análisis detallado del impacto de la clonación de tarjetas de crédito en el e-commerce de Lima en el año 2023, dado que el 43% de los encuestados informó investigar estos casos frecuentemente y otro 30% ocasionalmente. Estos porcentajes destacan la prevalencia del problema y la necesidad de comprender mejor sus implicaciones. Además, considerando que el 48% de las víctimas experimentaron pérdidas financieras clasificadas como altas y un 22% muy altas, es imperativo investigar las medidas de seguridad y prevención para mitigar estos impactos. Asimismo, el 30% de usuarios afectados de manera moderada y un 22% muy alta subrayan la urgencia de abordar los efectos adversos de la clonación de tarjetas en la confianza y la seguridad del e-commerce en Lima. Estos hallazgos respaldan la

importancia de investigar a fondo este tema para fortalecer la protección de los consumidores y la integridad del mercado electrónico en la región.

7.3 Se recomienda dirigir futuras investigaciones hacia el análisis detallado del fenómeno del phishing en el e-commerce de Lima durante el año 2023, dado que el 39% de los encuestados informó investigar casos relacionados con el phishing en transacciones comerciales con frecuencia, mientras que otro 30% lo hizo ocasionalmente y otro 30% lo hizo raramente. Estos porcentajes destacan la relevancia del tema y la necesidad de profundizar en su comprensión. Además, considerando que el 39% de las víctimas experimentaron pérdidas financieras clasificadas como bajas y un 22% como moderadas, pero un porcentaje significativo reportó niveles altos y muy altos de pérdidas (26% y 13% respectivamente), es crucial investigar las estrategias utilizadas por los estafadores y las medidas de seguridad implementadas por las plataformas de e-commerce para contrarrestar este tipo de fraude. Asimismo, dado que el 48% de los usuarios afectados experimentaron un nivel bajo de afectación y un porcentaje considerable reportó niveles moderados, altos y muy altos de afectación (22%, 22%, y 9% respectivamente), se sugiere investigar cómo la prevención y la respuesta al phishing pueden adaptarse para atender las necesidades de diferentes grupos de usuarios. Estas recomendaciones buscan profundizar en la comprensión del impacto del phishing en el e-commerce de Lima y contribuir al desarrollo de estrategias efectivas de prevención, así como respuesta.

7.4 Se recomienda dirigir futuras investigaciones hacia el análisis exhaustivo del fenómeno del vishing en el e-commerce de Lima durante el año 2023. Esto se sustenta en los datos obtenidos, donde el 39% de los encuestados informó investigar casos relacionados con el vishing ocasionalmente, mientras que otro 22% lo hizo frecuentemente. Estos porcentajes resaltan la importancia de estudiar en profundidad

este tipo de fraude informático. Además, considerando que el 30% de las víctimas experimentaron pérdidas financieras clasificadas como altas, y otro 30% como moderadas, es esencial investigar las tácticas utilizadas por los perpetradores y las estrategias de mitigación aplicadas por las plataformas de e-commerce.

7.5 Asimismo, dado que el 39% de los usuarios afectados reportaron un nivel bajo de afectación y otro 22% un nivel moderado, pero un porcentaje considerable reportó niveles altos de afectación (22%), se sugiere indagar en las medidas preventivas y de respuesta para abordar las diferentes escalas de impacto del vishing en los usuarios de e-commerce de Lima. Estas sugerencias tienen como objetivo mejorar nuestro conocimiento sobre el vishing y ayudar a crear métodos de prevención y respuesta dentro del entorno del comercio electrónico de Lima.

7.6 Se recomienda dirigir futuras investigaciones hacia el análisis detallado del fenómeno del **smishing** en el e-commerce de Lima durante el año 2023. Esto se sustenta en los datos obtenidos, donde el 30% de los encuestados informó que nunca investigaron casos relacionados con el smishing, y otro 30% lo hizo raramente. Estos porcentajes reflejan una brecha significativa en el conocimiento sobre este tipo de fraude informático, lo que justifica la necesidad de investigaciones adicionales para comprender mejor su impacto y desarrollar estrategias de mitigación. Además, considerando que el 30% de las víctimas reportaron pérdidas financieras clasificadas como moderadas, y otro 26% como altas, es crucial investigar las tácticas utilizadas por los estafadores y las medidas de protección aplicadas por las plataformas de e-commerce. Asimismo, dado que el 30% de los usuarios afectados experimentaron un nivel bajo de afectación, y otro 30% un nivel muy bajo, pero un porcentaje considerable reportó niveles moderados (17%) y altos (22%) de afectación, se sugiere explorar las diferentes escalas de impacto del smishing en los usuarios de e-commerce de Lima.

Estas recomendaciones buscan abordar las brechas identificadas en el conocimiento y la comprensión del smishing, así como contribuir al desarrollo de estrategias efectivas de prevención y respuesta en el contexto específico de e-commerce en Lima.

VIII. REFERENCIAS

Acosta M., Benavides M. & Garcia N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, vol. 25, núm. 89*, 351-368.

Acurio, S. (2020). *Delitos Informáticos: Generalidades.* Pontificia Universidad Católica del Ecuador. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alanya Rivera, M. (2021). *Inseguridad Informática y Delitos Informáticos del Usuario Fiscalía Provincial Penal Corporativa de Huancayo, 2019.* [Tesis de pregrado, Universidad Peruana Los Andes] Repositorio Institucional UPLA. https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/3944/ALANYA%20RIVERA%2C%20MARIA%20ISABEL%20TESIS%20%281%29%20%281%29%20%282%29.pdf? sequence=1&isAllowed=y

Amira, N., Razak, M., Firdau, A., Ernawan, F. y Akmar, N. (2023). Técnicas de aprendizaje automático para la detección de sitios web de Phishing. [Conferencia] *Octava Conferencia Internacional sobre Ingeniería de Software y Sistemas Informáticos*, Pulau Pinang, Malasia. https://ieeexplore.ieee.org/document/10256280

Asociación de Profesionales Financieros (2022) *Encuesta de Control y Fraude de Pagos. Aspectos destacados clave*. https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/highlights-afp-2022-payments-fraud-and-control-report.pdf

Avila, S. (2020, 11 de diciembre). *Fraude informático: 1771 personas han sido víctimas de los ciberdelincuentes según estadísticas de la DIVINDAT*. Trome. https://trome.com/actualidad/policiales/fraude-informatico-1771-personas-han-sido-victimas-de-los-ciberdelincuentes-segun-estadisticas-de-la-divindat-nczp-noticia/

Barrado, R. (2018, junio). Teoría del Delito. Evolución. Elementos Integrantes. [Seminario]. *XIX Seminario Internacional de Filosofía del Derecho y Derecho Penal*, León, España. https://ficp.es/wp-content/uploads/2019/03/Barrado-Castillo.-Comunicaci%C3%B3n.pdf

Bernal Torres, C. A. (2016). *Metodología de la Investigación* (4.ª ed.). Pearson Educación. https://bibliotecadigital.utn.edu.ec/download/files/original/fb0b0cfee2ae990609933d17c6890848960051aa.pdf

Bravo, F. (2020, 30 de junio*). Ecommerce Perú: este es el nivel de fraude que existe en las compras online.* Ecommerce News. https://www.ecommercenews.pe/comercio-electronico/2020/fraude-ecommerce-peru.html

Cajigas Moreano, L. y Pérez Chirinos, G. (2023). *La incidencia de las nuevas tecnologías en el delito de Fraude Informático y su aplicación en la Ley N° 30096 en el Perú*. [Tesis de pregrado, Universidad Andina del Cusco]. Repositorio Digital Universidad Andina del Cusco. https://repositorio.uandina.edu.pe/handle/20.500.12557/5739

Cangalaya Hilario, J. (2020). *Fraude Informático en los Bonos de Subsidio Social en Épocas de Pandemia, en la Provincia de Chanchamayo, 2020.* [Tesis de pregrado, Universidad de Huánuco]. Repositorio Institucional Universidad de Huánuco. https://repositorio.udh.edu.pe/handle/123456789/2662

Carranza Santos, J., y Hernandez Guandique, D. (2022). *El delito de Estafa Informática en el Salvador.* [Tesis de pregrado, Universidad de El Salvador]. Repositorio Institucional Universidad de El Salvador. https://repositorio.ues.edu.sv/items/9324f069-ccba-476d-b83e-45ec55ff1af2/full

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo [UNCTAD] (2021, 03 de mayo) *El comercio electrónico mundial alcanza los 26,7 billones de dólares mientras COVID-19 impulsa las ventas en línea*. https://unctad.org/es/news/el-comercio-electronico-mundial-alcanza-los-267-billones-de- dolares-mientras-covid-19-impulsa

Decreto Legislativo N° 1614. *Decreto Legislativo que modifica la Ley N° 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la Ciberdelincuencia.* (Publicado el 21 de diciembre de 2023). Diario El Peruano. Artículos 2 y 8. https://cdn.www.gob.pe/uploads/document/file/5928596/5258134-decreto-legislativo-1614.pdf?v=1708710590

Deyan, G. (2022, 07 de marzo). *Más de 61 estadísticas sobre fraude en el comercio electrónico que le ayudarán a mantenerse seguro en 2024.* Review 42. https://review42.com/resources/ecommerce-fraud-statistics/

Fernández-Bedoya, V. (2020). Tipos de justificación en la investigación científica. *Revista Trimestral del Instituto Superior Espíritu Santo,* 65-76.

Flores C., y Flores K. (2021). Pruebas para comprobar la normalidad de datos en procesos productivos: Andersondarling, Ryan-Joiner, Shapiro-Wilk Y Kolmogórov- Smirnov. *Revista de Ciencias Sociales y Humanísticas.* 87-91

Fuentes, T., Mazún, R., y Cancino, G. (2018). Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. *Revista Advance in Engineering and Innovation,* 82-94.

Galeano, S. (2024, 26 de abril). *Qué es el eCommerce: definición, modelos, ventajas y claves sobre la venta en línea en México.* Marketing4eCommerce. https://marketing4ecommerce.mx/que-es-el-ecommerce/

Giménez García, I. (2020). *El delito de fraude informático (art. 248.2.a CP): Aspectos problemáticos en relación con su interpretación y aplicación.* [Tesis de pregrado, Universidad de Alicante]. Repositorio Institucional de la Universidad de Alicante. https://rua.ua.es/dspace/bitstream/10045/130801/1/TFG-Isabel-Gimenez-Garcia.pdf

Gonzales Chavez, C. (2021). *El comercio electrónico y los problemas de la ciberdelincuencia en tiempo de COVID-19.* [Tesis de pregrado, Universidad Particular de Chiclayo]. Repositorio Institucional UDCH. http://repositorio.udch.edu.pe/bitstream/UDCH/1774/1/T044_45363605_T.pdf

Granizo Castillo J. y Paguay Calderón V. (2021). *Las Nuevas Perspectivas Regulatorias de delitos informáticos en las compras a través de Internet.* [Tesis de pregrado, Universidad Nacional de Chimborazo]. Repositorio Institucional UNACH. http://dspace.unach.edu.ec/handle/51000/7607

Harán, J. (2020, 25 de noviembre). *Crece el ecommerce y aumentan las estafas y los incidentes de seguridad.* We live Security. https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

Hartley, S., & Rudelius, W. (2018). *Marketing* (13.ª ed.). McGraw-Hill Interamericana. https://bookshelf.vitalsource.com/books/9781456261962

Hernandez D., Lutfor M., y Timko, D. (2023, 12 de noviembre) Un estudio cuantitativo de detección de phishing por SMS. *Cornell University: arXiv*. 2-5.

Hernández-Sampieri, R., & Mendoza, C (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta.* Editorial McGraw-Hill Interamericana. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Higuerey, E. (2019, 01 de junio). *Comercio electrónico: conoce todo sobre este modelo de negocios y cuáles son sus ventajas.* Rockcontent. https://rockcontent.com/es/blog/comercio-electronico/

Kuzmin, Y. (2022). Prevención del Fraude Telefónico (Aspecto Criminológico). *Oeconomia et Jus*. 47-52.

Linares Vila, J. (2022). *Fraude informático y la protección del patrimonio en tiempos de pandemia en el distrito fiscal Lima Este, 2021*. [Tesis de pregrado, Universidad Cesar Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/109240

Malca, O. (2020). *Comercio Electrónico.* (1.ª ed.). Universidad del Pacifico. https://repositorio.up.edu.pe/item/30747187-d455-4028-adf8-229c25275d1c

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis, Año 24, Nº 1*, 159-206.

Mayer L., y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de Derecho y Tecnología.* 151-184.

Mayuri, Shingavi, V., Palarpawar, R., y Nikam, S. (2023). Detección de fraude con tarjetas de crédito mediante un sistema de reconocimiento facial para comercio electrónico. *International Journal For Research in Applied Science and Engineering Technology*. 2065-2067.

Ministerio de Justicia y Derechos Humanos. (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú.* https://cdn.www.gob.pe/uploads/document/file/5948093/5270009-diagnostico-situacional-multisectorial-sobre-la-ciberdelincuencia-en-el-peru.pdf

Moran Cevallos, J., & Moran Cevallos, R. (2020). *Delitos Informáticos. Reforma al artículo 190 del COIP en el Contexto de la Emergencia Sanitaria Ecuador.* [Tesis de pregrado, Universidad de Guayaquil]. Repositorio Institucional UG. https://repositorio.ug.edu.ec/items/c50700ba-6076-42af-88d3-a2704261db8d

Organización para la Cooperación y el Desarrollo Económico. (2020). *Panorama del Comercio Electrónico. Políticas, Tendencias y Modelos de Negocio.* https://www.oecd.org/en/publications/unpacking-e-commerce_23561431-en.html

Perez, J. (2019). *Delitos regulados en leyes penales especiales.* (1.ª ed.) Gaceta Jurídica. https://es.scribd.com/document/484714405/DELITOS-REGULADOS-EN-LEYES-PENALES-ESPECIALES-pdf

Preciado Uribe, D. y Alvarez Florez, J. (2021). *Evolución del Fraude Informático: Una problemática en las Organizaciones Bancarias Colombianas* [Tesis de pregrado, Tecnológico de Antioquia Institución Universitaria]. Repositorio TDEA. https://dspace.tdea.edu.co/handle/tdea/2331?locale-attribute=en

Rahman, M., Timko, D., Wali, H., y Neupane, A. (2023, 25 de abril). Los Usuarios realmente responden al Smishing [conferencia]. *13.ª Conferencia ACM sobre Seguridad y Privacidad de Datos y Aplicaciones*, Nueva York, Estados Unidos. https://arxiv.org/pdf/2212.13312

Rajab, O., Nassreddine, G. y Massoud, M. (2023). Detector de fraude con tarjetas de crédito basado en técnicas de aprendizaje automático. *Revista de estudios de informática y tecnología*. 16-30.

Robayo-Botiva, D. (2020). *El Comercio Electrónico: concepto, características e importancia en las organizaciones.* Ediciones Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/server/api/core/bitstreams/693b8bdc-9024-429c-8182-37a4416d2c47/content

Rodriguez Bravo, O. (2020). *Análisis de los delitos informáticos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito.* [Tesis de pregrado, Universidad Laica Vicente Rocafuerte de Guayaquil]. Repositorio Institucional ULVR. http://repositorio.ulvr.edu.ec/handle/44000/4146

Safatle, P. (2020, 27 de julio). *Increíble estafa a un comerciante a través de Mercado Libre: le robaron un iPhone y 62 mil pesos*. Infobae. https://www.infobae.com/sociedad/policiales/2020/07/27/increible-estafa-a-un-comerciante-a-traves-de-mercado-libre-le-robaron-un-iphone-y-62-mil-pesos/

Stripe. (2022). *El estado del fraude en línea*. https://go.stripe.global/rs/072-MDK-283/images/State_of_online_fraud_report.pdf

Tuesta Estela, R. (2022). *Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima, 2022.* [Tesis de pregrado, Universidad Norbert Wiener]. Repositorio Uwiener. https://repositorio.uwiener.edu.pe/handle/20.500.13053/8054

Useche, M., Artigas, W., Queipo, B., Y Perozo, É. (2019). *Técnicas e instrumentos de recolección de datos cuali-cuantitativos* (1.ª ed.). Editorial Gente Nueva. https://repositoryinst.uniguajira.edu.co/bitstream/handle/uniguajira/467/88.%20Tecnicas%20e%20instrumentos%20recolecci%C3%B3n%20de%20datos.pdf?sequence=1

Ventura Quijano, M. (2021). *La Tipificación del Phishing, Smishing y Vishing en nuestro Sistema Penal, para la lucha contra la Ciberdelincuencia en Lima, 2020.* [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo]. Repositorio Institucional UNPRG. https://repositorio.upn.edu.pe/handle/11537/28942?locale-attribute=es

Verastegui Quintanilla, C. (2022). *El rol del Ministerio Publico de Lima Centro en el delito de fraude informático cometido a través del E-commerce.* [Tesis de pregrado, Universidad Cesar Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/22576

Vinelli, R. (2021). Los Delitos Informático y su relación con la Criminalidad Económica. *Ius et Praxis. Revista de la Facultad de Derecho de la Universidad de Lima,* 95-110.

Zevallos, O. (2020, 22 de mayo). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* Ius360. https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que- se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

IX. ANEXOS

Anexo A Matriz de Consistencia

TEMA : IMPACTO DEL FRAUDE INFORMÁTICO EN EL E-COMMERCE DE LIMA, 2023

PROBLEMA GENERAL Y ESPECÍFICOS	OBJETIVO GENERAL Y ESPECÍFICOS	HIPÓTESIS GENERAL Y ESPECÍFICOS	VARIABLES E INDICADORES	DISEÑO DE INVESTIGACIÓN	MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA DE ESTUDIO
PROBLEMA GENERAL ¿Cuál es el impacto del ***fraude informático*** en el ***e-commerce*** de Lima, 2023? ***PROBLEMAS ESPECÍFICOS*** 1. ¿Cuál es el impacto de la ***clonación de tarjetas de crédito*** en el e-***commerce*** de Lima, 2023? 2. ¿Cuál es el impacto del ***phishing*** en el ***e-commerce*** de Lima, 2023? 3. ¿Cuál es el impacto del ***vishing*** en el e-commerce de Lima, 2023? 4. ¿Cuál es el impacto del ***Smishing*** en el e-***commerce*** de Lima, 2023?	**OBJETIVO GENERAL** Determinar el impacto del ***fraude informático*** en el ***e-commerce*** de Lima, 2023. **OBJETIVOS ESPECÍFICOS** 1. Determinar cuál es el impacto de la ***clonación de tarjetas de crédito*** en el ***e-commerce*** de Lima, 2023. 2. Determinar cuál es el impacto del ***phishing*** en el ***e-commerce*** de Lima, 2023. 3. Determinar cuál es el impacto del ***vishing*** en el ***e-commerce*** de Lima, 2023. 4. Determinar cuál es el impacto del s***mishing*** en el ***e-commerce*** de Lima, 2023.	**HIPÓTESIS GENERAL** El ***fraude informático*** tiene un impacto significativo en el e-***commerce*** de Lima, 2023 **HIPÓTESIS ESPECIFICAS** 1. La ***clonación de tarjetas de crédito*** tiene un impacto significativo en el ***e-commerce*** de Lima, 2023. 2. El ***phishing*** tiene un impacto significativo en el ***e-commerce*** de Lima, 2023. 3. El ***vishing*** tiene un impacto significativo en el ***e-commerce*** de Lima, 2023. *4.* El ***Smishing*** tiene un impacto significativo en el ***e-commerce*** de Lima, 2023.	***VARIABLE X****:* X: Fraude Informático ***Dimensiones:*** *X.1: Clonación de tarjetas de crédito.* *X.2: Phishing* *X.3: Vishing* *X.4: Smishing* ***VARIABLE Y*** Y: *E-commerce* ***Dimensiones:*** *Y.1: Redes Sociales* *Y.2: Páginas Web* *Y.3: Aplicaciones Móviles*	***Tipo de Investigación:*** *Investigación básica.* ***Enfoque:*** *Cuantitativo* ***Alcance:*** *Correlacional* ***Diseño:*** *No experimental*	***TÉCNICAS DE RECOLECCIÓN DE DATOS*** Se utilizará la siguiente técnica de recolección de datos: 1.- Encuesta ***INSTRUMENTO DE RECOLECCIÓN DE DATOS*** Se utilizará el siguiente instrumento de recolección de datos: 1.- Cuestionario	***POBLACIÓN*** En el estudio la población estuvo constituida por 23 fiscales y asistentes en función fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia Lima. ***MUESTRA*** Se aplico un censo por lo que el tamaño de la muestra fue igual al de la población. Es decir, estuvo constituida por 23 fiscales y asistentes en función fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia Lima.

Anexo B Instrumentos De Recolección De Datos

Cuestionario 1: Variable X - Fraude Informático

Estimado(a) fiscal y asistente en función fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima el siguiente cuestionario es parte de un estudio titulado *"Impacto del Fraude Informático en el E-Commerce de Lima, 2023"*. A través de este cuestionario nos proponemos estudiar la variable "Fraude informático".

El cuestionario garantiza total anonimato y confidencialidad, por lo que le rogamos la máxima honestidad en sus respuestas.

Para responder tener en cuenta las siguientes escalas:

□	Nunca (1)	□	Muy bajo (1)	□	Totalmente en desacuerdo (1)
□	Raramente (2)	□	Bajo (2)	□	En desacuerdo (2)
□	Ocasionalmente (3)	□	Moderado (3)	□	Ni de acuerdo ni en desacuerdo (3)
□	Frecuentemente (4)	□	Alto (4)	□	De acuerdo (4)
□	Siempre (5)	□	Muy alto (5)	□	Totalmente de acuerdo (5)

DIMENSIÓN 1: Clonación de tarjetas de crédito o débito

1. ¿Con qué frecuencia has investigado casos relacionados con la ***clonación de tarjetas de crédito o débito*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

☐ Nunca

☐ Raramente

☐ Ocasionalmente

☐ Frecuentemente

☐ Siempre

2. ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de la ***clonación de tarjetas de crédito o débito*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

3.-¿Cuál ha sido el nivel de usuarios afectados debido a la ***clonación de tarjetas de crédito o débito*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

DIMENSIÓN 2: Phishing

4. ¿Con qué frecuencia has investigado casos relacionados con el ***phishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

☐ Nunca

☐ Raramente

☐ Ocasionalmente

☐ Frecuentemente

☐ Siempre

5. ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de ***phishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

6.-¿Cuál ha sido el nivel de usuarios afectados debido al ***phishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

DIMENSIÓN 3: Vishing

7.- ¿Con qué frecuencia has investigado casos relacionados con el ***vishing*** que se han producido en las transacciones comerciales del e-commerce de Lima durante el año 2023?

☐ Nunca

☐ Raramente

☐ Ocasionalmente

☐ Frecuentemente

☐ Siempre

8. ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de ***vishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

9.-¿Cuál ha sido el nivel de usuarios afectados debido al **vishing** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

DIMENSIÓN 4: Smishing

10.- ¿Con qué frecuencia has investigado casos relacionados con el ***smishing*** que se han producido en las transacciones comerciales del e-commerce de Lima durante el año 2023?

- ☐ Nunca
- ☐ Raramente
- ☐ Ocasionalmente
- ☐ Frecuentemente
- ☐ Siempre

11. ¿Cuál ha sido el nivel de pérdidas financieras de las víctimas de ***smishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima durante el año 2023?

- ☐ Muy bajo
- ☐ Bajo
- ☐ Moderado
- ☐ Alto
- ☐ Muy alto

12.-¿Cuál ha sido el nivel de usuarios afectados debido al ***smishing*** que se han producido en las transacciones comerciales del comercio electrónico (e-commerce) de Lima, durante el año 2023?

- ☐ Muy bajo
- ☐ Bajo
- ☐ Moderado
- ☐ Alto
- ☐ Muy alto

Cuestionario 2 : Variable Y - E-Commerce

Estimado(a) fiscal y asistente en función fiscal de la *Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima* el siguiente cuestionario es parte de un estudio titulado *"Impacto del Fraude Informático en el E-Commerce de Lima, 2023"*. A través de este cuestionario nos proponemos estudiar la variable "E-commerce".

El cuestionario garantiza total anonimato y confidencialidad, por lo que le rogamos la máxima honestidad en sus respuestas.

Para responder tener en cuenta las siguientes escalas:

□	Nunca (1)	□	Muy bajo (1)	□	Totalmente en desacuerdo (1)
□	Raramente (2)	□	Bajo (2)	□	En desacuerdo (2)
□	Ocasionalmente (3)	□	Moderado (3)	□	Ni de acuerdo ni en desacuerdo (3)
□	Frecuentemente (4)	□	Alto (4)	□	De acuerdo (4)
□	Siempre (5)	□	Muy alto (5)	□	Totalmente de acuerdo (5)

DIMENSIÓN 1: Redes Sociales

1.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la ***red social Facebook***?

☐ Nunca

☐ Raramente

☐ Ocasionalmente

☐ Frecuentemente

☐ Siempre

2.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático

en transacciones de e-commerce que se realizaron mediante la ***red social Facebook***?

- ☐ Muy bajo
- ☐ Bajo
- ☐ Moderado
- ☐ Alto
- ☐ Muy alto

3.- ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la ***red social Facebook***?

- ☐ Totalmente en desacuerdo
- ☐ En desacuerdo
- ☐ Ni de acuerdo ni en desacuerdo
- ☐ De acuerdo
- ☐ Totalmente de acuerdo

4.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante la ***red social WhatsApp***?

- ☐ Nunca
- ☐ Raramente
- ☐ Ocasionalmente
- ☐ Frecuentemente
- ☐ Siempre

5.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante la ***red social WhatsApp***?

- ☐ Muy bajo
- ☐ Bajo
- ☐ Moderado
- ☐ Alto
- ☐ Muy alto

6.- ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante la ***red social WhatsApp***?

- ☐ Totalmente en desacuerdo
- ☐ En desacuerdo
- ☐ Ni de acuerdo ni en desacuerdo
- ☐ De acuerdo
- ☐ Totalmente de acuerdo

DIMENSIÓN 2: Páginas Web

7.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante ***páginas web***?

- ☐ Nunca
- ☐ Raramente
- ☐ Ocasionalmente

☐ Frecuentemente

☐ Siempre

8.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante ***páginas web***?

☐ Muy bajo

☐ Bajo

☐ Moderado

☐ Alto

☐ Muy alto

9 ¿Considera que la regulación actual permite resolver eficientemente los casos de fraude informático realizados en las transacciones de e-commerce mediante ***páginas web***?

☐ Totalmente en desacuerdo

☐ En desacuerdo

☐ Ni de acuerdo ni en desacuerdo

☐ De acuerdo

☐ Totalmente de acuerdo

DIMENSIÓN 3: Aplicaciones Móviles

10.- ¿Con qué frecuencia ha investigado casos de fraude informático en transacciones de e-commerce que se realizaron mediante ***aplicaciones móviles***?

☐ Nunca

- ☐ Raramente
- ☐ Ocasionalmente
- ☐ Frecuentemente
- ☐ Siempre

11.- ¿Cuál ha sido el nivel de gravedad de los casos que investigo respecto al fraude informático en transacciones de e-commerce que se realizaron mediante ***aplicaciones móviles***

- ☐ Muy bajo
- ☐ Bajo
- ☐ Moderado
- ☐ Alto
- ☐ Muy alto

12.- ¿Considera usted que la regulación vigente permite resolver de manera eficiente los casos de fraude informático cometidos en las transacciones de e- commerce a través de ***aplicaciones móviles***?

- ☐ Totalmente en desacuerdo
- ☐ En desacuerdo
- ☐ Ni de acuerdo ni en desacuerdo
- ☐ De acuerdo
- ☐ Totalmente de acuerdo

Anexo C Confiabilidad de los Instrumentos de recolección de datos

Confiabilidad del Cuestionario1: Variable X- Fraude Informático

Cuadro 1 : Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,841	12

Nota: Calculado con el software estadístico SPSS versión 25

En el cuadros 1 se observa que el coeficiente de Alfa de Cronbach del *Cuestionario1: Variable X- Fraude Informático* arroja un valor de 0.841, determinando que el cuestionario es aplicable a las personas que participaron en nuestro estudio y tiene una consistencia interna confiable.

Confiabilidad del "Cuestionario 2: Variable Y - E-commerce"

Cuadro 2: Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,824	12

Nota: Calculado con el software estadístico SPSS versión 25

En el cuadros 2 se observa que el coeficiente de Alfa de Cronbach del *Cuestionario 2 : E-commerce* da como resultado una confiabilidad de consistencia interna de 0,824, lo que indica que el cuestionario es adecuado para su uso con las personas que participaron en nuestro estudio.

Anexo D Validez de los Instrumentos de recolección de datos

Fichas de Validación del "Cuestionario 1: Variable X - Fraude Informático"

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: HUAMANI GONZALEZ, TERESA ROHS
1.2. Cargo e institución donde labora: ABOGADO PRIVADO
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 1: FRAUDE INFORMÀTICO
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÀTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

ASPECTOS DE LA VALIDACIÓN

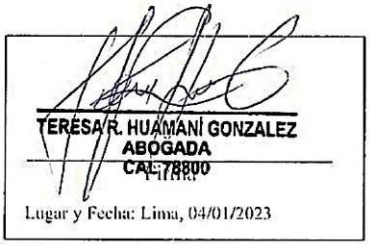
Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																				97
2. OBJETIVIDAD	Está expresado en conductas observables																				97
3. ACTUALIDAD	Adecuado al avance de la especialidad																			95	
4. ORGANIZACIÓN	Existe una organización lógica																			95	
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																			95	
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																				96
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				98
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																			95	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				98
10. PERTINENCIA	Es útil y adecuado para la investigación																				99

69

PROMEDIO DE VALORACIÓN: **96,5 %**

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ☒ Muy buena

Nombres y Apellidos:	**HUAMANI GONZALEZ, TERESA ROHS**	**DNI N°**	**46025507**
Teléfono/ Celular:	**997818036**		
Título profesional:	**ABOGADO**		
Grado Académico:	**LICENCIATURA**		
Mención	**7880 COLEGIO DE ABOGADOS DE LIMA**		



Lugar y Fecha: Lima, 04/01/2023

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: ROMERO VILLAFUERTE, ROBINSON JUAN
1.2. Cargo e institución donde labora: ABOGADO PRIVADO Y ADMINISTRADOR DE EMPRESAS
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 1: FRAUDE INFORMÀTICO
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÀTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

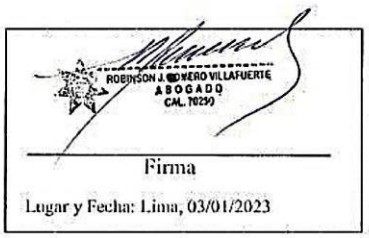
ASPECTOS DE LA VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																			95	
2. OBJETIVIDAD	Está expresado en conductas observables																				97
3. ACTUALIDAD	Adecuado al avance de la especialidad																				96
4. ORGANIZACIÓN	Existe una organización lógica																			95	
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																			95	
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																				96
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				99
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																				96
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				98
10. PERTINENCIA	Es útil y adecuado para la investigación																				99

PROMEDIO DE VALORACIÓN: **96,6 %**

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ✕ Muy buena

Nombres y Apellidos:	**ROMERO VILLAFUERTE, ROBINSON JUAN**	**DNI N°**	**08835319**
Teléfono/ Celular:	**965066342**		
Título profesional:	- **ABOGADO** - **ADMNISTRADOR DE EMPRESAS**		
Grado Académico:	**LICENCIATURA – POSTGRADO EN POLÌTICAS PÙBLICAS**		
Mención	**70290 COLEGIO DE ABOGADOS DE LIMA**		



Firma

Lugar y Fecha: Lima, 03/01/2023

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: TORRE TENORIO, ROBERT ELISEO
1.2. Cargo e institución donde labora: ABOGADO PRIVADO PENALISTA
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 1: FRAUDE INFORMÀTICO
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÀTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

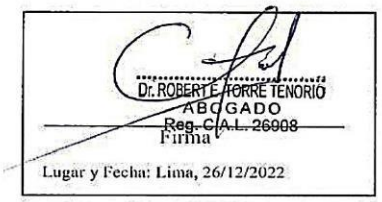
ASPECTOS DE LA VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																				98
2. OBJETIVIDAD	Está expresado en conductas observables																				98
3. ACTUALIDAD	Adecuado al avance de la especialidad																			94	
4. ORGANIZACIÓN	Existe una organización lógica																				97
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																				97
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																				96
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				100
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																			94	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				97
10. PERTINENCIA	Es útil y adecuado para la investigación																				98

PROMEDIO DE VALORACIÓN: 96,9 %

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ☒ Muy buena

Nombres y Apellidos:	**TORRE TENORIO, ROBERT ELISEO**	**DNI N°**	**06844080**
Teléfono/ Celular:	**959152945**		
Título profesional:	**ABOGADO**		
Grado Académico:	**LICENCIATURA**		
Mención	**26908 COLEGIO DE ABOGADOS DE LIMA**		



Fichas de Validación del Instrumento "Cuestionario 2: Variable Y - E-commerce"

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: TORRE TENORIO, ROBERT ELISEO
1.2. Cargo e institución donde labora: ABOGADO PRIVADO PENALISTA
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 2: E-COMMERCE
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÀTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

ASPECTOS DE LA VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																				99
2. OBJETIVIDAD	Está expresado en conductas observables																				97
3. ACTUALIDAD	Adecuado al avance de la especialidad																			95	
4. ORGANIZACIÓN	Existe una organización lógica																				98
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																				98
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				99
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																			95	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				97
10. PERTINENCIA	Es útil y adecuado para la investigación																				97

PROMEDIO DE VALORACIÓN: 97 %

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ☒ Muy buena

Nombres y Apellidos:	**TORRE TENORIO, ROBERT ELISEO**	**DNI N°**	**06844080**
Teléfono/ Celular:	**959152945**		
Título profesional:	**ABOGADO**		
Grado Académico:	**LICENCIATURA**		
Mención	**26908 COLEGIO DE ABOGADOS DE LIMA**		

76

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: ROMERO VILLAFUERTE, ROBINSON JUAN
1.2. Cargo e institución donde labora: ABOGADO PRIVADO Y ADMINISTRADOR DE EMPRESAS
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 2: E-COMMERCE
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÁTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

ASPECTOS DE LA VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																				97
2. OBJETIVIDAD	Está expresado en conductas observables																				96
3. ACTUALIDAD	Adecuado al avance de la especialidad																				96
4. ORGANIZACIÓN	Existe una organización lógica																				97
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																			95	
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				98
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																		90		
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																			95	
10. PERTINENCIA	Es útil y adecuado para la investigación																				98

PROMEDIO DE VALORACIÓN: **95.7 %**

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ☒ Muy buena

Nombres y Apellidos:	**ROMERO VILLAFUERTE, ROBINSON JUAN**	**DNI N°**	**08835319**
Teléfono/ Celular:	**965066342**		
Título profesional:	- **ABOGADO** - **ADMINISTRADOR DE EMPRESAS**		
Grado Académico:	**LICENCIATURA - POSTGRADO EN POLÌTICAS PÚBLICAS**		
Mención	**70290 COLEGIO DE ABOGADOS DE LIMA**		

Firma

Lugar y Fecha: Lima, 03/01/2023

Universidad Nacional
Federico Villarreal
Profesionales formando profesionales
ESCUELA UNIVERSITARIA DE POST GRADO

FICHA DE VALIDACIÓN DE DATOS

INFORME DE OPINIÓN DE JUICIO DE EXPERTOS

DATOS GENERALES

1.1. Apellidos y nombres del informante: HUAMANI GONZALEZ, TERESA ROHS
1.2. Cargo e institución donde labora: ABOGADO PRIVADO
1.3. Nombre del instrumento motivo de evaluación: CUESTIONARIO 2: E-COMMERCE
1.4. Título del Proyecto: IMPACTO DEL DELITO DE FRAUDE INFORMÀTICO EN LOS USUARIOS DE E-COMMERCE DE LIMA, 2023
1.4. Autor del Instrumento: ALLAZO TORIBIO, ANGELA STEFANNY

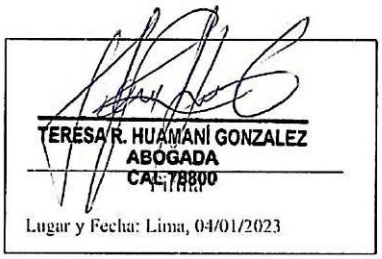
ASPECTOS DE LA VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado																				96
2. OBJETIVIDAD	Está expresado en conductas observables																			95	
3. ACTUALIDAD	Adecuado al avance de la especialidad																				96
4. ORGANIZACIÓN	Existe una organización lógica																				97
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad																				97
6. INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos científicos																				97
8. COHERENCIA	Esta descrito en dimensiones e indicadores.																				96
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				99
10. PERTINENCIA	Es útil y adecuado para la investigación																				98

PROMEDIO DE VALORACIÓN: **96.6 %**

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena ✕ Muy buena

Nombres y Apellidos:	**HUAMANI GONZALEZ, TERESA ROHS**	**DNI N°**	**46025507**
Teléfono/ Celular:	**997818036**		
Título profesional:	**ABOGADO**		
Grado Académico:	**LICENCIATURA**		
Mención	**7880 COLEGIO DE ABOGADOS DE LIMA**		



Lugar y Fecha: Lima, 04/01/2023

Anexo E Escala - Coeficiente Rho de Spearman

Valor	Significado
-1	Correlación negativa perfecta
.-0.9 a -0.99	Correlación negativa muy alta
.-0.7 a -0.89	Correlación negativa alta
.-0.4 a -0.69	Correlación negativa moderada
.-0.2 a -0.39	Correlación negativa baja
.-0.01 a -0.19	Correlación negativa muy baja
0	Correlación nula
0.01 a 0.19	Correlación positiva muy baja
0.2 a 0.39	Correlación positiva baja
0.4 a 0.69	Correlación positiva moderada
0.7 a 0.89	Correlación positiva alta
0.9 a 0.99	Correlación positiva muy ata
1	Correlación positiva perfecta