UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE CIENCIAS DE LA COMUNICACIÓN

Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Licenciada en Ciencias de la Comunicación

AUTORAS:

Chujutalli Aguilar, Nilda Eunice (orcid.org/0000-0003-4864-5441)

Retuerto Fernandez, Regina Gabriela (orcid.org/0000-0002-6728-9908)

ASESOR:

Dr. Matias Cristobal, Obed Isaias (orcid.org/0000-0001-6378-0719)

LÍNEA DE INVESTIGACIÓN:

Procesos Comunicacionales en la Sociedad Contemporánea

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

Dedicatoria

En primer lugar, queremos dedicar este trabajo a Dios por guiarnos durante nuestro proceso formativo. A nuestros padres, quienes han sido nuestro mayor apoyo y fuente de inspiración.

Agradecimiento

A Dios, por darnos las fuerzas y sabiduría para culminar este trabajo. A nuestros padres, este logro es tanto de ellos como el nuestro y esperamos que esta tesis sea una muestra de nuestro profundo agradecimiento y amor hacia cada uno de ellos.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE CIENCIAS DE LA COMUNICACIÓN

Declaratoria de Autenticidad del Asesor

Yo, MATIAS CRISTÓBAL OBED ISAIAS, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de CIENCIAS DE LA COMUNICACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023

", cuyos autores son CHUJUTALLI AGUILAR NILDA EUNICE, RETUERTO FERNANDEZ REGINA GABRIELA, constato que la investigación tiene un índice de similitud de 13.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 04 de Julio del 2023

Apellidos y Nombres del Asesor:	Firma
MATIAS CRISTÓBAL OBED ISAIAS **DNI:** 06917521 **ORCID:** 0000-0001-6378-0719	Firmado electrónicamente por: OMATIASCR el 04-07-2023 11:11:30

Código documento Trilce: TRI - 0569349

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE CIENCIAS DE LA COMUNICACIÓN

Declaratoria de Originalidad de los Autores

Nosotros, CHUJUTALLI AGUILAR NILDA EUNICE, RETUERTO FERNANDEZ REGINA GABRIELA estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de CIENCIAS DE LA COMUNICACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023

", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

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

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

Nombres y Apellidos	Firma
CHUJUTALLI AGUILAR NILDA EUNICE **DNI**: 72306822 **ORCID**: 0000-0003-4864-5441	Firmado electrónicamente por: NCHUJUTALLI el 05-07-2023 16:39:01
RETUERTO FERNANDEZ REGINA GABRIELA **DNI**: 73780386 **ORCID**: 0000-0002-6728-9908	Firmado electrónicamente por: RRETUERTOF el 05-07-2023 20:19:26

Código documento Trilce: INV - 1305850

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

Esta investigación buscó determinar cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023. Respecto a la metodología, pertenece a la investigación tipo básica, con un enfoque cuantitativo, de diseño no experimental de alcance transversal o también llamada transaccional. En cuanto al nivel de la investigación fue descriptivo simple porque la investigación buscó recolectar información de la población determinada la cual fue un total de 347 comerciantes con el fin de medir y analizar los datos sobre la variable que beneficie y sea relevante. Esta investigación utilizó la técnica de recolección de datos, donde se utilizó la encuesta descriptiva, como instrumento se aplicó el cuestionario que se realizó de forma presencial. Los resultados (sin fines de generalizar la información recolectada en relación a todos los comerciantes) indicaron que los actos comunicativos suelen presentarse mediante el uso de técnicas de comunicación como mensajes de supuestos premios de alto valor, links maliciosos, pishing y suplantación de entidades bancarias. Concluyendo que el acto comunicativo en la ciberdelincuencia de una billetera digital en los comerciantes se presenta mediante el uso de estrategias comunicativas de persuasión, manipulación y engaño en los mensajes por parte de los ciberdelincuentes.

Palabras clave:

Acto comunicativo, acción comunicativa, ciberdelincuencia, billetera digital.

Abstract

This research sought to determine how the communicative act is presented in the cybercrime of a digital wallet in merchants of a market of the district of Carabayllo, 2023. Regarding the methodology, it belongs to the basic type research, with a quantitative approach, of non experimental design of transversal scope or also called transactional. Regarding the level of the research, it was simple descriptive because the research sought to collect information from the determined population which was a total of 347 in order to measure and analyze the data on the variable that benefits and is relevant. This research used the data collection technique, where the descriptive survey was used, the questionnaire that was carried out in person was applied as an instrument. The results (without generalizing the information collected in relation to all merchants) indicated that communicative acts are usually presented through the use of communication techniques such as messages of supposed high value prizes, malicious links, pishing and impersonation of banking entities. Concluding that the communicative act in the cybercrime of digital wallets in the merchants of the Carabayllo market it is presented through the use of communicative strategies of persuasion, manipulation and deception in messages by cybercriminals.

Keywords:

Communicative act, communicative action, cybercrime, digital wallet.

I. INTRODUCCIÓN

El reciente aplicativo de la billetera digital Yape creado por un reconocido banco del Perú, ha facilitado a muchas personas con o sin negocios la nueva forma de recibir y transferir pagos, sin embargo, estas modernas plataformas virtuales han generado que sea más fácil la ciberdelincuencia, a través de actos comunicativos que incluye la comprensión del lenguaje, el contenido y la tecnología, perjudicando así a los comerciantes que buscan implementar nuevas tendencias de canales digitales en su negocio como cobros digitalizados por medio de esta App. (La República, 2022).

La problemática radicó desde el inicio de la emergencia sanitaria por el Coronavirus, los comerciantes debían adaptarse a la digitalización y el uso de la billetera digital. Según Líbero (2020), publicó una nota periodística sobre los problemas que presentaban los usuarios de esta billetera digital, las personas mencionaron que, les llegaban mensajes, llamadas, o correos maliciosos para compartir sus usuarios y contraseñas. Para ello, la empresa publicó un comunicado en sus redes sociales donde resaltaba que iban a reforzar la comunicación sobre las medidas de prevención. Es decir, las actividades comunicativas en el ciberdelito es una parte integral de comprender cómo los delincuentes utilizan un lenguaje y comunicación para promover su fechoría.

En el mundo, una mayor cantidad de personas han sido afectadas por los fraudes cibernéticos asociados a determinadas acciones comunicativas. Alrededor del mundo un estudio corroboró que un 34% de las organizaciones desean aumentar sus inversiones en su seguridad cibernética y durante el próximo año, cerca del 12% lo harán siendo más de un 50%. (Adaptix networks, 2020). Es decir, el ciberdelito ha ido creciendo a medida que se fueron desarrollando nuevas herramientas digitales a través de actos comunicativos que influyen a los usuarios a ser víctimas de ello.

En el contexto nacional, se presenció la misma realidad, de cómo los ciberdelincuentes usan la tecnología para interactuar y compartir información con otros. Por consiguiente, se requiere la implementación de una mejora de estrategias comunicacionales para promover en la sociedad una cultura preventiva sobre corroborar la información que reciben aquellos usuarios por

medio de distintas plataformas digitales de la billetera digital. Cuando se mencionan estrategias comunicacionales se requiere que dichas estrategias estén vinculadas a campañas de concientización a través de medios masivos que influyen al desarrollo de actividades para lograr el fin propuesto. (Ríos, Páez y Barbos 2020).

En este sentido, es importante analizar cómo la acción comunicativa en la ciberdelincuencia afecta a la seguridad de la información y la privacidad de los usuarios, así como identificar las estrategias que utilizan los delincuentes para llevar a cabo sus acciones y las medidas comunicacionales que se pueden implementar para prevenir y combatir estos delitos. Lo que abre paso al problema general de la investigación: ¿Cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023? .

De tal modo, se presentaron los siguientes problemas específicos: ¿Cómo los procesos del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023?, ¿Cómo los mensajes del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023? y ¿Cómo el acto comunicativo a través de la herramienta digital de SMS pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023?.

El estudio tuvo como justificación teórica al autor Habermas de la teoría de la acción comunicativa 1987, expresa que, la interacción comunicativa se da mediante un lenguaje entre dos o más sujetos, incidiendo en el mensaje un propósito y la consecuencia que puede tener entre el emisor y receptor. De tal forma, se da importancia a la sociedad quienes son la audiencia que se encarga de recibir y comunicar lingüísticamente una información (Garrido, 2011). Por lo tanto, la investigación se justifica teóricamente porque se amplió el conocimiento del acto comunicativo de la ciberdelincuencia en una billetera digital a través de la recopilación de artículos científicos, tesis doctorales y revistas científicas.

Por consiguiente, la justificación social de la investigación está vinculada al Objetivo de Desarrollo Sostenible específicamente con el número ocho titulado “Trabajo decente y crecimiento económico”, porque será una contribución a los comerciantes que implementan nuevas herramientas digitales como plan de estrategia para el crecimiento económico en sus negocios a fin de aportar mejoras en el uso correcto de la aplicación. Es por ello, que se debe tener en cuenta los riesgos como la ciberdelincuencia a las que se exponen al implementar nuevas plataformas virtuales para realizar transferencias bancarias, asimismo, la importancia de identificar mensajes con pretensiones maliciosos.

Respecto a la justificación metodológica, se realizó con un enfoque cuantitativo, el tipo de investigación fue básica y se recopilaron datos a la población de un mercado de Carabayllo que están relacionadas en dicha problemática, se recopiló datos por medio del instrumento del cuestionario que se midió mediante la escala de likert. Esta investigación también conllevó un exhaustivo procedimiento metodológico enfocado totalmente, cumpliendo con la expectativa de un proyecto de tesis.

Por consiguiente, se planteó como objetivo general: Determinar cómo se presenta el acto comunicativo en la ciberdelincuencia en una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023. Seguidamente se planteó los objetivos específicos: Determinar cómo los procesos del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023, Determinar cómo los mensajes del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023 y Determinar cómo el acto comunicativo a través de la herramienta digital de SMS pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023.

II. MARCO TEÓRICO

Después de comprender la realidad problemática que afronta la ciberdelincuencia a nivel internacional y nacional, es vital destacar que el adecuado uso de las herramientas digitales y la importancia de confirmar la información que se recibe a través de distintas plataformas de comunicación reduciría el porcentaje en las víctimas. De tal forma, se presentaron los antecedentes nacionales e internacionales desarrollados por diversos autores.

Baldera, A (2021), tuvo como objetivo encontrar la relación entre la publicidad digital y la posición otorgada de una billetera digital. Fue desarrollado con diseño no experimental, nivel correlacional, aplicada y cuantitativo, contó con un total de 40 microempresarios de SJL como muestra y sus resultados estadísticos favorecen la existencia de una relación de las variables por lo que se concluyó que existe una relación con el posicionamiento y la publicidad digital de la app Yape en los comerciantes de la zona específica.

Li, J. Li, Fan y Wang (2022), tuvieron como objetivo, analizar el impacto de las redes sociales, los videojuegos en aplicativos móviles y las creencias de religión de los padres en la tendencia de los adolescentes a los ciberdelitos en la era COVID-19. Su investigación utilizó a un total de 265 estudiantes de colegios en nivel secundaria y universidades para la recolección de datos con la escala de Likert mediante encuestas. Su conclusión determinó que el internet fue de manera negativa para los estudiantes en época de COVID-19 aumentando los casos de delitos digitales por la excesiva libertad en estos medios, atrayendo a los delincuentes cibernéticos.

Monteith, Bauer, Alda, Geddes, Whybrow y Glenn (2021), tuvieron como propósito, analizar los diferentes usos de la tecnología, su impacto durante la pandemia, la evolución de los ciberdelitos, sus debilidades y las preocupaciones en las personas con discapacidad mental, donde metodológicamente tuvieron un enfoque cualitativo y nivel descriptivo; aplicaron la técnica de la encuesta e instrumento cuestionario Concluyeron que la tecnología brindó herramientas necesarias que deben usarse con las medidas de seguridad correspondientes, que las capacidades de las personas son un elemento central en la

ciberseguridad y que las actividades en el internet y la tecnología dañan la susceptibilidad.

Mengoa, M (2021), el objetivo general del estudio, fue determinar la influencia de la conducta del *phisher-mule* en los delitos cibernéticos. Para ello, se utilizó un enfoque cualitativo de tipo básico y nivel descriptivo, y se empleó una técnica de recolección de datos que incluyó análisis y entrevistas de fuentes documentales utilizando un método sistemático. Sin embargo, los resultados obtenidos indicaron que la conducta del phisher-mule no fue individualizada para su inclusión en el código penal peruano, lo que sugiere la necesidad de llevar a cabo investigaciones más detalladas sobre el tema. En conclusión, la delincuencia digital ha ido avanzando con una rapidez junto con la tecnología, por lo que incluir de forma expresa en la legislación los diferentes tipos de modalidades, fraudes, hurtos cibernéticos y tanto la capacitación de los personales para un correcto procedimiento contra el delito informático.

Lopez y Palomino (2021), tuvieron como objetivo, identificar las relaciones entre la actitud, utilidad notada, facilidad percibida, confianza y riesgo con el interés de uso de las aplicaciones móviles para la realización de transacciones de dinero en Yape y otro aplicativo móvil. Asimismo, su enfoque fue cuantitativo y fue catalogado como diseño no experimental y de tipo correlacional y de corte transversal. Como resultado se detectó que 80 personas usan Plin y 235 usan Yape. Su conclusión fue que la mayoría de los usuarios usaron el aplicativo móvil por obligación y por necesidad, por motivo a que los contactos optaron por el uso de la app móvil siendo de facilidad en las transacciones. Asimismo, los millennials urbanos no son conscientes del peligro que hay en el ciberespacio y por ello no se animan a comprar en internet por temor a ser víctimas del fraude digital y al robo de información.

Carreña, I (2021), tuvo como objetivo, precisar las fallas en las investigaciones por delito de fraude informático en Lima, donde se aplicó un método no experimental, con un enfoque cualitativo, tipo básico. De tal forma, para la muestra se aplicó la entrevista a diferentes expertos en la materia. Su conclusión fue que las principales deficiencias fue la falta de capacitación a las diversas modalidades informáticas, causando daños en el curso y dirección de las investigaciones fiscales por estos ilícitos. Para finalizar el autor recalca que

una de las principales deficiencias, es la falta de capacidad que se ha dado ante los casos delitos informáticos cuando se pudo a presuntos delincuentes cibernéticos, siendo así otra deficiencia reconocida por el autor fue la falta de actualización normativa para realizar nuevas modalidades para combatir la delincuencia digital y el fraude cibernético.

Garcia, E (2021), en su investigación tuvo como objetivo, investigar la responsabilidad penal de las redes del pishing en Colombia. En lo metodológico, fue una investigación socio-jurídica que sirvió de la teoría de la sociedad del riesgo y de la hermenéutica jurídica. Concluyó que la evolución tecnológica y el alto influjo de las tecnologías de la comunicación y la información comunican un cambio, lo que pone en riesgo la privacidad de la información, la seguridad del patrimonio o la circulación de los datos. Para finalizar, desde la aparición de los nuevos desarrollos de las TIC, trajo consigo cambios que han perjudicado a una gran parte de usuarios en la pérdida de datos personales e integridad y privacidad.

Chávez, Miranda, Quispe y Robles (2019) realizaron un estudio con el objetivo de proponer y validar un modelo para determinar e identificar los factores significativos que influyen en el uso de la tecnología de pago móvil en los microempresarios. El estudio fue explicativo, con un enfoque cuantitativo y transversal. La encuesta se diseñó con base en preguntas de la literatura y se realizó con 200 gerentes de restaurantes en el distrito de Santiago de Surco. Su propósito era brindar recomendaciones a la gerencia en base a los resultados obtenidos.

Ghazi y Pontell (2021), tuvieron como objetivo, explicar el estado del phishing, los desarrollos tecnológicos esperados y mejores estrategias de prevención y utilidad. La investigación utilizó los datos que provinieron de entrevistas con un aproximado de 60 profesionales de la tecnología de la información, "hackers" e investigadores académicos. Donde concluyeron que el phishing evolucionó crecientemente convirtiéndose así en el causante directo del fraude financiero y que la correcta prevención procederá del aprendizaje y la educación cibernética.

Giannini, H (2008), explica que la comunicación se trata de una experiencia de acciones comunicativas no necesariamente verbales, pueden ser aquellas que se dan forma de gestos y que la acción comunicativa está constituida por la acción misma de relacionarse con las personas. Donde concluye que la comunicación está aludido a la acción y a procurar algún tipo de respuesta en el otro individuo.

Moya, C (2009), La autora en su artículo menciona el concepto de la pragmática que estudia el lenguaje en su uso y la acción que se da, donde evidenció la conexión entre el lenguaje y la acción. Concluyó que desde la perspectiva de la semiótica la comunicación lingüística tiene como base fundamental la comprensión del mensaje a través de las acciones.

Pons, V (2018), tuvo como objetivo, tener una visión teórica-práctica firme del ciberterrorismo. La investigación tuvo un enfoque cualitativo, aplicado desde una perspectiva hermenéutica. Así mismo se hizo uso de algunas herramientas cuantitativas para alimentar el proceso de análisis. Esta investigación concluyó que con la aparición del ciberespacio aumentó en dimensiones agigantadas los delincuentes digitales dándoles oportunidad de cometer actos ilícitos por la falta de información acerca del ciberespacio y sus consecuencias en el mal uso. Para finalizar, se recomendó que se deben reforzar estrategias, propuestas y mejoras que ayuden a frenar este acto delictivo que afecta a diferentes países del mundo.

Alarcon y Barrera (2017), tuvieron como objetivo, establecer de qué manera se relacionaron el uso del internet con los delitos informáticos. Así mismo utilizaron el método de tipo básico, con diseño no experimental, en la recolección de los datos acudieron a la validación de un cuestionario con la Técnica Delphi. Para concluir, llegaron a deducir que los estudiantes necesitaron una comprensión por parte de los profesores para el desarrollo de suficiencia, habilidades y actitudes en el uso del internet para las competencias informacionales por acceso a la información, porque depende de ello el uso adecuado y legal de la información. Para finalizar, la relación entre ambas variables son un problema que se ha ido encontrando en diferentes modalidades y ha ido avanzando de la mano con la tecnología, lo cual requiere una profunda reflexión ante la educación digital para desarrollar competencias de información en el uso adecuado del internet.

Ahmad y Jabin (2017), tuvieron como objetivo, presentar diversas categorías de características que fueron utilizados para la identificación de los perfiles falsos, donde encontraron distintos puntos de rastreo de datos y fuentes de información existentes. Utilizaron la recolección de datos artificiales para probar algoritmos y herramientas basadas en las estadísticas o parámetros de distintas redes sociales. Concluyendo que las redes sociales tienen un papel importante para la actividad diaria de los cibernautas, asimismo los ciberdelincuentes fueron atraídos por las redes sociales para cometer actos delincuenciales, especialmente la creación de perfiles falsos suplantando identidades para realizar estafas.

Hamzaoui, M (2019), tuvo como objetivo, ampliar el seguimiento de los delitos digitales para debatir las modalidades de fraude cibernéticas que no tienen mucho alcance como también realizar el estudio de las conductas del ser humano frente a los delitos cibernéticos. Asimismo, utilizaron el método de tipo básico, con diseño no experimental. También tuvo como muestra a jóvenes de la ciudad de El Jadida, en la recolección de datos realizó la observación de las conductas de los jóvenes y llegó a la conclusión que el comportamiento humano es múltiple frente a estos casos de delitos y es importante conocer las características porque permitirá gestionar estrategias en la lucha contra la ciberdelincuencia.

Ampuero y Smith (2017), tuvo como objetivo investigar de qué forma se da la eficacia de la estrategia de comunicación de una campaña de sensibilización en alumnos del 5to grado. Su tipo de investigación fue aplicada de nivel descriptivo simple, con un enfoque cuantitativo no experimental. Su muestra se conformó por 152 estudiantes donde aplicaron la técnica de la encuesta, a través de un cuestionario, donde tuvieron como resultado que los alumnos se desenvuelven de manera eficaz, ya que la mayoría de los estudiantes estuvieron concentrados en el mensaje y confirmaron haber tenido un cambio en su actitud.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1 Tipo de investigación: Para el presente trabajo se optó por una investigación tipo básica en donde el Consejo Nacional de Ciencias, Tecnología e Innovación Tecnológica (CONCYTEC) (2018), indicó que, la investigación pura o también llamada básica, incrementa la información o conocimientos de manera científica sin llevarlo a lo práctico. Por lo tanto, este trabajo buscó concretar las propiedades más reales y exactas adquiridas en base a la recolección de datos en la cual se podrá determinar cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, donde posteriormente la conclusión de este estudio servirá como base teórica para futuras investigaciones científicas que pretendan indagar en la variable.

Dicha investigación tuvo un enfoque cuantitativo, en la que Sampieri (2014), mencionó que, permite analizar y recoger datos estadísticos para contestar la cuestión de la presente investigación y demostrar así su confiabilidad. Es por ello, que para determinar cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo se llevó a cabo un enfoque cuantitativo en la que se realizó la técnica de la encuesta y recolección de datos, donde se procesó estadísticamente por el software SPSS, los resultados fueron interpretados para posteriormente realizar la discusión y las respectivas conclusiones de la investigación.

3.1.2 Diseño de investigación:

El diseño de la investigación es no experimental puesto que, el trabajo de investigación se realizó sin manipular la variable que es acto comunicativo basándose en la observación de los fenómenos para luego ser llevado a acabo un análisis estadísticos. De alcance transversal, debido a que se desarrolló un proceso de recolección de datos en un solo momento. Como lo define Huaire (2019), el estudio transversal recoge datos en un tiempo único, donde su propósito es describir, indagar variables en la población y distinguir su incidencia tanto como la interrelación en un tiempo dado.

En cuanto al nivel de la investigación fue descriptivo simple, donde Guevara, Verdesoto y Castro (2020), definen que, está orientado en identificar cualidades, describir características de conjuntos homogéneos para así determinar una decisión de los fenómenos del estudio. Es por ello que la investigación buscó recolectar información de la población determinada con el fin de medir y analizar los datos en base a métodos estadísticos sobre la variable.

3.2. Variables y operacionalización

Ante la temática de la investigación titulada “Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023”. Se determinó que la variable independiente del presente trabajo es el acto comunicativo.

Definición conceptual: Los actos comunicativos se dan en el uso del lenguaje verbal y no verbal, donde las personas seleccionan una expresión lingüística comprensible en donde puedan comprenderse el uno al otro. Todos estos elementos funcionan en conjunto para interpretar un mensaje como parte de un pensamiento y una narrativa, con el fin de comunicar exactamente lo que se quiere expresar tomando en cuenta el contexto en el que ocurre la comunicación (Rios y Christou, 2010).

Definición operacional: El presente ámbito temático se midió con un cuestionario a partir de un análisis de datos de acuerdo a las 3 dimensiones propuestas, en razón al acto comunicativo.

Indicadores:

Permite medir las características de la variable acto comunicativo. Como característica de la variable independiente se logró obtener a las siguientes: Lenguaje verbal, Whatsapp, Contenido, Construcción del mensaje, Interpretación del mensaje, Credibilidad del contenido, Finalidad de contenido y Respuesta del usuario.

Escala de medición:

La medición empleada para recolección de datos fue la escala de Likert, porque evaluará el nivel de grado de opinión de la muestra sobre el acto comunicativo. (Bertram, 2008 como se citó en Matas, 2018), estos instrumentos se encargaron de la medición donde el encuestado indica su acuerdo o desacuerdo, reactivo o ítem.

Tabla 1

Escala de medición de Likert

1	2	3	4	5
Nunca	Casi nunca	Ocasionalmente	Casi todos los días	Todos los días

Fuente: Elaboración propia

3.3. Población

3.3.1 Población: Hernández y Carpio (2019), definieron que, la población necesita buenas inversiones de recursos que sean limitados a la zona de investigación, la muestra es parte que representa la población que está formada por unidades muestréales que son parte del objetivo de estudio, donde se apoya del muestreo que se define como la parte de la población que ha de ser estudiada.

El estudio de investigación abarcó una población finita donde Arias y Covinos (2021), considera cuando se conoce la cantidad exacta de individuos que constituyen el universo. Dicha investigación contó con hombres y mujeres comerciantes mayores de edad que sean usuarios de una billetera digital de un mercado del distrito de Carabayllo. Lo cual contó con un total de 347 comerciantes.

Criterios de inclusión: Se incluyó a hombres y mujeres mayores de edad que fueran comerciantes de un mercado del distrito de Carabayllo.

Definición de mayores de edad

Personas mayores de edad en Perú son aquellas que han cumplido 18 años de edad, según lo establecido por la Constitución Política del Perú de 1993, artículo 1 (Ministerio de Justicia y Derechos Humanos, 2019).

Definición de comerciante

Se considera comerciantes a las personas que tienen la capacidad legal para realizar el comercio y se dedican a él regularmente. (Código del comercio, artículo 1).

Criterios de exclusión: Se excluyeron a hombres y mujeres de menor edad que no sean comerciantes de un mercado del distrito de Carabayllo y comerciantes que no hacen uso de la billetera digital Yape.

3.3.4 Unidad de análisis: Es el objeto que está en estudio, los cuales proporcionan información que permiten ser analizados (Arias, 2020). La unidad de análisis de esta investigación fueron los comerciantes mayores de edad, hombres y mujeres que usen una billetera digital en un mercado del distrito de Carabayllo, 2023.

3.4. Técnicas e instrumentos de recolección de datos

Técnica: Según López y Fachelli (2015), mencionaron que, el propósito de la técnica de la encuesta para una investigación cuantitativa es recolectar información sistematizada en base a la problemática que se plantea dentro de la investigación mediante un cuestionario.

Esta investigación utilizó la técnica de recolección de datos, donde se aplicó la encuesta descriptiva, que se realizó de forma presencial a nuestra población.

Instrumento: El cuestionario es un instrumento utilizado para obtener de manera ordenada la información que permitirá percibir las variables de interés del estudio de investigación. Bravo y Valenzuela (2019).

Para el presente estudio se trabajó con el instrumento del cuestionario el cual permitió conocer cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023, con base en 15 preguntas cerradas para la recolección de datos. (Ver anexo 3) Además, se esquematizó un proceso de operacionalización de la variable, dimensiones e indicadores cuyo ítem responde de manera ordenada y directa. (Anexo 1)

La calificación se basó en la escala tipo Likert, puesto que se recogió información mediante las respuestas donde permitió medir la opinión de los comerciantes del mercado del distrito de Carabayllo.

De la misma manera, el instrumento del cuestionario fue validado por tres expertos de la especialidad, donde calificaron cada interrogante del instrumento.

De tal forma, se realizó una autenticidad de contenido que estuvo enlazado con la validez de constructo, lo que posibilitó la adquisición de indicadores, luego de ello se generó la redacción de los ítems del cuestionario. Luego de tener la valoración del instrumento de los expertos se aplicó el coeficiente V de Aiken, lo que posibilitó medir la validez de los ítems.

Figura 1

Fórmula de Coeficiente V de Aiken

$$V = \frac{S}{\mathrm{N}(\mathrm{C}-1)}$$

Fuente: Elaboración propia, 2022

Dónde: S: La suma de si

SI: Valor asignado por el juez i

N: Número de Jueces

C: Número de valores de la escala de valoración

(Anexo 6)

3.5. Procedimientos

La investigación inició con la revisión de la literatura de la variable objeto de estudio, que permitió contextualizar la problemática y, por ende, la elaboración del marco teórico. Asimismo, mediante la teoría y la variable se definieron las dimensiones y objetivos de la investigación.

Después de efectuar la revisión en las bases de datos (Scopus, Redalyc, Elsevier y Alicia) y la realización del instrumento, este fue remitido para ser validado por tres profesionales, que fue enviada a sus correos electrónicos, lo cual se les envió los siguientes formatos: carta de presentación, operacionalización de la variable, matriz de consistencia, el instrumento y una ficha de evaluación académica entregada por la casa de estudios. (Anexo 4)

Tabla 2

Datos de validadores

N°	Experto	Grado Académico	Especialista
1	Rony Rafael Rojas Rojas	Grado de Magíster	Periodismo y Comunicación
2	Mariano Vargas Arias	Grado de Magíster	Comunicación y Audiovisual
3	Joohn Raúl Oblitas Carreño	Grado de Magíster	Comunicación

Fuente: Elaboración propia

Luego de ello, se procedió a entablar procesos con el personal administrativo del mercado “Asociación comerciantes Mayorista de las Tres Regiones” para la autorización de las encuestas. (Anexo 7)

Asimismo, se efectuó la encuesta a los comerciantes del mercado de Carabayllo, a lo que se elaboró un cuestionario de 15 preguntas correspondiente a la variable, la encuesta se realizó a cada comerciante mediante el cuestionario, posteriormente aplicado el instrumento a la muestra, se efectuó al software SPSS, para facilitar su descripción.

3.6. Método de análisis de datos

Peña (2017), concordó que, en la investigación los datos son de suma importancia para comenzar los procesos investigativos para su desarrollo.

Para el presente estudio, se consideró a una población finita del mercado “Asociación comerciantes Mayorista de las Tres Regiones” de Carabayllo. Asimismo, se utilizó una encuesta descriptiva en base a los ítems estructurados en el cuestionario con preguntas cerradas. Posteriormente los datos obtenidos fueron ordenados en Excel, para ser procesados en el programa estadístico SPSS, a fin de generar resultados descriptivos donde se gestionaron tablas y gráficas de porcentajes que fueron interpretados a fin de determinar las conclusiones de la investigación.

3.7. Aspectos éticos

Cabe importante mencionar que para el presente estudio se consideraron aportaciones teóricas de artículos científicos indexados, investigaciones de tesis de maestrías y de doctorado en bases de datos como Scopus, Redalyc, Elsevier y Alicia. Asimismo, este trabajo pretende ser un aporte a futuras investigaciones que sirva de herramienta para otros investigadores. Los datos reflejados en la investigación no fueron manipulados ni exagerados.

Con el fin de desarrollar adecuadamente los aspectos éticos, se tomaron en consideración las reglas del sistema APA séptima edición, para realizar las citas y referencias correspondientes, verificando la información, la autenticidad y confiabilidad de los datos, protegiendo los derechos de autor. Además, se emplearon los lineamientos de elaboración de informes académicos mencionados en la Guía de Elaboración de Tesis propuesta por la Universidad César Vallejo.

En cuanto a los principios éticos se consideró el código de ética de la universidad César Vallejo, los cuales se hace mención a los más destacados: El principio de autonomía, los autores tuvieron la capacidad de decidir la realización del proyecto de investigación; la beneficencia, dicha investigación tiene el objetivo de actuar en contribución a la sociedad; en cuanto al principio de justicia, este trabajo conlleva una problemática en el Perú, el cual no solo beneficiará a un grupo, sino a un país, y el trato hacia los participantes fue igualitario y decente y el principio de la no maleficencia, por lo que no hubo intención de hacer daño a terceras personas ni afectar la integridad psicológica y física de ningún participante. (Universidad César Vallejo, 2020; Código de ética en investigación, Vicerrectorado de Investigación Resolución de Consejo Universitario N°0262-2020-UCV).

IV. RESULTADOS

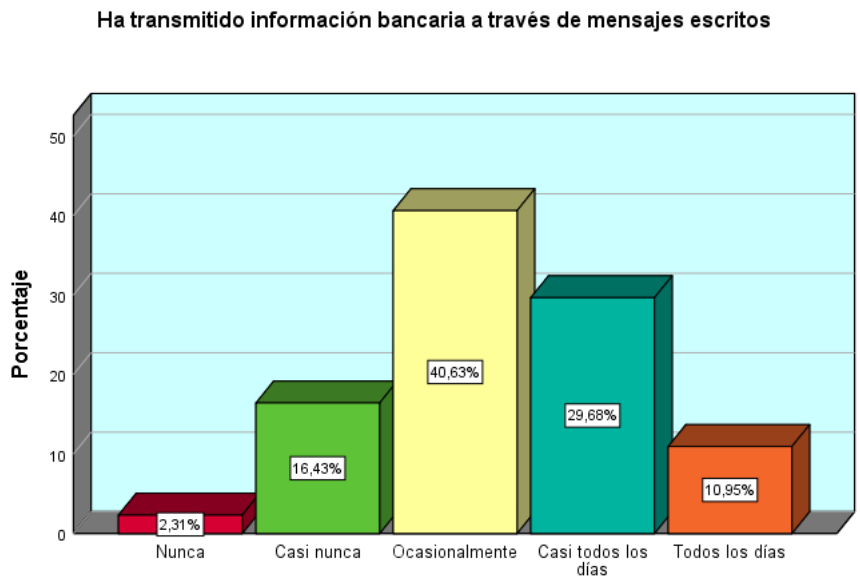
Luego de haber gestionado la encuesta en el mercado de Carabayllo, a 347 comerciantes, en cuestión a los actos comunicativos en la ciberdelincuencia en el mercado mayorista de las Tres Regiones, se analizaron los siguientes apuntes:

Ítem 1: Ha transmitido información bancaria a través de mensajes escritos (Gráfico 1)

Tabla 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	8	2.3	2.3	2.3
	Casi nunca	57	16.4	16.4	18.7
	Ocasionalmente	141	40.6	4.6	59.4
	Casi todos los días	103	29.7	29.7	89.0
	Todos los días	38	11.0	11.0	100.0
	Total	**347**	**100.0**	**100.0**	

Fuente: Elaboración propia SPSS



Fuente: Elaboración propia SPSS

Interpretación: Según los resultados obtenidos en la tabla 1, un 40,63% que representa a 141 comerciantes del mercado de Carabayllo, afirmaron que, ocasionalmente han transmitido información bancaria a través de mensajes escritos. Por otro lado, un 29,68% que representa a 103 encuestados, mencionaron que, casi todos los días transmiten información bancaria, mientras que, un 2,31% que representa a 8 comerciantes, indicaron que, nunca han transmitido información bancaria de una billetera digital. Se infirió que, los comerciantes en algunas ocasiones si comparten información bancaria en mensajes escritos cuando el remitente se lo pide.

Ítem 2: Ha trasmitido información bancaria por medio de mensajes de mensajes de audio (Gráfico 2)

Interpretación: Según lo expuesto en la tabla 2, se observó que, un 54,76% que representa a 190 encuestados, afirmaron que, ocasionalmente han transmitido información bancaria por medio de mensajes de audio. Por otro lado, un 0,29% que representa a un comerciante, indicaron que, transmitieron información bancaria por este medio todos los días. Se infirió que, los participantes en algunas ocasiones han brindado información por mensajes de audio porque se les hace más instantánea.

Ítem 3: Recibe mensajes de transferencia bancaria por medio del WhatsApp (Gráfico 3)

Interpretación: Según lo expuesto en la tabla 3, un 51,30%, que representa a 178 comerciantes encuestados, mencionaron que, casi todos los días reciben mensajes de transferencia bancaria por medio del WhatsApp, mientras que, un 31,41% que representa a 109 personas encuestadas, comentaron que, ocasionalmente reciben este tipo de mensajes por medio del aplicativo WhatsApp, mientras que, un 1,44%, que representan 5 comerciantes no lo reciben nunca. Se infirió que, los comerciantes se les hace más útil usar el Whatsapp como medio de mensajes de transferencia de una billetera digital.

Ítem 4: Ha sido víctima de pago por supuestos clientes que muestran captura por medio del WhatsApp (Gráfico 4)

Interpretación: Según lo expuesto en la tabla 4, un 56,20% de los encuestados conformado por 195 personas, indicaron que, ocasionalmente han sido víctimas de pago por supuestos clientes que muestran captura por medio del WhatsApp, mientras que, un 0,86% conformado por 3 personas de la muestra sufrieron este tipo de estafas todos los días. Se infirió que, los comerciantes ocasionalmente no corroboraron el pago que les hicieron por medio del aplicativo de WhatsApp.

Ítem 5: Ha recibido un monto depositado de diferente color en su aplicación (Gráfico 5)

Interpretación: Según lo expuesto en la tabla 5, un 46,69% que corresponde a 162 encuestados han recibido ocasionalmente un monto depositado de diferente color en su aplicación. Por otro lado, un 34,87% que corresponde a 121 personas, afirmaron que, casi todos los días pasan por esa situación y el 1,15% de los encuestados conformado por 4 personas nunca han recibido un monto de diferente color de una transferencia bancaria. Se infirió que, los comerciantes no supieron diferenciar las características del recibo digital de su aplicativo de pago.

Ítem 6: Ha recibido una compra de un QR falso en su billetera digital (Gráfico 6)

Interpretación: Según lo expuesto en la tabla 6, un 50,72% de los encuestados que representa a 176 encuestados, indicaron que, ocasionalmente han recibido una compra de un QR falso en su billetera digital, mientras que, un 23,34% conformado por 81 participantes, indicaron que, casi nunca han recibido una compra de QR falso en sus billeteras digitales, y que el 1,15% que conforman 4 comerciantes lo reciben todos los días. Se infirió que, los comerciantes ocasionalmete al momento de ver el código QR del pago de la billetera digital no reconocieron la veracidad de este.

Ítem 7: Ha recibido mensajes de propuestas diciéndole que al pagar usted aumenta sus probabilidades de obtener su premio ganador (Gráfico 7)

Interpretación: Según lo expuesto en la tabla 7, el 56,20% de los encuestados que representa a 195 personas, afirmaron que, han recibido casi todos los días mensajes de propuestas diciéndoles que al pagar aumentan sus probabilidades de obtener su premio ganador en su billetera digital, mientras que, un 25,65% que representa a 89 comerciantes, ocasionalmente han recibido este tipo de mensajes donde les piden realizar pagos y el 2,59% de los encuestados que representa a 9 personas, casi nunca han recibido este tipo de mensajes. Se infirió que, los comerciantes casi todos los días han sido abrumados por mensajes de dudosa procedencia.

Ítem 8: Por medio de los mensajes ha recibido enlaces o un archivo adjunto diciendo que se ganó un premio de alto precio (lotería, IPad, carro nuevo, etc.) (Gráfico 8)

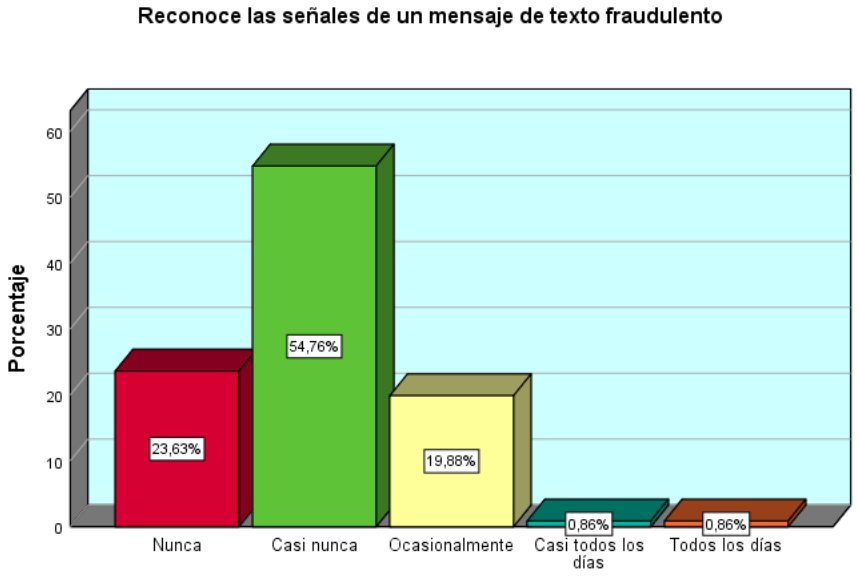
Interpretación: Según lo expuesto en la tabla 8, un 55,62% que está conformado por 193 encuestados, mencionaron que, ocasionalmente recibieron enlaces o archivos adjuntos diciendo que ganaron un premio de alto precio. Por otro lado, un 20,46% afirmaron que casi todos los días le suelen llegar este tipo de mensaje de texto, mientras que, un 2,59% que representa a 9 comerciantes, afirmaron que, nunca lo han recibido. Se infirió que, los estafadores suelen enviar ocasionalmente enlaces por medio de mensajes.

Ítem 9: Reconoce las señales de un mensaje de texto fraudulento (Gráfico 9)

Tabla 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	82	23.6	23.6	23.6
	Casi nunca	190	54.8	54.8	78.4
	Ocasionalmente	69	19.9	19.9	98.3
	Casi todos los días	3	.9	.9	99.1
	Todos los días	3	.9	.9	100.0
	Total	**347**	**100**	**100**	

Fuente: Elaboración propia SPSS



Fuente. Elaboración propia SPSS

Interpretación: Según lo expuesto en la tabla 9, un 54,76% que representa a 190 encuestados, afirmaron que, casi nunca reconocen las señales de un mensaje de texto fraudulento. Por otro lado, un 23,63% nunca han sabido reconocer un mensaje de texto sobre una estafa y lo suelen confundir como un mensaje normal, mientras que, un 0,86% indicaron que, saben perfectamente reconocer cuando un mensaje de texto es fraudulento. Se infirió que, los comerciantes al momento que les llega un mensaje de dudosa procedencia, ellos no saben reconocer la veracidad de su contenido.

Ítem 10: Identifica los mensajes de texto que se hacen pasar por una entidad financiera (Gráfico 10)

Interpretación: Según lo expuesto en la tabla 10, un 43,80% que es la mayor parte de los encuestados casi nunca han identificado los mensajes de texto que se hacen pasar por una entidad financiera, mientras que, un 38,04% que representa a 132 comerciantes, afirmaron que, ocasionalmente han identificado las características de un mensaje de texto que intentan suplantar entidades bancarias y un 5,19% saben identificar perfectamente un mensaje que intenta suplantar su billetera digital. Se infirió que, los comerciantes no logran identificar la originalidad de texto de una entidad bancaria y suelen caer en mensajes fraudulententos de entidades ficticias que les ofrecen supuestos beneficios.

Ítem 11: Brinda información personal por medio de mensajes a personas o entidades desconocidas (Gráfico 11)

Interpretación: Según lo expuesto en la tabla 11, un 44,67% que está comprendido por 155 encuestados, afirmaron que, casi todos los días han brindado información personal por medio de mensajes a personas o entidades desconocidas que le ofrecen algún beneficio. Por otro lado, un 27,36% manifestaron que, ocasionalmente suelen compartir información personal por medio de mensajes a personas o entidades nuevas, mientras que, un 0,58% lo hacen todos los días. Se infirió que, los comerciantes no tomaron medidas de seguridad con respecto a brindar información personal por tratatar de ser beneficiados.

Ítem 12: Responde o acepta mensajes de texto de remitentes desconocidos que ofrecen algún beneficio (Gráfico 12)

Interpretación: Según lo expuesto en la tabla 12, un 47,84% que está comprendido por 166 encuestados, indicaron que, ocasionalmente responden o aceptan mensajes de texto de remitentes desconocidos que ofrecen algún beneficio, mientras que, un 6,34% conformado por 22 comerciantes, afirmaron que, están dispuestos a responder los mensajes que ofrecen beneficios sin importar la persona que sea el remitente. Se infirió que, los comerciantes ocasionalmente han brindado parte de su tiempo para escuchar o responder remitentes que ofrecen un beneficio de procedencia dudosa.

Ítem 13: Le han solicitado verificar transacciones a través de un enlace de sitio web que aparece en el SMS (Gráfico 13)

Interpretación: Según lo expuesto en la tabla 13, un 54,18% que representa a 188 encuestados, afirmaron que, todos los días han recibido mensajes de texto en donde les han solicitado verificar transacciones a través de un enlace de sitio web. Mientras que, un 31,19% mencionan que, casi todos los días les han llegado un mensaje mediante un enlace de sitio web para dar seguimiento a las operaciones que han realizado y un 0,29% nunca les han solicitado verificar transacciones de su billetera digital. Se infirió que, los comerciantes han sido seleccionados para que les llegue este tipo de SMS fraudulentos que tienen de propósito robar datos e información personal.

Ítem 14: Suele recibir SMS en su móvil simulando ser su banco (Gráfico 14)

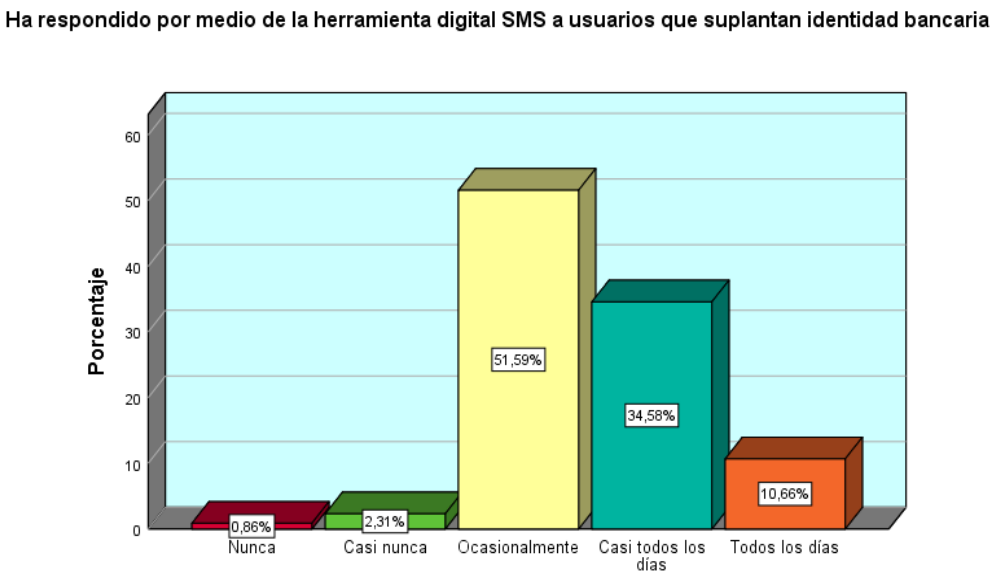
Interpretación: Según lo expuesto en la tabla 14, un gran porcentaje de encuestados que corresponde a 31,12%, ocasionalmente han recibido SMS en su móvil de remitentes desconocidos que simulan ser su banco. Por otro lado, el 29,11% afirmaron que es un problema que tienen casi diario debido a que han recibido mensajes de esa índole, mientras que, un 6,05% que representa a 21 comerciantes no lo han recibido nunca. Se infirió que, a los comerciantes ocasionalmente les llegan SMS con el fin de robar datos personales, haciendose pasar por su banco.

Ítem 15: Ha respondido por medio de la herramienta digital SMS a usuarios que suplantan identidad bancaria (Gráfico 15)

Tabla 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	3	.9	.9	.9
	Casi nunca	8	2.3	2.3	3.2
	Ocasionalmente	179	51.6	51.6	54.8
	Casi todos los días	120	34.6	34.6	89.3
	Todos los días	37	10.7	107	100.0
	Total	**347**	**100.0**	**100.0**	

Fuente: Elaboración propia SPSS



Fuente: Elaboración propia SPSS

Interpretación: Según lo expuesto en la tabla 15, un 51,59% que representa a 179 encuestados, indicaron que, ocasionalmente han respondido por medio de la herramienta digital SMS a usuarios que suplantan su identidad bancaria, mientras que, un 34,58% afirmaron que, casi todos los días han respondido por SMS a usuarios que suplantan a alguna entidad bancaria y un 0,86% que representa a 3 comerciantes no han respondido nunca. Se infirió que, los encuestados han respondido a aquellos mensajes que les ofrecen algún beneficio u ofertas económicos sin verificar la veracidad de los mensajes.

Cabe resaltar que, los resultados alcanzados no fueron realizados con intención de generalizar las respuestas en relación al acto comunicativo en la ciberdelincuencia, de lo contrario, estos fueron tomados en cuenta desde una perspectiva de los comerciantes.

V. DISCUSIÓN

Ya obtenidos los resultados de la investigación, se realizó una recolección de información que se tomó en cuenta de los antecedentes utilizados en el marco teórico. Esto permitió tener una visión más amplia y detallada del tema en cuestión. Además, esta recopilación de datos permitió identificar posibles patrones o tendencias que pueden ser relevantes para el estudio. En resumen, una buena recolección de información es esencial para cualquier investigación seria y rigurosa.

En cuanto al objetivo general y de acuerdo a los resultados obtenidos, este suelen presentarse mediante el uso de diversas técnicas de comunicación como mensajes de supuestos premios de alto valor, links maliciosos, *phishing* y suplantación de entidades bancarias. Según Carreña (2021), las estrategias comunicacionales se refiere a la manipulación de las personas para obtener información confidencial o acceso no autorizado a sistemas protegidos. En este contexto, los ciberdelincuentes utilizan tácticas como el *phishing*, el envío de mensajes engañosos y la suplantación de identidad para obtener acceso a las billeteras digitales de los comerciantes y realizar transacciones fraudulentas.

García (2021), señala que el *phishing* es una técnica común en la ciberdelincuencia, donde los delincuentes envían correos electrónicos o mensajes falsos que parecen legítimos para engañar a los comerciantes y obtener información confidencial. En este estudio, se encontró que muchos comerciantes fueron víctimas de *phishing*, ya que recibieron correos electrónicos fraudulentos que solicitaban información personal o financiera relacionada con sus billeteras digitales.

Además del *phishing*, los delincuentes también utilizan el envío de mensajes engañosos y la suplantación de identidad para acceder a las billeteras digitales de los comerciantes. Según Ghazi y Pontell (2021), los mensajes engañosos, como SMS o mensajes instantáneos, se utilizan para engañar a las personas y obtener información confidencial. En este estudio, se observó que los comerciantes recibían mensajes que aparentaban ser de entidades financieras o proveedores de servicios, pero en realidad eran fraudulentos y buscaban obtener acceso a sus billeteras digitales.

Por otro lado, Ahmad y Jabin (2017), resaltaron que la suplantación de identidad es una estrategia común en la ciberdelincuencia, donde los delincuentes se hacen pasar por otra persona o entidad para obtener información confidencial. En el contexto de las billeteras digitales, los comerciantes pueden ser víctimas de suplantación de identidad a través de correos electrónicos o mensajes que aparentan ser de instituciones financieras o plataformas de pago, solicitando información personal. Este tipo de acto comunicativo engañoso puede resultar en la divulgación de información confidencial y el acceso no autorizado a las billeteras digitales.

De acuerdo con el primer objetivo específico de la investigación, Giannini (2008), informó que la comunicación está aludido a la acción y a procurar algún tipo de respuesta en el otro individuo, en los resultados obtenidos los ciberdelincuentes emplean un lenguaje persuasivo y convincente para engañar a los comerciantes y obtener información confidencial de sus billeteras digitales. Utilizan técnicas de manipulación y persuasión para generar confianza y lograr que los comerciantes compartan datos sensibles.

De acuerdo con lo expuesto por Pons (2018), el 43% de las brechas de seguridad en el sector minorista se deben a la falta de conciencia y educación en materia de seguridad cibernética. Esto demuestra que muchos comerciantes no están familiarizados con las prácticas de seguridad adecuadas, como el uso de contraseñas seguras y la autenticación de dos factores, lo que los hace más vulnerables a los ataques cibernéticos. La negligencia en la implementación de medidas de seguridad también es un problema significativo. Para Alarcón y Barrera (2017), el 60% de las pequeñas empresas no realizaron copias de seguridad de manera regular, lo que pone en riesgo la información almacenada en las billeteras digitales en caso de un ataque cibernético. Además, la misma investigación reveló que solo el 39% de las empresas encuestadas cifraban sus datos de manera consistente, lo que aumenta el riesgo de exposición de información confidencial.

Por otro lado, Chávez, Miranda, Quispe y Robles (2019) afirmaron que, el 55% de las personas confían plenamente en las instituciones financieras y proveedores de servicios para proteger sus datos financieros. Esta confianza ciega puede llevar a los comerciantes a compartir información sensible sin

verificar la autenticidad de las comunicaciones recibidas, lo que los hace susceptibles a ataques de suplantación de identidad y *phishing*.

Con respecto al segundo objetivo específico, se obtuvo que los mensajes del acto comunicativo juegan un papel crucial en la seguridad de la información en las billeteras digitales de los comerciantes. Ghazi y Pontell (2021), mencionaron que el 91% de los ataques cibernéticos comienzan con un correo electrónico de *phishing*. Los ciberdelincuentes utilizan mensajes persuasivos y convincentes que apelan a las emociones y necesidades de los comerciantes. Estos mensajes pueden presentar una apariencia legítima y engañosa, haciéndolos difíciles de detectar como fraudulentos. La construcción cuidadosa del mensaje puede influir en la probabilidad de que los comerciantes compartan información confidencial y en última instancia, comprometen la seguridad de sus billeteras digitales.

La utilización de mensajes de texto como medio de comunicación también puede afectar la seguridad de la información. Mengoa (2021) mencionó en su investigación que el 85% de los mensajes de texto fraudulentos se dirigen a dispositivos móviles. Estos mensajes de texto maliciosos pueden contener enlaces maliciosos o solicitar información personal, lo que puede conducir al acceso no autorizado a las billeteras digitales de los comerciantes.

La influencia de las redes sociales en los mensajes del acto comunicativo también debe considerarse. Según Li, J. Li, Fan y Wang (2022), el 74% de los adultos utilizan las redes sociales y comparten información personal en estas plataformas. Los ciberdelincuentes pueden aprovechar esta información compartida para personalizar sus mensajes fraudulentos, aumentando la efectividad de sus ataques y comprometiendo la seguridad de las billeteras digitales.

Asimismo, la falta de autenticación y verificación en los mensajes del acto comunicativo puede contribuir a la inseguridad de las billeteras digitales. Chávez, Miranda, Quispe y Robles (2019), mencionaron que la gran mayoría de los comerciantes no verificaban la autenticidad de los mensajes recibidos antes de compartir información sensible. Esta falta de verificación permite que los

mensajes falsos o manipulados engañen a los comerciantes y los lleven a divulgar información confidencial.

Por último, en cuanto al tercer objetivo específico, se obtuvo que tiene un impacto significativo en la seguridad de la información en las billeteras digitales de los comerciantes. Según Hamzaoui (2019), se espera que el número de usuarios de servicios de mensajería SMS alcance los 3.5 mil millones para el año 2023. Sin embargo, el SMS también se ha convertido en un objetivo para los ciberdelincuentes debido a su vulnerabilidad inherente.

Uno de los riesgos asociado con el acto comunicativo a través de SMS es la interceptación de mensajes. Según Pons (2018), existen vulnerabilidades en los protocolos de transmisión de mensajes SMS que pueden permitir a los atacantes interceptar y leer los mensajes enviados entre los comerciantes y sus clientes. Esto podría exponer inf ormación confidencial, como contraseñas o códigos de autenticación, comprometiendo la seguridad de las billeteras digitales.

Además, los mensajes SMS también pueden ser utilizados para distribuir enlaces maliciosos. Según García (2021), se estima que el 20% de los mensajes SMS enviados contienen enlaces a sitios web maliciosos. Estos enlaces pueden llevar a los comerciantes a páginas falsas diseñadas para robar información personal o instalar malware en sus dispositivos, lo que representa un riesgo para la seguridad de las billeteras digitales. La falta de cifrado en los mensajes SMS es otro aspecto preocupante en términos de seguridad de la información. Según López y Palomino (2021), la mayoría de los mensajes SMS se transmiten en texto claro, lo que los hace susceptibles a ser interceptados y leídos por terceros malintencionados. Esto representa un peligro potencial para la confidencialidad de la información transmitida a través de los mensajes SMS en relación con las billeteras digitales.

La investigación también ha identificado la falta de autenticación en los mensajes SMS como un factor de riesgo. Ghazi y Pontell (2021), mencionan que el 43% de los mensajes SMS no tienen una autenticación adecuada, lo que significa que los comerciantes no pueden estar seguros de la legitimidad de los mensajes recibidos. Esto puede llevar a que los comerciantes compartan información confidencial con atacantes disfrazados de remitentes legítimos, comprometiendo la seguridad de sus billeteras digitales. Por otro lado, la respuesta del usuario es otro aspecto crítico, dado que los ciberdelincuentes emplean técnicas de manipulación emocional y urgencia para generar respuestas rápidas de los comerciantes. Por ende, la construcción cuidadosa del mensaje influye en la probabilidad de que los comerciantes respondan a equellos mensajes sin cuestionar su autenticidad exponiendolos a riesgos de ciberdelincuencia.

Como debilidades encontradas durante el proceso de la investigación fue la escasa referencias de tesis, artículos científicos tanto nacionales como internacionales, por otro lado las referencias con el enfoque cuantitativo eran pocas, también al hacerse las búsquedas por medio de las palabras claves se evindencio vacíos de conocimiento en cuestión a la información buscada.

En cuestión a las fortalezas de la investigación, habiendo evidenciado la escasez de referencias sobre el tema de la investigación acto comunicativo en la ciberdelincuencia de una billetera digital, se pudo dar una nueva mirada con esta investigación y así con los datos obtenidos los comerciantes tendrán en cuenta el uso seguro de la billetera digital y la identificación de los mensajes maliciosos.

VI. CONLUSIONES

1. Como conclusión general, se determinó que el acto comunicativo en la ciberdelincuencia de una billetera digital se presenta mediante el uso de estrategias comunicativas de persuasión, manipulación y engaño en los mensajes por parte de los ciberdelincuentes, utilizando los canales de comunicación como el SMS y el phishing instantáneo para establecer contacto con los comerciantes y obtener acceso no autorizado a sus billeteras digitales.

2. Como primera conclusión específica, se determinó que los procesos del acto comunicativo en la ciberdelincuencia de una billetera digital afecta de manera significativa en la seguridad de la información en los comerciantes llevándose a cabo a través de técnicas comunicativas, como el uso de un lenguaje verbal adecuado y la plataforma digital por la cuál cometen el fraude cibernético, además, el 56,20% de los encuestados, mencionaron qué, por medio del WhatsApp ocasionalmente han sido víctimas de ciberdelincuentes.

3. Como segunda conclusión específica, se determinó que los mensajes del acto comunicativo afecta directamente en la seguridad de la información de una billetera digital en los comerciantes, donde la construcción cuidadosa del mensaje por parte de los ciberdelincuentes, la interpretación del mensaje por parte de los comerciantes y la credibilidad del contenido son factores que influyeron en la exposición de riesgos cibernéticos en su billetera digital de los comerciantes.

4. Como tercera conclusión específica, se determinó que el acto comunicativo a través de la herramienta digital de SMS afecta de manera significativa en la seguridad de la información de una billetera digital en los comerciantes, debido a que la finalidad de contenido engañosa que emiten los delincuentes y la respuesta del usuario ante los textos recibidos son factores claves que los ciberdelincuentes aprovechan para obtener acceso no autorizado a las billeteras digitales.

VII. RECOMENDACIONES

Se recomienda a los futuros investigadores explorar nuevas formas de aplicar la metodología de investigación, donde los investigadores deberían estar abiertos a la exploración de nuevas técnicas y enfoques para aplicar la metodología de investigación. Esto puede implicar la utilización de las nuevas tecnologías, como el análisis de datos en redes sociales, para obtener una visión más profunda en los resultados.

Se sugiere considerar otro tipo y tamaño de población debido a que la población es un factor crítico en la investigación cuantitativa, ya que influye en la precisión y generalización de los resultados. Es importante asegurarse de que la muestra sea lo suficientemente grande como para detectar diferencias significativas y representativas de la población objetivo.

Se recomienda que los futuros investigadores tomen en cuenta la importancia de la validez y confiabilidad en la recolección de datos en investigaciones cuantitativas. Para ello, se sugiere utilizar instrumentos estandarizados ya validados y confiables, así como también verificar la consistencia del instrumento mediante el análisis de la confiabilidad.

Se recomienda a los investigadores explorar a detalle los antecedentes que utilizarán en su marco teórico, porque mediante ello se analizará el planteamiento del problema, la justificación y las preguntas de la investigación en la cual permitirá tener una base sólida de autores que respalden el tema vinculado a la problemática de la investigación. También se sugiere seguir a pie el formato de las normas APA en cuanto a la citas de cada antecedente.

REFERENCIAS

Ahmad, M & Jabin, S. (2017*). A sneak into the Devils Colony- Fake profiles in online social networks.* Arxis. 2(8), 31.

https://arxiv.org/abs/1705.09929

Alarcon, D. y Barrera, J.(2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016. [Tesis de maestría].* Universidad privada Norbert Wiener. https://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20-%20%20Barrera%20Bar%C3%B3n%2C%20Javier%20Antonio.pdf?sequen ce=1&isAllowed=y

Ampuero M, & Smith, C. (2017). La eficacia de la estrategia de comunicación de la campaña de sensibilización *"Escuela Segura" del Municipio de Comas, en los alumnos del 5to grado de secundaria de la institución educativa "Estados Unidos*" en la ciudad de Lima en el año 2017. *Universidad César Vallejo*.

https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=alma991002877984607001&context=L&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_and_CI&adaptor=Local%20Search%20Engine&tab=Everything&query=any,contains,eficacia%20estrategia&offset=0

Arias, J & Covinos, M. (2021). Diseño y metodología de la investigación.

https://www.researchgate.net/publication/352157132_DISENO_Y_METOD

Arias, J. (2020). *Proyecto de tesis guía para la elaboración. (1.ª ed.)*. Depósito Legal en la Biblioteca Nacional. https://www.studocu.com/co/document/universidad-delvallecolombia/comprension-y-produccion-de-textos-examen/ariasgonzalesproyecto-de-tesis-libro/13566353

Avello, R., López, R., Palmero, D., Sánchez, S. y Quintana, M. (2019). *Validación de instrumentos como garantía de la credibilidad en las investigaciones científicas*. Revista Cubana de Medicina Militar, 48(2), 441-450. http://www.revmedmilitar.sld.cu/index.php/mil/article/view/390/331

Baldera, A. (2021). *Publicidad digital y posicionamiento de la aplicación "Yape" en los microempresarios de San Juan de Lurigancho. Lima, 2021*. Universidad César Vallejo.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/87503/Baldera_HAA-SD.pdf?sequence=1&isAllowed=y

BCP se pronuncia tras denuncia de robos en YAPE y advierte modalidad de estafa. (17.12.2020). Líbero

https://libero.pe/ocio/1599003-bcp-robos-yape-denuncias-pronunciamiento-diferentes-denuncias-estafas-via-yape-consumos-erroneos-tarjetas-credito-diciembre-2020

Bravo, T. y Valenzuela, S. (2019). *Desarrollo de instrumentos de evaluación: Cuestionarios. Centro UC.*

https://www.inee.edu.mx/wp-content/uploads/2019/08/P2A355.pdf

Carrera Peña, I. d. R. (2021). *Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021. [Tesis para obtener el grado académico de: Maestra en Derecho Penal y Procesal Penal*]. Universidad César Vallejo.

https://hdl.handle.net/20.500.12692/71492

Chavez, J., Miranda, E., Quispe, N. y Robles, S. *Factores que influyen en la intención de usos de tecnología de medios de pago móvil en negocios minoristas en Lima Metropolitana. [Tesis para obtener el grado de Maestro en Marketing]. Universidad ESAM.* https://repositorio.esan.edu.pe/bitstream/handle/20.500.12640/1742/2019_MAM_17-2_06_T.pdf?sequence=1&isAllowed=y

Ciberdelincuencia en el mundo. (2020, 17, febrero). Adaptixnetworks.

https://www.adaptixnetworks.com/ciberdelincuencia-en-elmundo/#:~:text=La%20ciberdelincuencia%20ataca%20a%20todos,que%20 m%C3%A1s%20invierte%20en%20protecci%C3%B3n

Código del Comercio, Libro Primero, Art. 1. (1902) https://scc.pj.gob.pe/wps/wcm/connect/3c0d35804d90aee08507f5db524a342a/C%C3%B3digo+de+Comercio.pdf?MOD=AJPERES&CACHEID=3c0d35804d90aee08507f5db524a342a#:~:text=Art%C3%ADculo%201%C2%BA.,con%20arreglo%20a%20este%20C%C3%B3digo.

Concytec, N. (2018). Reglamento de calificación, clasificación y registro de los investigadores del sistema nacional deficiencia, tecnología e innovación tecnológica.

https://portal.concytec.gob.pe/images/renacyt/reglamento_renacyt_version_final.pdf

Cordero, N. (2021) *La Ciberdelincuencia [Trabajo Fin de Máster. Universidad de Alcalá].*

http://hdl.handle.net/10017/49563

*“Falso Yape”: ¿Cómo funciona esta nueva modalidad de estafa a comerciantes? (*09.06.2022). La República.

https://larepublica.pe/sociedad/2022/07/06/falso-yape-como-funciona-esta-nueva-modalidad-de-estafa

García Sánchez, E. (2021). *Delitos contra el patrimonio económico, el phishing en Colombia, aproximación criminológica. [Tesis de grado Maestría]*. Universidad Nacional de Colombia.

https://repositorio.unal.edu.co/handle/unal/82270

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). *Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders,* 16(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224

Giannini, H. (2008). Experiencia moral y accion comunicativa. Revista de Filosofía[Chile],64,5. https://link.gale.com/apps/doc/A209405019/IFME?u=univcv&sid=bookmark-IFME&xid=f85a19e4

Guevara Alban, G. P., Verdesoto Arguello, A. E., & Castro Molina, N. E. (2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción*). *RECIMUNDO*, *4*(3), 163-173. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Hamzaoui, M. E., & Bensalah, F. (2019). *Cybercrime in Morocco. International Journal of Advanced Computer Science & Applications,* 10(4).

https://doi.org/10.14569/IJACSA.2019.0100457

Hernández-Ávila, C. E., & Carpio Escobar, N. A. (2019). *Introducción a los tipos de muestreo. Alerta, Revista científica Del Instituto Nacional De Salud*, 2(1 (enero-junio), 75–79.

https://doi.org/10.5377/alerta.v2i1.7535

Hernàndez, O. (2021). *"Aproximación a los distintos tipos de muestreo no probabilísticos que existen". Revista Cubana de Medicina General Integral. 37(3).*

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21252021000300002

Hernández Sampieri, R (2014). Metodología de la Investigación. México D.F., México: Sexta Edición. Editorial McGraw-Hill. Recuperado de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-lainvestigacion-sexta-edicion.compressed.pdf

Li, Y., Li, J., Fan, Q. and Wang, Z. (2022), *"Cybercrime's tendencies of the teenagers in the COVID-19 era: assessing the influence of mobile games, social networks and religious attitudes",* Kybernetes, Vol. ahead-of-print No. ahead-of-print.

https://doi.org/10.1108/K-07-2021-0582

López, A. y Palomino, J. (2021). *Factores que Influyen en la Intención de Uso de Tecnología Móvil para Realizar Transacciones de Dinero. [Tesis para obtener el grado de magíster en gerencia de tecnología de información*]. Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/20916/Factores%20que%20Influyen%20en%20la%20Intenci%C3%B3n%20de%20Uso%20de%20Tecnolog%C3%ADa%20M%C3%B3vil%20para%20Realizar%20Transacciones%20de%20Dinero%20-%20LOPEZ.pdf?sequence=1&isAllowed=y

López, P. y Fachelli, S. (2015). *Metodología de la investigación social cuantitativa. (1ª ed.)*

https://ddd.uab.cat/pub/caplli/2016/163567/metinvsoccua_a2016_cap23.pdf

Matas, A. (2018). *Diseño del formato de escalas tipo Likert: un estado de la cuestión. Revista Electrónica de Investigación Educativa,* 20(1), 38-47. https://doi.org/10.24320/redie.2018.20.1.1347

Mengoa Valdivia, M. M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú. [Tesis para obtener el título profesional de Abogada]*. Universidad Cèsar Vallejo. https://hdl.handle.net/20.500.12692/62379

Ministerio Público: denuncias por delitos informáticos aumentaron en 92.9 % en el último año. (04.09.2022).RRP Noticias.

https://rpp.pe/peru/actualidad/ministerio-publico-denuncias-por-delitosinformaticos-aumentaron-en-929-en-el-ultimo-ano-noticia-1429523?ref=rpp

Ministerio de Justicia y Derechos Humanos (2019). Constitución Política del Perú. Recuperado de

http://www.minjus.gob.pe/wp-content/uploads/2017/04/Constitucion-Politica-del-Peru.pdf

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry*. Current Psychiatry Reports, 23(4), 18–18.https://doi.org/10.1007/s11920-021-01228-w

Moya, C. (2009). *Aproximación pragmática a los conceptos de "acto de habla" y de "acción comunicativa".* Desde el jardín de Freud: revista de psicoanálisis, 9, 229243.

https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_doaj_primary_oai_doaj_org_article_0089c7d78fc64671962d9dc9ed112c78&context=PC&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,accion%20comunicativa&sortby=rank&offset=20

Otzen, T. & Manterola, C. (2017). *Sampling Techniques on a population study. Int.J.Morphol*, 35 (1). 227-232.

http://www.intjmorphol.com/wpcontent/uploads/2017/04/art_37_351.pdf

Peña, S. (2017). *Análisis de datos.(1ª ed.) Fondo editorial Areandino*. Bogotá.

https://core.ac.uk/download/pdf/326425169.pdf

Pons, V. (2018). *Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional. [Tesis doctoral].* Universidad Nacional de Educación a Distancia.

http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSocVpons/PONS_GAMON__Vicente_Tesis.pdf

Rios, E. Páez, H. & Barbos, H. (2020). *Estrategias de comunicación: diseño, ejecución y seguimiento*. REDIPE.

https://redipe.org/wp-content/uploads/2020/10/Libro-estrategias-decomunicacion.pdf

Rios, O., & Christou, M. (2010). Más allá del lenguaje sexista: Actos comunicativos en las relaciones afectivo-sexuales de los y las adolescentes. *Revista Signos, Suppl.Supplement 2, 43*, 311. https://www.proquest.com/scholarly-journals/más-allá-del-lenguaje-sexista-actos-comunicativos/docview/1017674317/se-2

Risco, A. (2020). *Nota Académica 5 (18.04.2021) .Justificación de la Investigación.* https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10821/Nota%20Acad%C3%A9mica%205%20%2818.04.2021%29%20%20Justificaci%C3%B3n%20de%20la%20Investigaci%C3%B3n.pdf?sequence=4&isAllowed=y#:~:text=Justificaci%C3%B3n%20te%C3%B3rica%20Implica%20describir%20cu%C3%A1les,el%20punto%20de%20vista%20te%C3%B3rico.

Romero, L. (2012). *Aplicabilidad de técnicas de desinformación en la gestión comunicacional de crisis. [Trabajo fin de Máster]*. Universidad de Almería. https://core.ac.uk/download/pdf/143454714.pdf

Ventura, M. A. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020 [Tesis de licenciatura, Universidad Privada del Norte]*. Repositorio de la Universidad Privada del Norte.

https://hdl.handle.net/11537/28942

ANEXOS

ANEXO 1

Tabla 6

Matriz de Operacionalización de la Variable

c	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Escala de medición
Acto comunicativo	Los actos comunicativos se dan en el uso del lenguaje verbal y no verbal, donde las personas seleccionan una expresión lingüística comprensible en donde puedan comprenderse el uno al otro. Todos estos elementos funcionan en conjunto para interpretar un mensaje como parte de un pensamiento y una narrativa, con el fin de comunicar exactamente lo que se quiere expresar tomando en cuenta el contexto en el que ocurre la comunicación (Ríos y Christou, 2010).	El presente ámbito temático se medirá con un cuestionario a partir de un análisis de datos de acuerdo a las 3 dimensiones propuestas, en razón al acto comunicativo.	Procesos comunicativos	Lenguaje verbal	1, 2	Likert Nunca (1) Casi nunca (2) Ocasionalmente (3) Casi todos los días (4) Todos los días (5)
				Whatsapp	3, 4	
				Contenido	5, 6	
			Mensaje	Construcción del mensaje	7, 8	
				Interpretación del mensaje	9, 10	
				Credibilidad del contenido	11, 12	
			Herramienta digital SMS	Finalidad de contenido	13, 14	
				Respuesta del usuario	15	

Fuente: Elaboración propia.

ANEXO 2

Tabla 7

Matriz de Consistencia

<table>
<tr><td colspan="2">TÍTULO</td><td colspan="4">Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023</td></tr>
<tr><td colspan="2">AUTORES</td><td colspan="4">Chujutalli Aguilar, Nilda Eunice
Retuerto Fernandez Regina Gabriela</td></tr>
<tr><td>PROBLEMA GENERAL</td><td>OBJETIVO GENERAL</td><td>VARIABLE</td><td>DIMENSIONES</td><td>INDICADORES</td><td>METODOLOGÍA</td></tr>
<tr><td>¿Cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023?</td><td>Determinar cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023.</td><td rowspan="3"></td><td rowspan="2">Procesos comunicativos</td><td rowspan="2">Lenguaje verbal
WhatsApp
Contenido</td><td rowspan="3">Enfoque:
Cuantitativo

Tipo:
Básica

Diseño:
No experimental-transversal

Nivel:</td></tr>
<tr><td>PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td></tr>
<tr><td>¿Cómo se presenta el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023?</td><td>Determinar cómo los procesos del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023.</td><td>Mensaje</td><td>Construcción del mensaje
Interpretación del mensaje</td></tr>
</table>

PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**ACTO COMUNICATIVO**			Descriptiva **Técnica:** Encuesta **Instrumento:** Cuestionario
¿Cómo los mensajes del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023?	Determinar cómo los mensajes del acto comunicativo pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023.			• Credibilidad del contenido	
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**		**Herramienta digital SMS**	• Finalidad de contenido • Respuesta del usuario	
¿Cómo el acto comunicativo a través de la herramienta digital de SMS pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023?	Determinar cómo el acto comunicativo a través de la herramienta digital de SMS pueden afectar la seguridad de la información de las billeteras digitales en comerciantes de un mercado del distrito de Carabayllo, 2023.				

Fuente: Elaboración propia

ANEXO 3:

Instrumento

Encuesta sobre el acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023

Estimado emprendedor (a) este cuestionario está conformado por una serie de preguntas cuyo objetivo es recolectar datos acerca del acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, las cuales deberá leer atentamente y responder con sinceridad. Garantizamos a usted que sus respuestas son confidenciales y solo se usarán con propósitos académicos. Agradecemos sinceramente su participación y le invitamos a responder de acuerdo a la siguiente:

Escala de medición Likert	
Nunca	1
Casi nunca	2
Ocasionalmente	3
Casi todos los días	4
Todos los días	5

Cuestionario						
ACTO COMUNICATIVO						
Nro.	Procesos comunicativos	1	2	3	4	5
1	Ha transmitido información bancaria a través de mensajes escritos					
2	Ha transmitido información bancaria por medio de mensajes de audio					
3	Recibe mensajes de transferencia bancaria por medio del WhatsApp					
4	Ha sido víctima de pago por supuestos clientes que muestran captura por medio del WhatsApp					
5	Ha recibido un monto depositado de diferente color en su aplicación					
6	Ha recibido una compra de un QR falso en su billetera digital					
	Mensaje	1	2	3	4	5
7	Ha recibido mensajes de propuestas diciéndole que al pagar usted aumenta sus probabilidades de obtener su premio ganador					
8	Por medio de los mensajes ha recibido enlaces o un archivo adjunto diciendo que se ganó un premio de alto precio (lotería, IPad, carro nuevo, etc.)					
9	Reconoce las señales de un mensaje de texto fraudulento					
10	Identifica los mensajes de texto que se hacen pasar por una entidad financiera					
11	Brinda información personal por medio de mensajes a personas o entidades desconocidas					
12	Responde o acepta mensajes de texto de remitentes desconocidos que ofrecen algún beneficio					
	Herramienta digital SMS	1	2	3	4	5
13	Le han solicitado verificar transacciones a través de un enlace de sitio web que aparece en el SMS					
14	Suele recibir SMS en su móvil simulando ser su banco					
15	Ha respondido por medio de la herramienta digital SMS a usuarios que suplantan identidad bancaria					

ANEXO 4:

MATRIZ EVALUACIÓN POR JUICIO DE EXPERTOS

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres del experto: OBLITAS CARREÑO JOOHN RAÚL
Título y/o Grado:

Ph. D ( )	Doctor ( )	Magister (x)	Licenciado ( )	Otros. ( ) Especifique

Universidad que labora:

Fecha:

TÍTULO DE LA INVESTIGACIÓN

Mediante la tabla para evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con "x" en las columnas de SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre clima organizacional.

		APRECIA		
ITEMS	PREGUNTAS	SI	NO	OBSERVACIONES
1	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	x		
2	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	x		
3	¿El instrumento de recolección de datos, facilitará el logro de los objetivos de la investigación?	x		
4	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	x		
5	¿La redacción de las preguntas es con sentido coherente?	x		
6	¿Cada una de las preguntas del instrumento de medición, se relacionan con cada uno de los elementos de los indicadores?	x		
7	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	x		
8	¿Del instrumento de medición, los datos serán objetivos?	x		
9	¿El instrumento de medición será accesible a la población sujeto de estudio?	x		
10	¿El instrumento de medición es claro, preciso, y sencillo para que contesten y de esta manera obtener los datos requeridos?	x		
	TOTAL			

SUGERENCIAS:
Firma del experto:

Nombres y apellidos:

SEGUNDO VALIDADOR:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres del experto: Ronny Rafael Rojas Rojas
Título y/o Grado:

Ph. D ( )	Doctor ( )	Magister (X)	Licenciado ( )	Otros. ( ) Especifique

Universidad que labora: Universidad César Vallejo

Fecha: 22 de abril de 2023

TÍTULO DE LA INVESTIGACIÓN

Mediante la tabla para evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con "x" en las columnas de SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre clima organizacional.

		APRECIA		
ITEMS	PREGUNTAS	SI	NO	OBSERVACIONES
1	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	x		Aunque hay que cambiar algunas preguntas.
2	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	x		
3	¿El instrumento de recolección de datos, facilitará el logro de los objetivos de la investigación?	x		
4	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	x		
5	¿La redacción de las preguntas es con sentido coherente?		x	
6	¿Cada una de las preguntas del instrumento de medición, se relacionan con cada uno de los elementos de los indicadores?		x	
7	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	x		
8	¿Del instrumento de medición, los datos serán objetivos?	x		
9	¿El instrumento de medición será accesible a la población sujeto de estudio?	x		
10	¿El instrumento de medición es claro, preciso, y sencillo para que contesten y de esta manera obtener los datos requeridos?	x		
	TOTAL			

SUGERENCIAS: Hay que estudiar la teoría sobre los indicadores para desarrollar las preguntas.
Firma del experto:

Nombres y apellidos:

TERCER VALIDADOR:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres del experto: Mariano Vargas Arias
Título y/o Grado: LIC. CC.CC. / MGTR DOCENCIA UNIVERSITARIA

Ph. D ( )	Doctor ( )	Magister (X)	Licenciado ( )	Otros. ( ) Especifique

Universidad que labora: UCV

Fecha: 26/04/2023

TÍTULO DE LA INVESTIGACIÓN

Mediante la tabla para evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con "x" en las columnas de SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre clima organizacional.

		APRECIA		
ITEMS	PREGUNTAS	SI	NO	OBSERVACIONES
1	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
2	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
3	¿El instrumento de recolección de datos, facilitará el logro de los objetivos de la investigación?	X		
4	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
5	¿La redacción de las preguntas es con sentido coherente?	X		
6	¿Cada una de las preguntas del instrumento de medición, se relacionan con cada uno de los elementos de los indicadores?	X		
7	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
8	¿Del instrumento de medición, los datos serán objetivos?	X		
9	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
10	¿El instrumento de medición es claro, preciso, y sencillo para que contesten y de esta manera obtener los datos requeridos?	X		
	TOTAL			

SUGERENCIAS:
Firma del experto:

Mariano Vargas Arias

ANEXO 6

RESULTADOS DE COEFICIENTE V DE AIKEN

Tabla 8

Resultados de coeficiente V de Aiken

PREGUNTAS	PRIMER EXPERTO	SEGUNDO EXPERTO	TERCER EXPERTO	SUMA	V DE AIKEN
ÌTEM 1	1	1	1	3	1
ÌTEM 2	1	1	1	3	1
ÌTEM 3	1	1	1	3	1
ÌTEM 4	1	1	1	3	1
ÌTEM 5	1	1	0	2	0,666667
ÌTEM 6	1	1	0	2	0,666667
ÍTEM 7	1	1	1	3	1
ÍTEM 8	1	1	1	3	1
ÍTEM 9	1	1	1	3	1
ÍTEM 10	1	1	1	3	1
ÍTEM 11	1	1	1	3	1
ÍTEM 12	1	1	1	3	1
ÍTEM 13	1	1	1	3	1
ÍTEM 14	1	1	1	3	1
ÍTEM 15	1	1	1	3	1

0,955556

Fuente: Elaboración propia

El coeficiente V de Aiken es 0,95 esto quiere decir que el instrumento de recolección de datos tiene excelente validez.

$$V = \frac{S}{N(C-1)}$$

Dónde: S: La suma de si

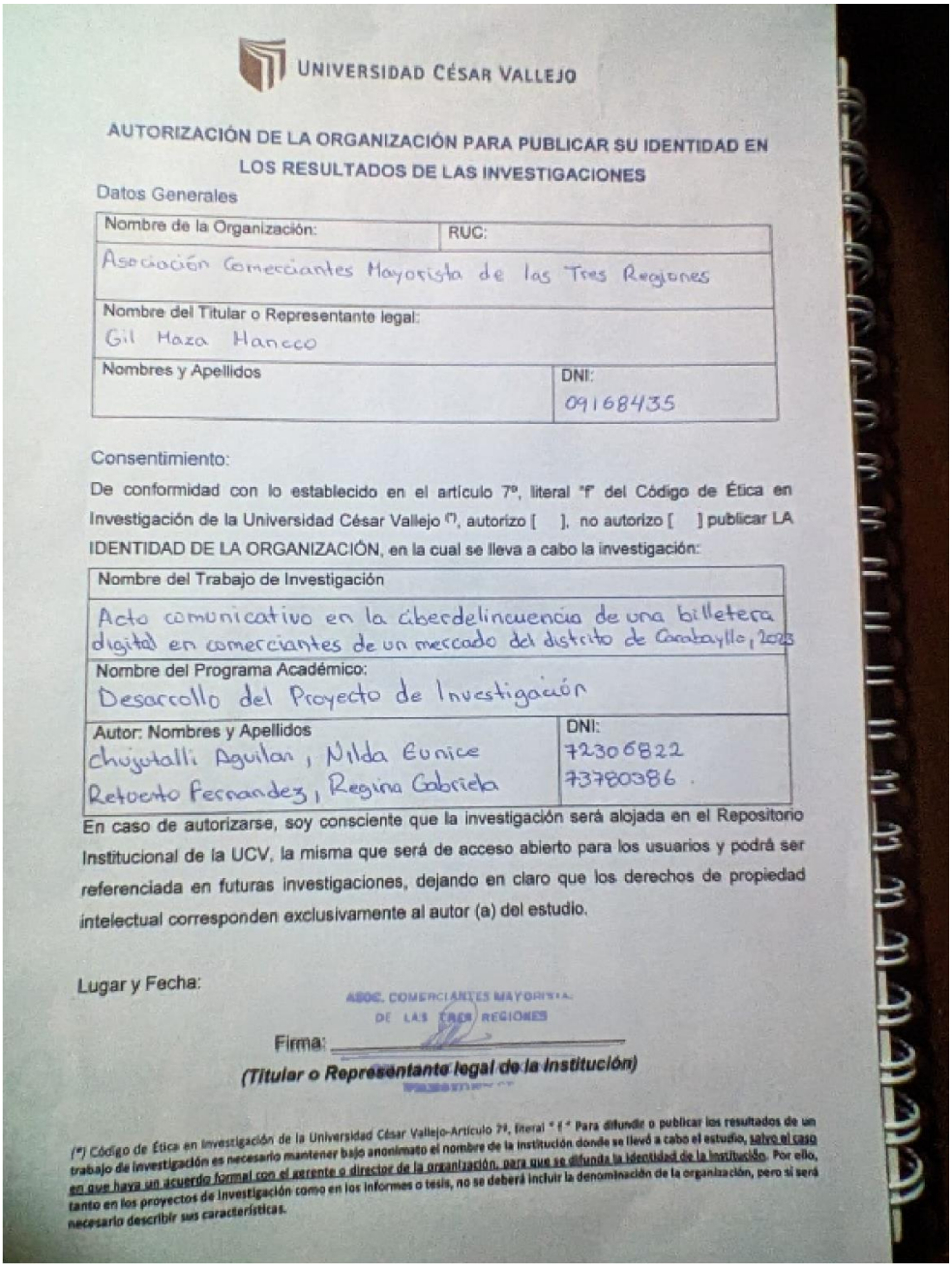
SI: Valor asignado por el juez i

N: Número de Jueces

C: Número de valores de la escala de valoración

ANEXO 7

AUTORIZACIÓN DE LA ORGANIZACIÓN



UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA ORGANIZACIÓN PARA PUBLICAR SU IDENTIDAD EN LOS RESULTADOS DE LAS INVESTIGACIONES

Datos Generales

Nombre de la Organización:	RUC:
Asociación Comerciantes Mayorista de las Tres Regiones	
Nombre del Titular o Representante legal: Gil Haza Hancco	
Nombres y Apellidos	DNI: 09168435

Consentimiento:

De conformidad con lo establecido en el artículo 7º, literal "f" del Código de Ética en Investigación de la Universidad César Vallejo (*), autorizo [ ], no autorizo [ ] publicar LA IDENTIDAD DE LA ORGANIZACIÓN, en la cual se lleva a cabo la investigación:

Nombre del Trabajo de Investigación	
Acto comunicativo en la ciberdelincuencia de una billetera digital en comerciantes de un mercado del distrito de Carabayllo, 2023	
Nombre del Programa Académico: Desarrollo del Proyecto de Investigación	
Autor: Nombres y Apellidos Chujutalli Aguilar, Nilda Eunice Retuerto Fernandez, Regina Gabriela	DNI: 72306822 73780386

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente al autor (a) del estudio.

Lugar y Fecha:

ASOC. COMERCIANTES MAYORISTAS DE LAS TRES REGIONES

Firma: _____

(Titular o Representante legal de la institución)

(*) Código de Ética en Investigación de la Universidad César Vallejo-Artículo 7º, literal " f " Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución. Por ello, tanto en los proyectos de investigación como en los informes o tesis, no se deberá incluir la denominación de la organización, pero sí será necesario describir sus características.

ANEXO 8

RESULTADO DEL ALFA DE CRONBACH

Tabla 9

Resumen de procesamiento de casos

		N	%
Casos	Válido	15	100,0
	Excluido[a]	0	,0
	Total	15	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
0,786	15

Interpretación:

El instrumento de la variable acto comunicativo, el cual cuenta con un total de 15 ítems, arrojó un coeficiente de Cronbach del 0.786, en donde, según la escala de valoración de fiabilidad de ítems se ubica en una valoración aceptable, lo que significa que el cuestionario puede ser aplicado a la muestra de estudio.

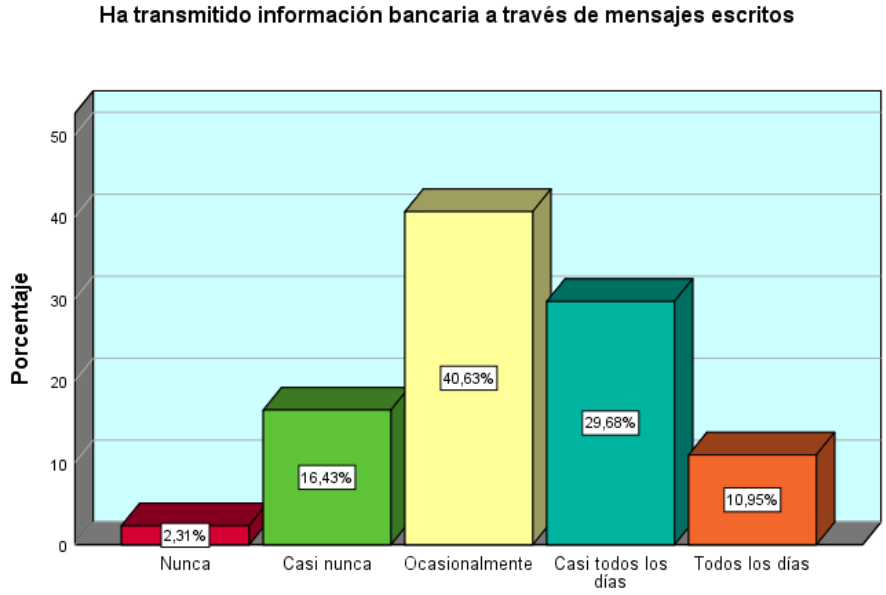
ANEXO 10

RESULTADOS TABLAS Y GRÁFICAS

TABLAS POR CADA ÍTEM

Ítem 1

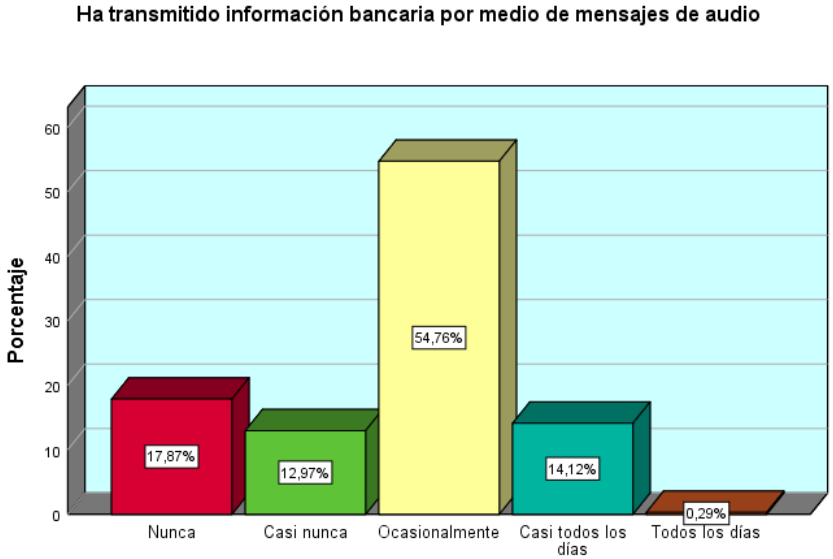
1.-Ha transmitido información bancaria a través de mensajes escritos (Gráfico 1)



Fuente: Elaboración propia SPSS

Ítem 2

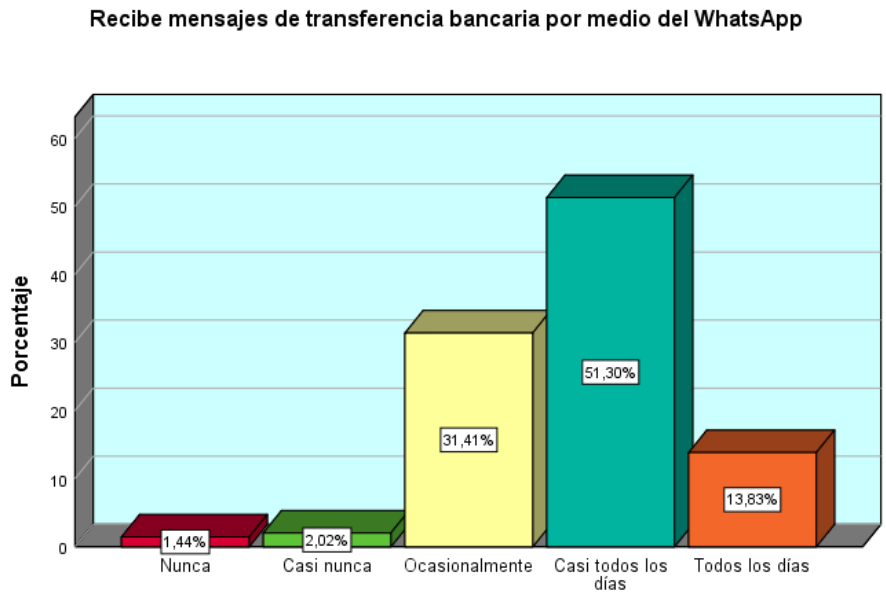
2.-Ha trasmitido información bancaria por medio de mensajes de mensajes de audio (Gráfico 2)



Fuente: Elaboración propia SPSS

Ítem 3

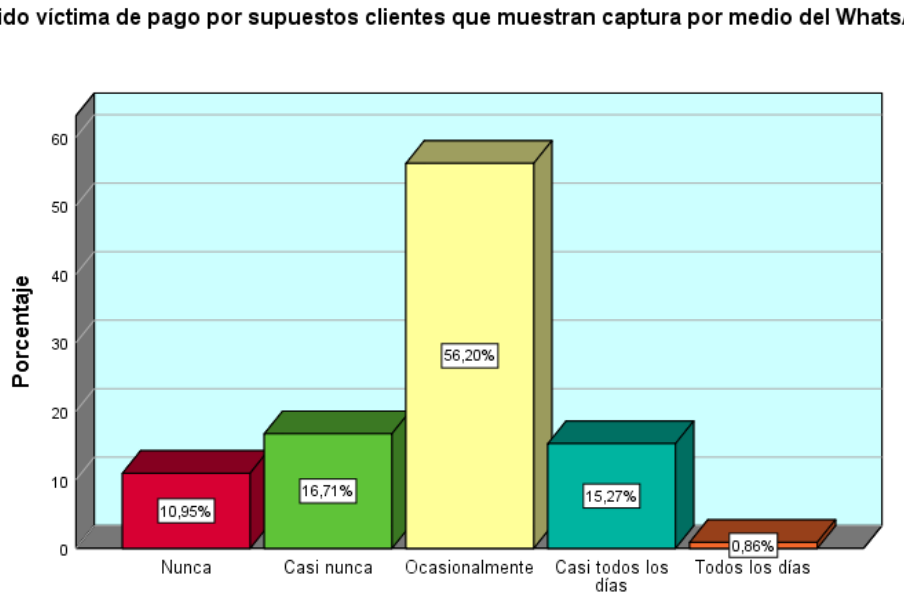
3.-Recibe mensajes de transferencia bancaria por medio del WhatsApp (Gráfico 3)



Fuente: Elaboración propia SPSS

Ítem 4

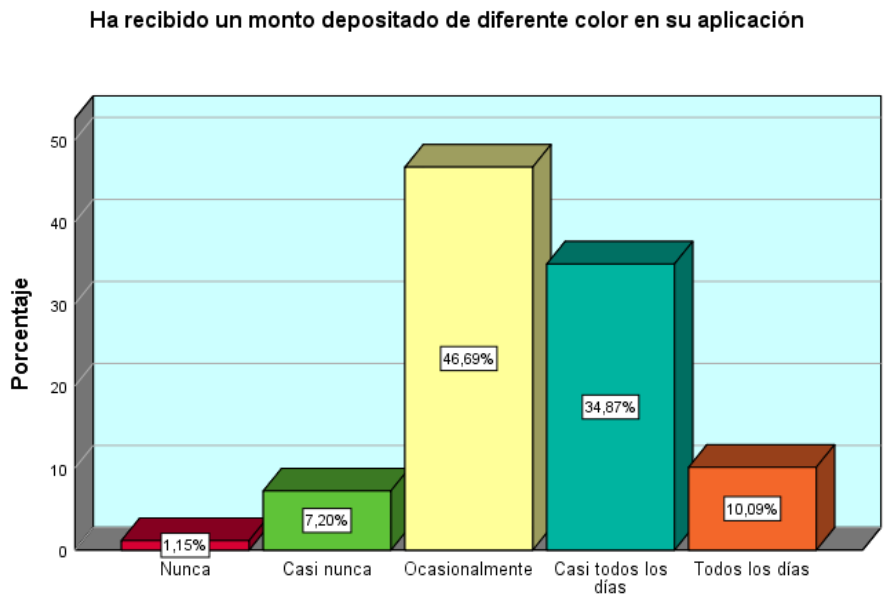
4.- Ha sido víctima de pago por supuestos clientes que muestran captura por medio del WhatsApp (Gráfico 4)



Fuente: Elaboración propia SPSS

Ítem 5

5.- Ha recibido un monto depositado de diferente color en su aplicación (Gráfico 5)

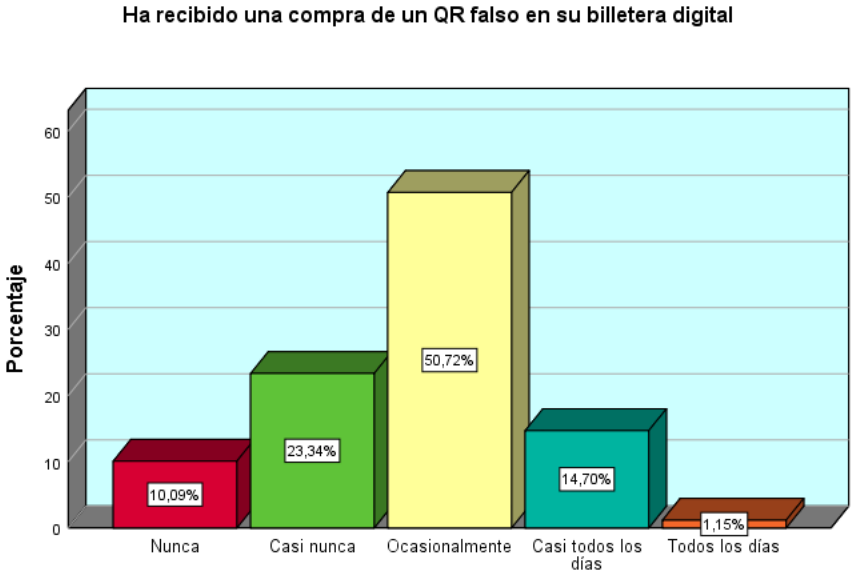


.

Fuente: Elaboración propia SPSS

Ítem 6

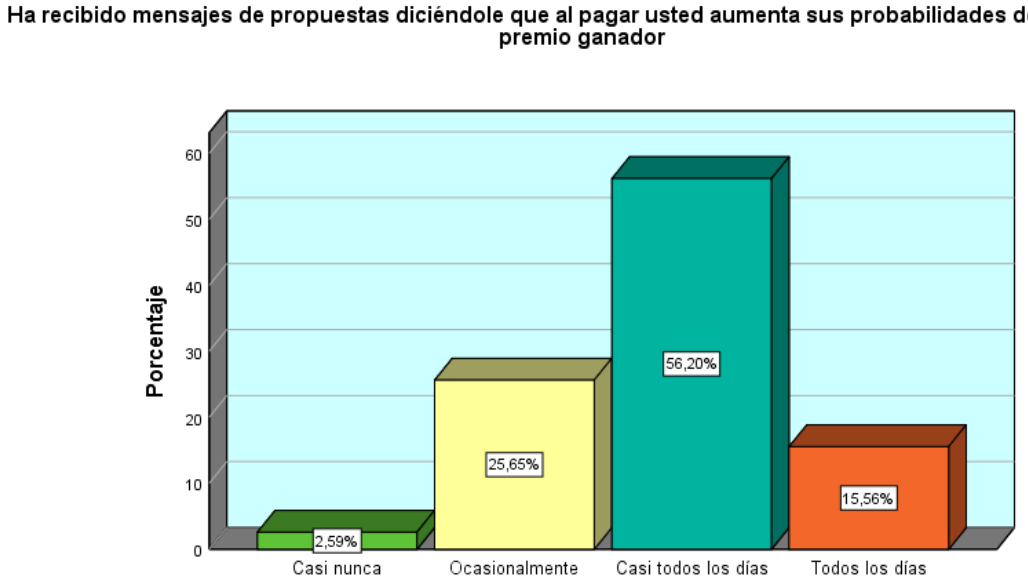
6.- Ha recibido una compra de un QR falso en su billetera digital (Gráfico 6)



Fuente: Elaboración propia SPSS

Ítem 7

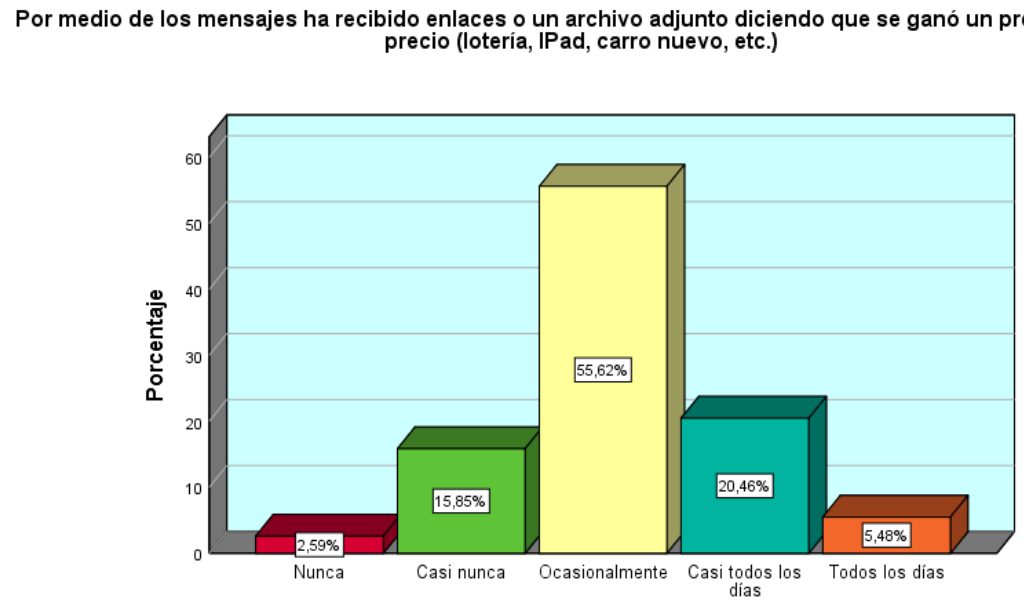
7.- Ha recibido mensajes de propuestas diciéndole que al pagar usted aumenta sus probabilidades de obtener su premio ganador (Gráfico 7)



Fuente: Elaboración propia SPSS

Ítem 8

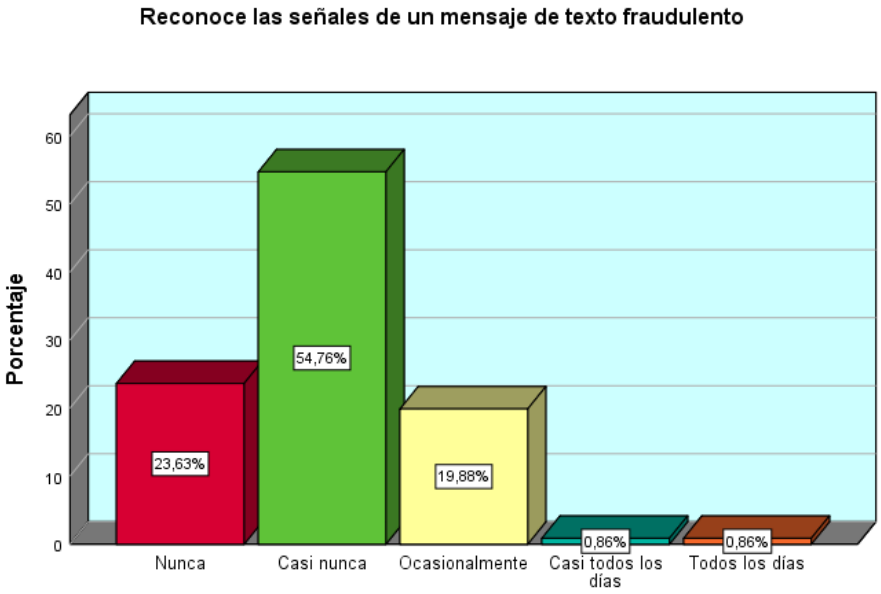
8.- Por medio de los mensajes ha recibido enlaces o un archivo adjunto diciendo que se ganó un premio de alto precio (lotería, IPad, carro nuevo, etc.) (Gráfico 8)



Fuente: Elaboración propia SPSS

Ítem 9

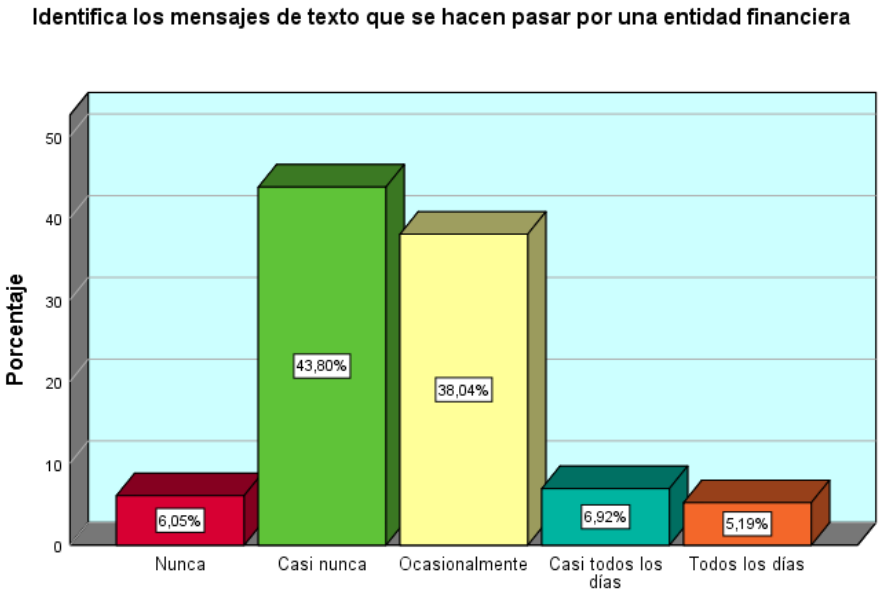
9.- Reconoce las señales de un mensaje de texto fraudulento (Gráfico 9)



Fuente: Elaboración propia SPSS

Ítem 10

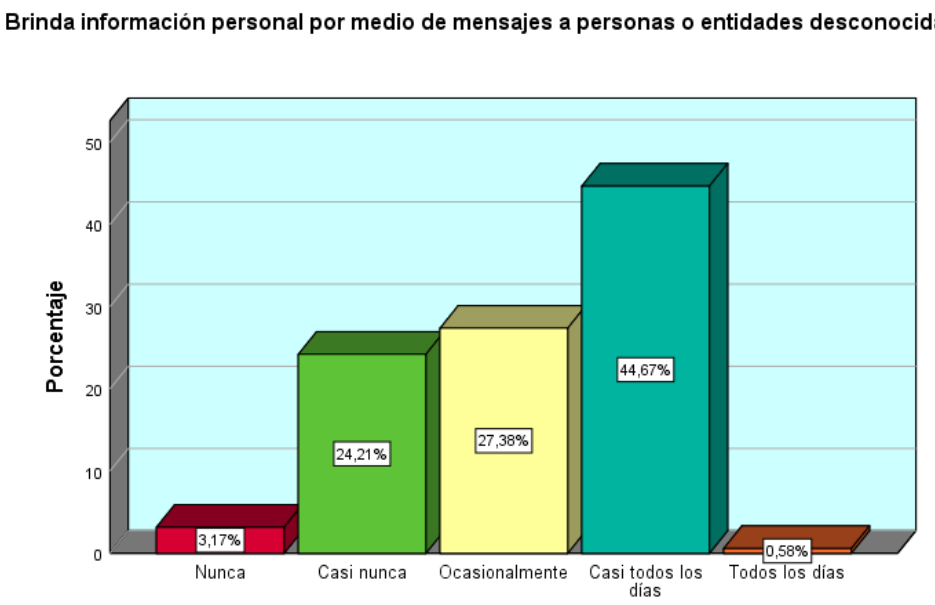
10.- Identifica los mensajes de texto que se hacen pasar por una entidad financiera (Gráfico 10)



Fuente: Elaboración propia SPSS

Ítem 11

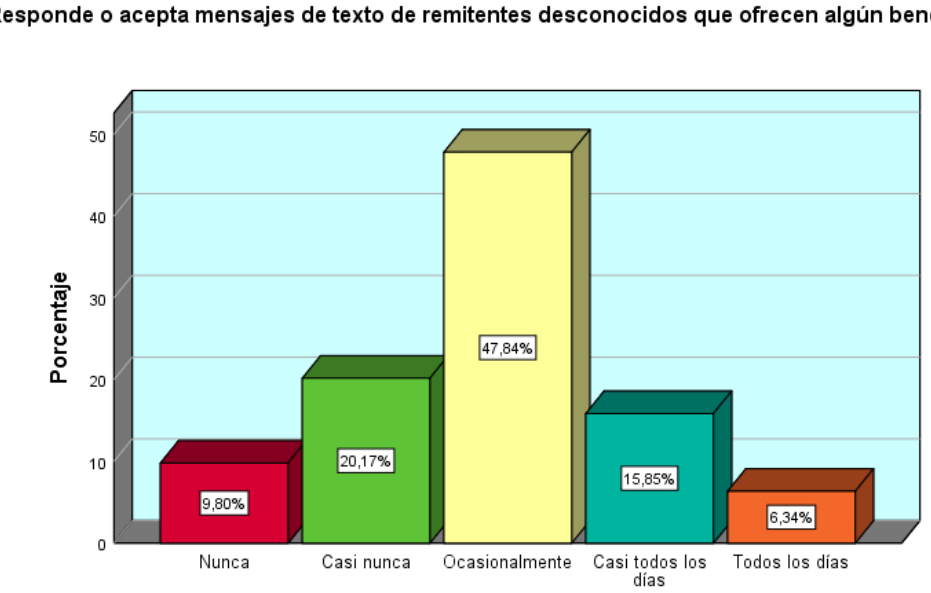
11.- **Brinda información personal por medio de mensajes a personas o entidades desconocidas (Gráfico 11)**



Fuente: Elaboración propia SPSS

Ítem 12

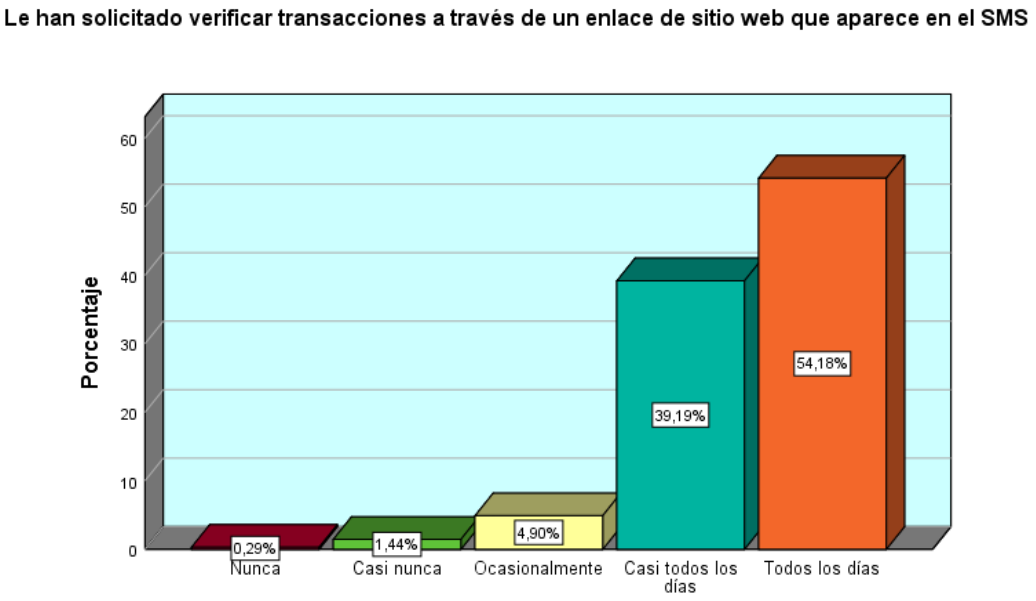
12.- Responde o acepta mensajes de texto de remitentes desconocidos que ofrecen algún beneficio (Gráfico 12)



Fuente: Elaboración propia SPSS

Ítem 13

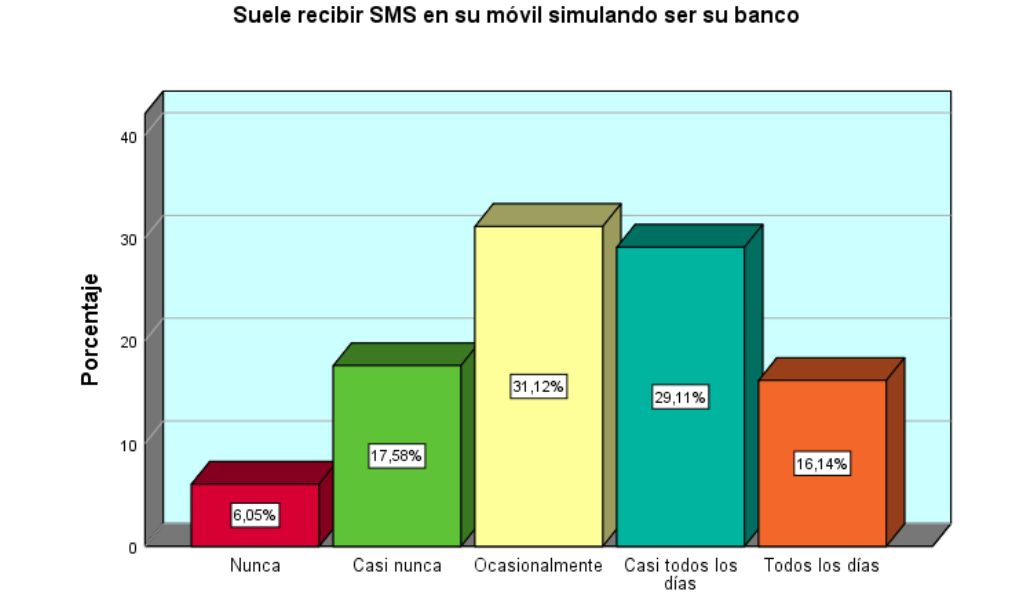
13.- Le han solicitado verificar transacciones a través de un enlace de sitio web que aparece en el SMS (Gráfico 13)



Fuente: Elaboración propia SPSS

Ítem 14

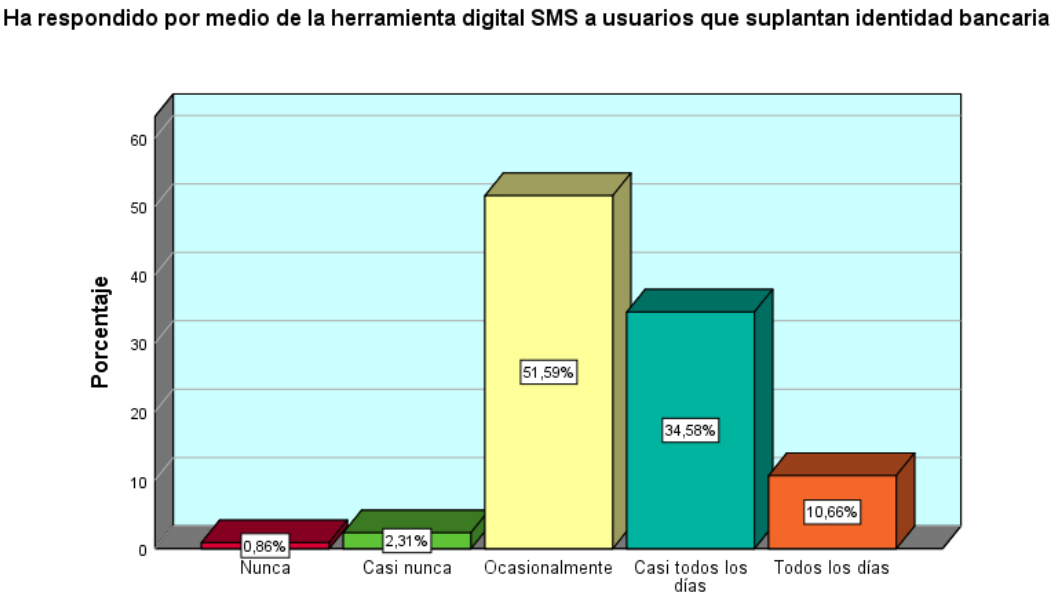
14.- Suele recibir SMS en su móvil simulando ser su banco (Gráfico 14)



Fuente: Elaboración propia SPSS

Ítem 15

15.- Ha respondido por medio de la herramienta digital SMS a usuarios que suplantan identidad bancaria (Gráfico 15)



Fuente: Elaboración propia SPSS