Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

PLATAFORMA DE PAGO MÓVIL Y NIVEL DE CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES EN UNA UNIVERSIDAD DE LIMA, 2024

Línea de investigación:
Herramientas informáticas para una gestión eficiente y transparente

Tesis para optar el Grado Académico de Maestro en Ingeniería Industrial con mención en Gestión de Operaciones y Productividad

Autor

Diaz Ricalde, Manuel Antonio

Asesora

Tejada Estrada, Gina Coral

ORCID: 0000-0002-0023-5147

Jurado

Diaz Garcia, Martin Fernando

Sanchez Camargo, Mario Rodolfo

Bances Suclupe, José Hildebrando

Lima - Perú

2025

PLATAFORMA DE PAGO MÓVIL Y NIVEL DE CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES EN UNA UNIVERSIDAD DE LIMA, 2024.

INFORME DE ORIGINALIDAD

21%	19%	5%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	2%
2	www.coursehero.com Fuente de Internet	2%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	repositorio.unfv.edu.pe Fuente de Internet	1%
5	repository.unad.edu.co Fuente de Internet	1%
6	Submitted to Universidad Privada del Norte Trabajo del estudiante	1%
7	dspace.univd.edu.ua Fuente de Internet	1%
8	repositorio.uncp.edu.pe Fuente de Internet	1%
9	hdl.handle.net Fuente de Internet	1%
10	Submitted to uncedu Trabajo del estudiante	<1%
11	Submitted to University of Notre Dame Trabajo del estudiante	<1%

ESCUELA UNIVERSITARIA DE POSGRADO

PLATAFORMA DE PAGO MÓVIL Y NIVEL DE CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES EN UNA UNIVERSIDAD DE LIMA, 2024

Línea de Investigación:

Herramientas informáticas para una gestión eficiente y transparente

Tesis para optar el Grado Académico de Maestro en Ingeniería Industrial con mención en Gestión de Operaciones y Productividad

Autor:

Diaz Ricalde, Manuel Antonio

Asesora

Tejada Estrada, Gina Coral

ORCID: 0000-0002-0023-5147

Jurado:

Diaz Garcia, Martin Fernando

Sanchez Camargo, Mario Rodolfo

Bances Suclupe, José Hildebrando

Lima – Perú

2025

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Objetivo: Es determinar la relación entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024. **Método:** La investigación se clasifica como aplicada y de nivel correlacional. La población está integrada por 200 estudiantes, y la muestra se compone de los mismos 200 alumnos de la Facultad de Administración, a través de un muestreo censal. **Resultados:** El 38% de los encuestados considera "totalmente de acuerdo" en que las plataformas de pago móvil son seguras, mientras que un 21% está "de acuerdo". Sin embargo, un 25% se muestra neutral y un 17% manifiesta desacuerdo, lo que indica una falta de confianza general. En cuanto al conocimiento sobre protección de datos financieros, el 37% se siente "totalmente de acuerdo" y el 34% "de acuerdo". Por otro lado, un 16% permanece neutral y un 13% expresa desacuerdo. Aunque muchos se sienten informados, hay un porcentaje significativo que podría no estarlo. Se registró un coeficiente de correlación de Spearman de 0.812, indicando una fuerte relación positiva, con significancia bilateral de 0.000 que permite rechazar la hipótesis nula. **Conclusiones:** Los resultados demostraron que el nivel de seguridad en transacciones de plataformas de pago móvil está positivamente relacionado con el conocimiento sobre gestión de riesgos. Implementar controles de seguridad avanzados puede disminuir la exposición a vulnerabilidades, lo que permite a las organizaciones estar mejor preparadas para mitigar riesgos globales en la seguridad de datos.

***Palabras claves**:* Plataformas de Pago, vulnerables, tecnologías, información financiera.

ABSTRACT

Objective: To determine the relationship between the mobile payment platform and the level of knowledge about the protection of financial and personal data at a University in Lima, 2024. Method: The research is classified as applied and correlational level. The population is made up of 200 students, and the sample is composed of the same 200 students from the Faculty of Administration, through a census sampling. Results: 38% of respondents consider that they "totally agree" that mobile payment platforms are safe, while 21% "agree". However, 25% are neutral and 17% disagree, indicating a general lack of confidence. Regarding knowledge about financial data protection, 37% feel "totally agree" and 34% "agree". On the other hand, 16% remain neutral and 13% express disagreement. Although many feel informed, there is a significant percentage that may not be. A Spearman correlation coefficient of 0.812 was recorded, indicating a strong positive relationship, with a bilateral significance of 0.000 that allows rejecting the null hypothesis. Conclusions: The results showed that the level of security in mobile payment platform transactions is positively related to knowledge about risk management. Implementing advanced security controls can reduce exposure to vulnerabilities, allowing organizations to be better prepared to mitigate global data security risks.

Keywords: Payment Platforms, vulnerable, technologies, financial information.

I. INTRODUCCIÓN

En los últimos años, el uso de plataformas de pago móvil ha crecido de manera notable en diversas partes del mundo, incluyendo Perú. Estas herramientas permiten realizar transacciones de manera rápida y sencilla, lo que ha llevado a muchas universidades a adoptarlas para facilitar los pagos de matrícula, servicios y otros gastos. Sin embargo, este avance tecnológico también ha traído consigo importantes desafíos relacionados con la seguridad de la información.

La protección de datos financieros y personales se ha convertido en un tema crítico, especialmente en un entorno donde las amenazas cibernéticas son cada vez más comunes.

A pesar de la comodidad que ofrecen estas plataformas, muchos usuarios no están completamente informados sobre los riesgos asociados con el uso de aplicaciones móviles para realizar pagos.

Esto es preocupante, ya que una falta de conocimiento puede llevar a la exposición de información sensible, como números de tarjetas de crédito o datos personales.

En el contexto de una universidad en Lima, es esencial investigar el nivel de conocimiento que tienen los estudiantes y el personal sobre cómo proteger su información al utilizar estas plataformas.

Entender esta situación no solo ayudará a identificar brechas en la educación sobre seguridad, sino que también permitirá desarrollar estrategias efectivas para mejorar la confianza de los usuarios en el uso de estas herramientas.

Por lo tanto, esta investigación busca analizar cómo el conocimiento sobre la protección de datos influye en la disposición de los usuarios para utilizar plataformas de pago móvil de manera segura.

Al abordar este tema, se espera contribuir a una mayor conciencia sobre la importancia de la seguridad en el ámbito digital, promoviendo así un uso más seguro y responsable de la tecnología en la comunidad universitaria.

1.1. Planteamiento del problema

Hoy en día, muchas universidades están usando plataformas de pago móvil para facilitar las transacciones de estudiantes y personal. Sin embargo, esto también trae preocupaciones sobre la seguridad de los datos financieros y personales de los usuarios. Es importante saber cuánto conocen los estudiantes y el personal sobre cómo proteger su información al usar estas aplicaciones.

En Lima, el uso de tecnología está creciendo, pero se ha notado que muchas personas no tienen suficiente información sobre cómo cuidar su información personal y financiera al hacer pagos en línea. Esta falta de conocimiento puede hacer que sean más vulnerables a problemas de seguridad, lo que podría afectar su confianza en el uso de estas plataformas.

La creciente implementación de tecnologías financieras móviles, como las plataformas de pago, presenta desafíos significativos en relación con la protección de datos financieros y personales.

En el contexto del entorno universitario de Lima, donde interactúan diversos actores con distintos niveles de conocimiento y familiaridad con estas herramientas, se hace evidente la necesidad de evaluar el grado de conocimiento sobre la protección de datos financieros y personales entre los integrantes de la comunidad universitaria.

El uso de plataformas de pago móvil por parte de los estudiantes conlleva la transmisión y el almacenamiento de información financiera sensible, que incluye datos bancarios y de tarjetas de crédito, así como información personal, como nombres, direcciones y números de identificación. Por lo tanto, es fundamental profundizar en esta temática para garantizar la seguridad de la información en un ámbito tan vulnerable.

No obstante, la carencia de conciencia y comprensión sobre las mejores prácticas de seguridad cibernética puede dejar a los usuarios vulnerables ante riesgos considerables, tales como el robo de identidad, el fraude financiero y la violación de la privacidad.

En este contexto, surge la pregunta sobre el nivel de conocimiento y comprensión que tienen los miembros de la comunidad universitaria de Lima respecto a los riesgos específicos asociados con el uso de plataformas de pago móvil como Yape y Plin.

Asimismo, es crucial indagar sobre las medidas de protección de datos financieros y personales que deben implementarse para mitigar estos peligros. Por lo tanto, se hace necesario evaluar y fomentar la educación en este ámbito para garantizar una mayor seguridad entre los usuarios.

1.2. Descripción del problema

La tecnología digital ha simplificado numerosos aspectos de nuestras vidas, pero también ha creado nuevas oportunidades para delitos y fraudes. En este contexto, es fundamental mantener una vigilancia constante y comprender los riesgos asociados para proteger nuestras finanzas en la era digital.

Desde marzo de 2020 hasta el presente, hemos experimentado un cambio en la manera de adquirir bienes, pagar servicios e incluso en las modalidades de trabajo. Esta transformación exige una mayor atención a la seguridad y a la educación sobre los posibles peligros que conlleva el uso de herramientas digitales.

Esta "evolución" hacia un entorno digital y virtual ha traído consigo numerosos beneficios. Sin embargo, también ha dado lugar a una serie de desafíos significativos.

Uno de los problemas más destacados son las actividades delictivas que se llevan a cabo a través de los sistemas informáticos, las cuales han sido reguladas por los legisladores nacionales mediante la Ley 30096, conocida como Ley de Delitos Informáticos, que fue

modificada por la Ley 30171. A pesar de estos esfuerzos, todavía no se ha logrado prevenir eficazmente los delitos en las plataformas de pago móvil.

Ramírez (2023) en investigación publicada en el Diario el Comercio comenta que Sharon Domínguez experimentó una pérdida repentina de 190 soles en un lapso de menos de un minuto. Este incidente ocurrió cuando dos individuos jóvenes visitaron su óptica con la intención de adquirir cuatro pares de lentes. Durante la transacción, le mostraron un comprobante de pago a través de la plataforma Plin, lo que generó confianza en ella, lo que hizo que no verificara el movimiento bancario de inmediato. Domínguez señaló que los estafadores utilizaron una aplicación que genera capturas de pantalla falsas, simulando así un pago exitoso a través de la plataforma de pago móvil.

Se trata de un nuevo método de estafa que aprovecha la confianza de los comerciantes en las plataformas de pago móvil como Plin y Yape. Los estafadores simulan realizar un pago exitoso al mostrar una captura de pantalla falsa al vendedor, lo que lleva al vendedor a creer que la transacción se ha completado.

Sin embargo, en realidad, no se ha realizado ningún pago y los estafadores se benefician al obtener los productos sin pagar por ellos. Esta situación resalta la importancia de que los comerciantes estén alerta y tomen medidas de precaución al aceptar pagos a través de plataformas de pago móvil.

Además, subraya la necesidad de que los usuarios de estas plataformas sean conscientes de posibles fraudes y se aseguren de confirmar los pagos de manera adecuada antes de entregar los productos o servicios. Los casos de estafa en esta modalidad han aumentado considerablemente, ya que en 2023 la Policía Nacional del Perú (PNP) registró al menos 609 denuncias relacionadas con estafas vinculadas a las aplicaciones de billeteras digitales Yape y Plin (Espinoza, 2023).

Con un total de 453 y 153 denuncias respectivamente, Lima encabeza los reportes de la PNP, con las bodegueras siendo las víctimas más afectadas (Buenapepa, 2023). Sin duda existen una gran preocupación por el incremento de las denuncias por estafas relacionadas con aplicaciones de pago en Lima, donde las bodegas son las principales víctimas.

Los delincuentes utilizan métodos sofisticados, como herramientas de edición y programación, para falsificar transacciones y generar recibos falsos que engañan a los comerciantes.

Es notable cómo los estafadores aprovechan la tecnología, incluso haciendo uso de la Inteligencia Artificial para simular notificaciones auténticas de las aplicaciones de pago. Esto subraya la necesidad de que tanto los usuarios como los comerciantes estén alerta y tomen medidas de seguridad adicionales al realizar transacciones a través de estas plataformas.

El crecimiento de estas prácticas fraudulentas se atribuye en parte a la creciente popularidad de las aplicaciones de pago, que han ganado terreno como una alternativa al efectivo en el entorno comercial.

Esta situación destaca la importancia de una mayor conciencia sobre la seguridad cibernética y la necesidad de desarrollar medidas más efectivas para combatir el fraude en el ámbito de los pagos digitales.

Por consiguiente, resulta fundamental evaluar el grado de conocimiento y conciencia sobre la protección de datos financieros y personales entre los integrantes de la comunidad universitaria de Lima, especialmente en el contexto de la implementación de plataformas de pago móvil en 2024.

1.3. Formulación del problema

- Problema general

¿Cuál es la relación entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

- Problemas específicos

¿Cuál es la relación entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

¿Qué relación existe entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

¿Qué relación existe entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

¿Cuál es la relación entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

¿Cuál es la relación entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?

1.4. Antecedentes

- Internacionales

Castro (2019) en su estudio "Protección de datos personales a través de herramientas de procesamiento automatizado de datos: desafíos y recomendaciones" subraya la importancia de abordar los retos que emergen en la salvaguarda de los datos personales dentro de un contexto de procesamiento automatizado. Entre estos desafíos se encuentran el acceso no autorizado y el uso indebido de la información. Para garantizar la privacidad de los individuos, es fundamental establecer medidas adecuadas y adherirse a las normativas de protección de datos pertinentes. Con el fin de reducir los riesgos asociados con el procesamiento automatizado, es esencial seguir las mejores prácticas y recomendaciones, lo que incluye la adopción de robustas medidas de seguridad y la formación del personal en temas de privacidad y seguridad de la información. Asimismo, cumplir con las leyes y regulaciones de protección de datos vigentes es crucial para resguardar los derechos de privacidad y evitar sanciones por posibles incumplimientos.

Hernández y Londoño (2020) en su tesis “La Responsabilidad De Las Entidades Financieras Por Fraudes Electrónicos” cuestionan la viabilidad de limitar los recursos y excluir excepciones en este sistema, ya que no toma en consideración la naturaleza contractual de la relación, las medidas de protección de las partes y las normativas sobre comercio electrónico. Se propone una interpretación exhaustiva del marco legal para que los encargados de hacer cumplir la ley consideren todos los elementos relevantes al analizar fraudes en el sistema financiero. En síntesis, dada la naturaleza contractual de la responsabilidad por fraude electrónico bancario, se sugiere que esta se resuelva mediante el cumplimiento de obligaciones de debida diligencia por ambas partes, utilizando criterios subjetivos en lugar de aplicar una responsabilidad objetiva restrictiva.

Nacionales

Según Juli (2024) la inclusión financiera ha permitido, a lo largo del tiempo, que se acceda de manera equitativa a los servicios financieros fundamentales. En este contexto, Action Bank se erige como un referente significativo, especialmente en su labor de promover la inclusión financiera en diversas comunidades. El objetivo de este estudio es analizar la relación entre la bancarización y la inclusión financiera entre los estudiantes de una universidad. Los hallazgos revelan una correlación positiva moderada entre las variables analizadas, con un coeficiente de correlación de Spearman de $rs = 0.503$. Esto sugiere que, a medida que aumenta la exposición a Action Bank, también se eleva el nivel de inclusión financiera de los estudiantes.

García y Soto (2022) centran su estudio en esta región debido a su constante crecimiento y a las restricciones en el acceso a servicios financieros formales y a la educación. A través de un análisis de regresión lineal, los autores descubrieron un impacto significativo del financiamiento de las campañas en la inclusión financiera. Estos hallazgos son de gran relevancia para empresas e instituciones financieras, ya que ofrecen información valiosa que

puede ser utilizada para promover la inclusión financiera en Lima Norte y que, además, podría ser replicada en otras zonas del país.

Balarezo y Gálvez (2020) concluyen que existe una relación moderadamente positiva entre el uso de métodos de pago digitales y la satisfacción del cliente, respaldada por los resultados del cuestionario empleado en su investigación. Además, enfatizan la importancia de evaluar la atención al usuario mediante encuestas y mediciones automatizadas. Los autores sugieren que es fundamental establecer una cultura de datos dentro de las empresas y fortalecer el vínculo entre la utilización de métodos de pago digitales y la satisfacción del cliente.

Rayo (2020) ajustó los cuestionarios relacionados con el financiamiento de campañas, la confianza y la inclusión financiera de acuerdo con las variables relevantes para evaluar las hipótesis. El análisis de los datos, llevado a cabo mediante regresión lineal, evidenció un impacto significativo del dinero destinado a campañas en la inclusión financiera. Estos hallazgos son de gran utilidad para empresas e instituciones financieras, ya que proporcionan información valiosa para promover la inclusión financiera en Lima Norte y, potencialmente, en otras regiones del país.

Arrunátegui (2020) señala la escasez de estudios empíricos sobre este tema, particularmente en el contexto peruano. No obstante, mediante una revisión exhaustiva de la literatura, se ha desarrollado un marco analítico que explora la relación entre la inclusión financiera y los factores que afectan la adopción de pagos móviles. Además, se investiga el impacto del uso de aplicaciones bancarias en el crecimiento de las bodegas y el desarrollo de los bodegueros.

Pacheco (2019) destaca que, en los últimos años, los servicios financieros han experimentado una evolución significativa gracias a los avances tecnológicos, poniendo especial énfasis en la importancia de la banca móvil. A nivel global, se han implementado exitosamente modelos transformacionales y complementarios. Aunque Perú cuenta con un

número reducido de bancos, está en búsqueda de estrategias para impulsar la actividad bancaria, priorizando la banca móvil. En este contexto, se ha investigado una institución financiera pública que ofrece servicios de banca móvil desde 2015, con el fin de mejorar el acceso y satisfacer la demanda. Este estudio pretende abordar la falta de información sobre el impacto de la banca móvil en los servicios financieros en Perú, buscando proporcionar apoyo teórico y fomentar el desarrollo económico.

1.5. Justificación de la investigación

1.5.1. Práctica

La investigación se realiza debido a que, en la actualidad, en esta era digital, la información personal y financiera se ha vuelto cada vez más vulnerable a amenazas cibernéticas. Por lo tanto, es imperativo, que tanto la institución educativa como los usuarios estén debidamente informados y preparados para proteger sus datos.

La falta de conocimiento sobre los riesgos asociados con la divulgación indebida de información financiera y personal puede exponer a los individuos a fraudes, robos de identidad y otros delitos financieros.

Por lo tanto, la realización de un estudio que evalúe el nivel de conocimiento sobre la protección de datos financieros y personales entre los miembros de la comunidad universitaria, en el contexto de la implementación de una plataforma de pago móvil, es fundamental. Este estudio proporcionará información valiosa sobre las percepciones, actitudes y prácticas actuales en cuanto a la seguridad de la información financiera y personal. Los resultados de este estudio servirán como base para el diseño e implementación de programas de capacitación y concientización dirigidos a estudiantes, e incluso todos los usuarios que hoy en día es inevitable el uso de plataformas virtuales.

Estos programas buscarán mejorar la comprensión de los riesgos asociados con el uso de plataformas de pago móvil y promover prácticas seguras para proteger la información

financiera y personal. En última instancia, la realización de este estudio y la implementación de medidas educativas contribuirán a fortalecer la seguridad cibernética, protegiendo así los datos y la privacidad de sus miembros y fomentando un ambiente de confianza y seguridad en el uso de tecnologías financieras emergentes.

1.5.2. Teórica

La investigación sobre plataformas de pago móvil y el conocimiento sobre la protección de datos en una universidad de Lima se fundamenta en cuatro teorías clave: la Teoría de la Adopción de Tecnología (TAM), la Teoría de la Seguridad de la Información, la Teoría de la Privacidad de la Información y la Teoría del Riesgo y la Confianza. Estas teorías se entrelazan y proporcionan un marco integral para comprender cómo los usuarios adoptan tecnologías y perciben la seguridad y la privacidad.

La Teoría de la Adopción de Tecnología (TAM) es esencial para entender las razones por las cuales los estudiantes deciden utilizar plataformas de pago móvil. Al analizar la facilidad de uso y la utilidad percibida, se pueden identificar los factores que impulsan a los estudiantes a usar estas tecnologías.

Esta investigación permitirá determinar si consideran que las plataformas de pago son prácticas y beneficiosas para su día a día, lo que podría influir en su disposición para aprender sobre la protección de sus datos.

La seguridad de la información es crucial al usar plataformas de pago móvil, ya que se maneja información sensible. La Teoría de la Seguridad de la Información ayuda a investigar cómo la percepción de seguridad afecta la confianza de los estudiantes en estas plataformas. Un mayor entendimiento de las medidas de seguridad puede promover una adopción más responsable de estas tecnologías, resaltando la importancia de educar a los estudiantes sobre la protección de datos.

Por su parte, la Teoría de la Privacidad de la Información se enfoca en el derecho de los individuos a gestionar su información personal. En el contexto de los pagos móviles, es fundamental comprender cómo los estudiantes perciben su privacidad y cuán informados están sobre sus derechos.

Un buen conocimiento de la privacidad puede influir en la manera en que los estudiantes interactúan con las plataformas y en su disposición a compartir sus datos personales.

Finalmente, la Teoría del Riesgo y la Confianza analiza la relación entre la percepción de riesgos y la confianza en el uso de plataformas de pago móvil. Esta teoría permite investigar cómo los estudiantes evalúan los riesgos asociados a estas tecnologías y cómo influyen en su confianza.

Si consideran que los beneficios superan los riesgos, es más probable que adopten estas plataformas. La investigación también puede explorar cómo la educación sobre protección de datos puede reducir la percepción del riesgo.

1.5.3. Metodológica

Se basa en un tipo aplicado y un diseño correlacional, que permite explorar la relación entre el uso de plataformas de pago móvil y el conocimiento sobre la protección de datos. Se empleó el juicio de expertos para validar la relevancia y claridad de los ítems del cuestionario, asegurando que las preguntas aborden de manera efectiva los conceptos que se quieren medir. Además, se utilizó el coeficiente alfa de Cronbach para evaluar la confiabilidad del instrumento, garantizando que los resultados sean consistentes y válidos.

Esta metodología no solo enriquece la comprensión teórica del tema, sino que también tiene importantes implicaciones prácticas para la educación sobre el uso seguro de tecnologías digitales entre los estudiantes.

1.5.4. Legal

Se fundamenta en el cumplimiento de las normativas peruanas y principios internacionales vinculados a la protección de datos y la privacidad. En primer lugar, la Ley N° 29733, conocida como Ley de Protección de Datos Personales, establece el marco legal para la recopilación y gestión de datos personales en Perú, asegurando el derecho a la privacidad y la protección de la información. Al investigar el nivel de conocimiento de los estudiantes sobre la protección de sus datos financieros y personales, el estudio fomenta una cultura de respeto y salvaguarda de la privacidad.

Adicionalmente, el Decreto Supremo N° 003-2013-JUS, que regula la ley mencionada, proporciona directrices sobre el consentimiento informado, el acceso a la información y el derecho a la rectificación de datos. Este estudio busca determinar si los estudiantes están conscientes de estos derechos y de cómo pueden ejercerlos al utilizar plataformas de pago móvil, lo que les permite empoderarse como usuarios.

Por último, aunque el Reglamento General de Protección de Datos (GDPR) de la Unión Europea no se aplica directamente en Perú, establece principios que pueden servir como referencia para mejorar la protección de datos y la privacidad. Este enfoque internacional subraya la importancia de que las instituciones educativas fomenten la educación y la conciencia sobre la protección de datos en un mundo digital cada vez más interconectado.

1.5.5. Importancia de la investigación

Se tiene una relevancia significativa en el contexto de los Objetivos de Desarrollo Sostenible (ODS) de la ONU, particularmente en los siguientes aspectos:

- Objetivo 4: Educación de Calidad: Esta investigación contribuye a mejorar la educación de calidad al abordar la necesidad de enseñar a los estudiantes sobre la protección de datos y el uso seguro de plataformas digitales. Fomentar el conocimiento en este ámbito

es esencial para preparar a los jóvenes para enfrentar los desafíos de un mundo cada vez más digitalizado.

- Objetivo 8: Trabajo Decente y Crecimiento Económico: Promover el uso seguro de plataformas de pago móvil puede facilitar la inclusión financiera, lo que es crucial para el crecimiento económico. Al capacitar a los estudiantes sobre la gestión segura de sus datos, se fomenta la confianza en el uso de servicios financieros digitales, lo que puede contribuir al desarrollo de la economía local.
- Objetivo 9: Industria, Innovación e Infraestructura: Al investigar la adopción de tecnologías de pago móvil, la investigación apoya el desarrollo de infraestructura tecnológica y promueve la innovación en el ámbito financiero. Un mayor conocimiento sobre la protección de datos puede incentivar a más usuarios a participar en la economía digital.

1.6. Limitaciones de la investigación

Al examinar el desarrollo de la investigación en la que se estará involucrada, es fundamental considerar el tamaño de la muestra, ya que este factor podría influir significativamente en el alcance del estudio, debido a restricciones de tiempo y recursos para encuestar a una muestra representativa de la comunidad universitaria.

Esto podría resultar en una generalización limitada de los resultados obtenidos. Sesgo de selección: Existe la posibilidad de que ciertos grupos dentro de la universidad estén más inclinados a participar en la investigación que otros, lo que podría sesgar los resultados y limitar su validez externa.

1.7. Objetivos

-Objetivo general

Determinar la relación entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

-Objetivos específicos

Determinar la relación entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Establecer la relación entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Establecer la relación entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Determinar la relación entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Establecer la relación entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

1.8. Hipótesis

1.8.1. Hipótesis general

Existe relación positiva entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

1.8.2 Hipótesis específicas

- Existe relación positiva entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
- Existe relación positiva entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
- Existe relación positiva entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
- Existe relación positiva entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

- Existe relación positiva entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

II. MARCO TEÓRICO

2.1. Marco conceptual

2.1.1. Teorías generales sobre

2.1.1.1. Teoría de la Adopción de Tecnología (TAM). Su finalidad es explicar y predecir de qué manera los usuarios aceptan y utilizan nuevas tecnologías. Incluye: (a) Facilidad de Uso Percibida, que se refiere a cómo los usuarios perciben la facilidad de uso de la tecnología; a mayor simplicidad en la interacción con la plataforma de pago móvil, mayor será la probabilidad de adopción (López y López, 2011).

(b) Utilidad Percibida: Esta dimensión se refiere a la creencia de que el uso de la tecnología mejorará su desempeño en una tarea específica. En el contexto de los pagos móviles, si los estudiantes perciben que la plataforma les ahorra tiempo o es más conveniente que métodos tradicionales, es más probable que la utilicen (López y López, 2011).

2.1.1.2. Teoría de la Seguridad de la Información. La Teoría de la Seguridad de la Información se centra en cómo los individuos perciben y manejan el riesgo asociado con la seguridad de sus datos personales y financieros. En un contexto de plataformas de pago móvil, esta teoría es especialmente relevante debido a la naturaleza sensible de la información que se maneja. Incluye:

(a) Confianza: La confianza es un elemento fundamental. Los usuarios deben confiar en que la plataforma protegerá sus datos y realizará transacciones de manera segura. Factores como la reputación de la plataforma, las certificaciones de seguridad y la transparencia en el manejo de datos influyen en esta percepción (Parada et al., 2018).

(b) Riesgo Percibido: Este se refiere a la evaluación que hace el usuario sobre la posibilidad de sufrir un daño, como el robo de identidad o la pérdida de dinero. Una percepción alta de riesgo puede disuadir a los usuarios de adoptar la tecnología, mientras que una percepción baja puede facilitar su aceptación (Parada et al., 2018).

2.1.1.3. Teoría de la Privacidad de la Información. Esta teoría se centra en el derecho de los individuos a controlar su información personal y en cómo gestionan su privacidad. Es fundamental para entender cómo los usuarios perciben y manejan su información en el contexto digital. Incluye:

(a) Consentimiento Informado: Los usuarios deben ser plenamente informados sobre la recopilación y uso de sus datos antes de dar su consentimiento (Rapimán y Chibey, 2022).

(b) Acceso y Corrección: Los individuos deben poder acceder a sus datos y corregir cualquier inexactitud, asegurando que su información esté actualizada y sea precisa (Rapimán y Chibey, 2022).

2.1.1.4. Teoría del Riesgo y la Confianza. Esta teoría aborda la relación entre la percepción del riesgo y la confianza en el manejo de datos personales. La confianza es un factor crucial para la adopción de plataformas de pago, especialmente en lo que respecta a la seguridad de la información. Incluye:

(a) Percepción del Riesgo: Los usuarios evalúan el riesgo de fraude y la pérdida de datos al utilizar plataformas de pago (Sganderla et al., 2014).

(b) Construcción de Confianza: La confianza se construye a través de factores como la transparencia en las políticas de privacidad y las medidas de seguridad implementadas (Sganderla et al., 2014).

2.1.2. Plataformas de Pago (billeteras electrónicas) en el Perú

Cárdenas (2022) A causa de la epidémica, ha habido un aumento significativo en la utilización y vinculación de canales digitales en el sector bancario. Entre estos canales, sobresalen las plataformas de pago o carteras digitales, que posibilitan la realización de transacciones a través de dispositivos móviles.

Dos de las plataformas más relevantes en este ámbito son YAPE y PLIN. YAPE, inicialmente concebida como un servicio adicional del Banco de Crédito BCP, se centraba en

proveer servicios de transacciones a clientes individuales. Por otro lado, PLIN surgió poco después mediante una colaboración entre los bancos BBVA, Interbank y Scotiabank.

En cuanto a YAPE, la plataforma ahora opera de manera independiente, lo que significa que puede descargarse sin estar vinculada a ningún sistema operativo en particular. En contraste, PLIN es una plataforma integrada dentro del entorno del banco digital de cada entidad bancaria.

En principio, la aplicación Yape fue desarrollada por el Banco de Crédito del Perú (BCP) en 2016 y presentada al público en 2017. Este hecho ha propiciado un crecimiento considerable a lo largo del tiempo, alcanzando los 5 millones de usuarios en 2020. López y Palomino (2021) sostienen que, durante la pandemia, Yape facilitó la inclusión financiera de 650.000 peruanos, quienes accedieron por primera vez a servicios financieros, y permitió que más de 700.000 micro y pequeñas empresas pudieran acceder a servicios financieros de manera sencilla y sin contacto.

Por otro lado, Plin ha sido incorporada en las aplicaciones de banca móvil de BBVA, Interbank, BanBif, Scotiabank y Caja Arequipa, lo que permite transferencias de dinero. En 2020, el consorcio bancario puso la aplicación a disposición de sus clientes y afirmó haber realizado Plin ha logrado 12,2 millones de transferencias, evidenciando su éxito y beneficios para usuarios y bancos.

Asimismo, los líderes de Yape y Plin han mostrado un mayor optimismo sobre la posibilidad de lograr la interoperabilidad debido al impacto de la pandemia. En una entrevista con Semana Económica a principios de este año, el director general de Yape, Raimundo Morales, expresó su apoyo a la interoperabilidad, reflejando la postura previamente manifestada por el líder de Yape, Rufino Arriba, quien dijo que competimos con el efectivo, esto sugiere que, más allá de la competencia, su verdadero objetivo es introducir innovación

gradualmente las monedas digitales en las micro transacciones diarias de los individuos (Mercantil, 2024).

Los pagos electrónicos se han empoderado en el Perú. Según el Banco Central de Reserva del Perú (BCRP), desde diciembre de 2022, el número de transacciones en línea por persona se había multiplicado por cinco en comparación con 2015. Este crecimiento se debe a la posibilidad de utilizar tarjetas de débito como medio de pago y a los avances recientes en billeteras virtuales.

El aumento en el uso de pagos digitales también se debe a las estrategias comerciales de varios actores del mercado financiero, incluidos muchos comerciantes que emplean billeteras digitales para realizar ventas.

Además, el uso intensivo de super aplicaciones y redes sociales también influye en este crecimiento. ¿Cómo impacta esto en las personas? Beneficios para los ciudadanos Los pagos digitales son significativos porque benefician a la sociedad y brindan a las personas un acceso más amplio a los servicios financieros.

Además, los sistemas de adquisición fomentan que los dueños de negocios realicen transacciones financieras formales con regularidad, lo que aumenta la transparencia financiera y reduce la corrupción en forma de sobornos y otras actividades ilícitas.

El uso de pagos digitales también puede impulsar las ventas, ya que reduce los costos y riesgos asociados con la gestión de efectivo y se vuelve más visible durante situaciones de emergencia. Además, a diferencia de los pagos en efectivo, los pagos digitales pueden realizarse sin necesidad de que nadie esté presente.

Los pagos digitales se efectúan mediante dispositivos electrónicos como teléfonos inteligentes, computadoras y tabletas. Se adoptan medidas de seguridad, como la autenticación de dos factores, para proteger la información, el uso de aplicaciones genuinas descargadas de

tiendas oficiales y sistemas de bloqueo de dispositivos móviles para garantizar la seguridad de estas transacciones.

Además, los pagos digitales deben cumplir con cinco requisitos básicos de seguridad: confidencialidad, autenticación, autorización, integridad y disponibilidad (Vergara, 2023).

Una plataforma de pago móvil es un sistema digital que permite a los usuarios llevar a cabo transacciones financieras utilizando dispositivos móviles, como teléfonos inteligentes o tabletas.

Estas plataformas facilitan el envío y recepción de dinero, el pago de productos y servicios, así como la gestión de cuentas bancarias, empleando tecnologías como códigos QR, NFC (comunicación de campo cercano) y transferencias mediante aplicaciones. Además, suelen incorporar medidas de seguridad, como la autenticación de dos factores, para salvaguardar la información financiera y personal de los usuarios.

2.1.3. Interoperabilidad

Vallejos (2023) destaca la relevancia de la interoperabilidad en el progreso de los pagos digitales y la inclusión financiera en Perú, así como las inquietudes relacionadas con la seguridad en las aplicaciones Yape y Plin. En cuanto a la interoperabilidad y la seguridad, se enfatiza cómo estas dos cuestiones están estrechamente ligadas.

Aunque la interoperabilidad es crucial para facilitar los pagos digitales y mejorar la inclusión financiera, las preocupaciones sobre la seguridad, especialmente en relación con la compatibilidad entre Yape y Plin, son evidentes.

El aumento de denuncias de estafas y fraudes relacionados con el uso de estas aplicaciones, según registros de la Policía Estatal, resalta la necesidad de garantizar la seguridad en las transacciones digitales para proteger a los usuarios y promover su confianza en estos sistemas. Se hace mención de las medidas de seguridad implementadas por ambas

aplicaciones, Yape y Plin, que incluyen el uso de tecnologías como el cifrado y filtros antifraude para prevenir interferencias de terceros y detectar transacciones sospechosas.

Además, se destaca la autenticación de usuario mediante claves de configuración o verificación biométrica para restringir el acceso solo a usuarios autorizados. Los bancos detrás de Yape y Plin, BCP y BBVA Continental, respectivamente, han implementado sistemas de seguridad probados en sus sistemas financieros para proporcionar una mayor confianza a los usuarios.

La presencia de expertos en seguridad es destacada, ya que están encargados de proporcionar múltiples capas de seguridad para minimizar los riesgos potenciales asociados con las aplicaciones y sus usuarios. Además, se subraya la importancia de establecer políticas claras sobre la confidencialidad y privacidad de los datos, junto con protocolos de seguridad para el manejo y almacenamiento de la información. Se subraya que las claves de acceso se almacenan de manera encriptada para salvaguardar la información sensible de los clientes.

Por más que han hecho esfuerzos para proteger los datos personales y financieros, al parecer no han sido suficientes para protegerse de los ciberataques. Uno de los ataques más peligros es la suplantación de identidad llamado también phishing.

2.1.4. Origen de la Palabra Phishing

El término "Phishing" proviene de "fishing", que significa pescar en inglés. Se llama así porque busca "pescar" a los usuarios de Internet para que revelen información sensible. En otras palabras, los estafadores intentan que los usuarios caigan en la trampa y proporcionen dicha información. Sin embargo, también hay una razón por la cual se utiliza la letra "ph" en lugar de "f" en el término.

Esto se debe a que los primeros hackers eran conocidos como "phreaks", un término derivado de "phreaking", que se refiere al estudio y aprendizaje de nuevas tecnologías. Tanto

"hacker" como "phreaker" han estado siempre estrechamente relacionados, y el uso de "PH" ayuda a asociar estos ataques con estas comunidades (Leguizamón, 2019).

En la actualidad, la forma más prevalente de phishing consiste en el envío masivo de correos electrónicos fraudulentos con el fin de obtener datos personales de los usuarios. A su vez, se emplean otras técnicas más sofisticadas, como la creación de sitios web falsos, la utilización de troyanos, key-loggers, así como el envío de mensajes SMS o la realización de llamadas telefónicas engañosas. Además del phishing, también se presentan estafas como el pharming, que redirige el tráfico a sitios web fraudulentos mediante ataques al servidor DNS.

Asimismo, está el vishing, que alienta al usuario a llamar a un número especificado en un correo electrónico para proporcionar información personal; y el smishing, que utiliza mensajes de texto para el mismo propósito.

Estas estafas pueden clasificarse según el método utilizado para obtener información o en función de los datos que intentan obtener, como el phishing bancario o el phishing en redes sociales. Se calcula que hay más de 10,000 modalidades de phishing, y la definición más referenciada es la ofrecida por el APWG, la cual ha sido actualizada y ampliada a lo largo del tiempo para reflejar la evolución de este tipo de fraude (Leguizamón, 2019).

Los ataques de phishing utilizan ingeniería social para obtener datos personales y credenciales financieras. Emplean correos electrónicos engañosos que redirigen a sitios web falsos, donde los consumidores son inducidos a revelar información confidencial, como contraseñas y números de tarjetas de crédito, los estafadores suelen utilizar nombres de bancos y minoristas para aumentar la credibilidad.

Las técnicas también pueden incluir la instalación de software malicioso, como troyanos, que registran las pulsaciones del teclado.

En años recientes, el término "phishing" ha cobrado cada vez más relevancia y notoriedad, debido a las enormes pérdidas económicas que provoca y a la mejora continua de sus técnicas, lo que ha supuesto un importante aumento del número de víctimas.

Este tipo de fraude, conocido como phishing, consiste en suplantar la identidad de una empresa o institución bancaria para engañar a la víctima. A través de este engaño, se induce a la persona a creer que está recibiendo una comunicación de una fuente legítima, la cual solicita su información personal.

Las víctimas creen que se trata de una comunicación legítima de una empresa o entidad jurídica, por lo tanto, proporcionan la información confidencial descrita anteriormente, sin darse cuenta de que están siendo objeto de una estafa.

Este enfoque funciona bien porque las personas tienden a confiar en las comunicaciones que parecen legítimas y, por lo tanto, entregan sus datos sin cuestionarlas.

Estos datos luego se utilizan para causar pérdidas financieras o daños a la víctima.

El phishing emplea una técnica conocida como "minería de contraseñas". Este tipo de fraude se caracteriza por la suplantación de la identidad de una empresa o institución bancaria, con el objetivo de engañar a la víctima.

A través de esta estrategia, se induce a la persona a creer que está recibiendo una comunicación de una fuente legítima que solicita su información personal.

Los correos electrónicos asociados a esta práctica contienen enlaces falsos que dirigen a los usuarios a páginas web fraudulentas, donde se les solicita información personal. Además, estos correos suelen utilizar tácticas persuasivas, como la advertencia de que es necesario proporcionar información actualizada para evitar la caducidad de los servicios bancarios.

Esta técnica resulta altamente efectiva, ya que las páginas web fraudulentas suelen ser muy similares a las legítimas, y los phishers emplean la imagen corporativa de la empresa en los correos electrónicos para generar mayor confianza.

Es importante destacar que este tipo de delito cibernético se distingue en cuatro dimensiones principales: primero, la manipulación social, que explota la interacción humana y las vulnerabilidades inherentes; segundo, la automatización, donde los phishers utilizan tecnología y comunicaciones avanzadas para enviar correos masivos; tercero, las comunicaciones electrónicas, que representan el medio principal a través del cual se ejecutan estos ataques, especialmente en Internet; y, finalmente, la suplantación de identidad, ya que los perpetradores necesitan hacerse pasar por una entidad legítima para llevar a cabo un ataque de manera efectiva.

2.1.5. Fases Del Phishing

Dado los importantes avances experimentados en el campo del phishing en los últimos años, varios estudios han identificado diferentes etapas en la comisión de este tipo de delito. Comprender estos pasos puede ayudar a prevenir y prevenir estos ataques.

Es esencial tener en cuenta que cada paso puede variar según la gravedad del ataque, los métodos empleados, la complejidad involucrada y las implicaciones para la víctima. En términos generales, podemos identificar seis etapas distintas.

2.1.5.1. Fase de Planificación. Como su nombre indica, esta fase corresponde a la preparación del ataque por parte del delincuente.

En este momento, el atacante elige a su víctima, determina el método que empleará y decide qué organización o empresa simulará para llevar a cabo el engaño, qué buscará para ataque y qué método utilizará para golpear.

Aquí es donde los phishers toman una de las decisiones más importantes: si atacar individualmente o en grupo. A partir de esta decisión, el atacante también considera qué datos quiere obtener: Dependiendo de si el objetivo son contraseñas de redes sociales, números de tarjetas bancarias o información personal, es crucial entender tanto el tipo de datos como la complejidad del ataque.

Además, se considera el nivel de complicidad y sacrificios involucrados, aspectos que están estrechamente vinculados a la modalidad de phishing empleada. Una vez que el delincuente ha tomado estas decisiones, evalúa los recursos disponibles para alcanzar sus objetivos.

A partir de estas elecciones, podemos clasificar el phishing en tres categorías: 1) víctimas de alta complejidad y baja cooperación, como en el caso de ataques a servidores DNS; 2) víctimas de complejidad media y cooperación media, que involucran malware; y 3) víctimas de baja complejidad y alta cooperación, típicamente asociadas a correos electrónicos.

2.1.5.2. Fase de preparación: En términos generales, las distinciones entre los tres tipos de phishing son mínimas en lo que respecta a su complejidad y grado de implicación, pero la ejecución del ataque, es decir, la forma en que se crea y ejecuta el ataque, es diferente.

Esto se debe a que el perpetrador tiene que utilizar diferentes medios dependiendo del tipo de información que quiera obtener, es decir, teniendo en cuenta las necesidades de cada delito individual.

Por ejemplo, si hablamos de destinatarios individuales, los correos electrónicos que se les envíen deberían ser más detallados, preparados y personalizados, ya que la víctima es más específica. Si se trata de un destinatario de grupo, el correo electrónico que les envíe no tiene por qué ser tan personal como si fuera un correo masivo. Un ejemplo de un ataque más personal en España en 2007 fue hacerse pasar por una oficina de impuestos con exactamente el mismo logo.

Aquí, a los usuarios se les dice que se les debe un reembolso de impuestos y se le redirige a un sitio web fraudulento mediante un enlace falso. Al acceder al sitio web, se solicita a los usuarios que llenen un formulario en el que deben proporcionar su información bancaria.

2.1.5.3. Etapa de ataque. Una vez que se envían estos correos electrónicos, los intentos de phishing que demandan una participación alta a moderada por parte de la víctima

se llevan a cabo, como abrir un enlace fraudulento y proporcionar información personal, tendrán éxito cuando queden atrapados.

Llegados a este punto, resulta interesante aprender a utilizar malware para llevar a cabo ataques de phishing. En otras palabras, ¿cuál es la "anatomía del phishing"? Se pueden identificar siete elementos fundamentales: el malware, la infección, la ejecución, la entrada de datos, el atacante y el servidor legítimo.

Es esencial destacar dos momentos clave en el proceso de infección: el instante en que el malware accede al sistema sin ejecutarse y el momento en que se activa el código malicioso.

2.1.5.4. Fase de recogida de datos. En la fase de adquisición de datos, como se mencionó previamente, se distinguen tres tipos de phishing. En el contexto de una colaboración media o alta por parte de la víctima, se anticipa que esta proporcione sus datos confidenciales, lo que facilita su obtención.

En contraste, en un ataque dirigido al servidor, el objetivo principal es ejecutar el malware para recopilar dicha información. El gráfico siguiente representa esta fase en relación con los distintos tipos de phishing.

2.1.6. Dimensiones

2.1.6.1. Protección de datos financiero y personales. Malwarebytes, (2024) proporciona consejos sobre cómo protegerse del phishing, una amenaza omnipresente que puede afectar a una variedad de dispositivos.

Destaca la importancia del juicio personal como primer paso en la defensa, pero también recomienda medidas adicionales para fortalecer la ciberseguridad. Se ha reconocido que el phishing afecta a dispositivos que van desde computadoras de escritorio hasta teléfonos inteligentes.

Aunque la mayoría de los navegadores web cuentan con herramientas para comprobar la seguridad de un enlace, es importante enfatizar que el criterio personal es esencial para protegerse.

Proporciona consejos específicos sobre cómo identificar y evitar el phishing, como no abrir correos electrónicos de remitentes desconocidos, no hacer clic en enlaces de correo electrónico a menos que sepa su destino exacto y usar un navegador web para acceder manualmente a enlaces desconocidos.

También es aconsejable comprobar las credenciales digitales de tu sitio web y asegurarte de que la URL comience con "HTTPS", lo que indica una conexión segura. Se recomienda software antimalware para agregar una capa adicional de protección. Estos programas pueden ayudar a detectar enlaces o archivos adjuntos maliciosos incluso en situaciones complejas de phishing.

En general, este artículo proporciona una guía práctica para evitar trampas de phishing, enfatizando la importancia de la vigilancia constante y el uso de herramientas de seguridad en línea.

2.1.6.2. Gestión de riesgos. De acuerdo a los descrito se puede considerar que la gestión de riesgos en plataformas de pago móvil es un aspecto crítico para asegurar tanto la seguridad como la integridad de las transacciones financieras. Aquí hay algunos aspectos importantes a considerar en la gestión de riesgos en este contexto: Seguridad de la plataforma:

Es fundamental evaluar y mejorar constantemente la seguridad de la plataforma de pago móvil en sí misma. Esto requiere la implementación de medidas de seguridad sólidas, como el cifrado de datos, la autenticación de dos factores y sistemas de detección de fraudes, con el fin de salvaguardar la información financiera y personal de los usuarios.

Autenticación y autorización: Es fundamental implementar procesos de autenticación robustos que validen la identidad de los usuarios antes de concederles acceso a la plataforma o permitirles llevar a cabo transacciones.

Asimismo, es crucial asegurarse de que únicamente los usuarios autorizados tengan la capacidad de realizar acciones específicas como transferencias de fondos o cambios en la configuración de la cuenta. Monitoreo de transacciones: Es fundamental implementar procesos de autenticación robustos que validen la identidad de los usuarios antes de concederles acceso a la plataforma o permitirles llevar a cabo transacciones.

Asimismo, es crucial asegurarse de que únicamente los usuarios autorizados tengan la capacidad de realizar acciones específicas. Esto puede incluir la identificación de patrones inusuales de actividad, el seguimiento de transacciones de alto riesgo y la notificación rápida, es esencial educar y concienciar a los usuarios acerca de las mejores prácticas de seguridad para que puedan identificar y responder adecuadamente a posibles amenazas y los riesgos asociados con el uso de plataformas de pago móvil. Esto incluye la importancia de proteger sus credenciales de inicio de sesión, evitar el acceso a la plataforma desde dispositivos no seguros y estar atentos a posibles signos de actividad fraudulenta.

Colaboración con reguladores y entidades de seguridad: Las empresas que operan plataformas de pago móvil deben trabajar en estrecha colaboración con reguladores y entidades de seguridad cibernética para asegurar que se cumplan las normativas y estándares de seguridad pertinentes.

Esto podría abarcar la implicación en programas de certificación de seguridad y la cooperación en investigaciones de incidentes de seguridad. Respaldo y recuperación ante desastres: Es importante tener planes de contingencia en su lugar para abordar eventuales incidentes de seguridad, tales como violaciones de datos o interrupciones en el servicio. Esto puede implicar la implementación de sistemas de respaldo de datos, la capacitación del

personal en procedimientos de respuesta a incidentes y la realización de pruebas regulares de recuperación ante desastres.

2.1.6.3. Seguridad y Protección. International Business Machines Corporation [IBM] (2024) El texto aborda la importancia de educar a los usuarios sobre las estafas de phishing y desarrollar prácticas efectivas para lidiar con mensajes sospechosos, particularmente correos electrónicos y mensajes de texto. A continuación, se analizan los puntos clave del texto:

Identificación de señales de phishing: Se destacan diversas señales que pueden indicar la presencia de un correo electrónico de phishing, como solicitudes de información personal o financiera, sensación de urgencia, errores gramaticales, uso de servicios de acortamiento de enlaces y empleo de imágenes de texto en lugar de texto real.

Esta lista no es exhaustiva, ya que los piratas informáticos están en constante evolución, pero actúa como base para la formación de los usuarios. En este sentido, la capacitación continua es esencial, ya que permite a los usuarios mantenerse actualizados sobre las últimas tácticas de phishing. Además, se señala que recursos como informes sobre tendencias de phishing pueden ser útiles para que las organizaciones se mantengan actualizadas sobre las amenazas más recientes.

Prácticas recomendadas: El texto sugiere varias prácticas recomendadas para reducir el riesgo de caer en ataques de phishing, como establecer políticas claras sobre comunicaciones financieras por correo electrónico, requerir que los empleados confirmen solicitudes de información confidencial a través de canales alternativos y fomentar una cultura de reporte de intentos de phishing sospechosos al equipo de TI o seguridad.

2.1.6.4. Cumplimiento normativo. Respeto a lo referente al cumplimiento normativo Kobra (2024) refiere los siguiente: En lo referente al “cumplimiento normativo” trata sobre acciones y protocolos que una institución financiera emprende para garantizar el cumplimiento

de las leyes, regulaciones y estándares establecidos por las entidades y autoridades responsables de guiar y supervisar los procedimientos a seguir.

Dichas normas abarcan múltiples áreas, incluyendo la prevención del blanqueo de capitales, la protección de los derechos del consumidor, la seguridad de la información y la gestión de riesgos. Asimismo, agrega que el cumplimiento normativo es fundamental por diversas razones:

a) Protección al consumidor: La observancia de la regulación garantiza que las instituciones financieras actúen con claridad y honestidad, salvaguardando así los intereses de los clientes y protegiéndolos contra posibles engaños, abusos o conductas fraudulentas;

b) Prevención de actividades ilícitas: La supervisión regulatoria contribuye a prevenir delitos como el blanqueo de capitales, la financiación del terrorismo y otras acciones delictivas. A través de estrictos protocolos de supervisión y diligencia debida, las instituciones financieras ayudan a identificar y evitar operaciones ilícitas.

(c) Estabilidad financiera: El cumplimiento de las normativas regulatorias fomenta la estabilidad y robustez del sistema financiero al imponer requisitos de capital, liquidez y gestión de riesgos.

De este modo, disminuye la posibilidad de crisis financieras y salvaguarda la economía en su totalidad.

2.1.6.5. Políticas de privacidad y datos personales – YAPE. Las políticas de privacidad y protección de datos personales son esenciales en toda plataforma de pago móvil, incluyendo YAPE. Aunque las políticas específicas pueden variar con el tiempo y estar sujetas a actualizaciones, a continuación, se presentan algunos aspectos generales que suelen estar incluidos en las políticas de privacidad de YAPE: Recopilación de datos personales: YAPE recoge información personal de los usuarios durante el registro y uso de la plataforma. Esto puede abarcar datos como nombres, números de teléfono, direcciones de correo electrónico y

detalles de cuentas bancarias vinculadas y otros detalles necesarios para facilitar las transacciones.

Uso de la información: La información personal recopilada por YAPE se utiliza principalmente para proporcionar y mejorar los servicios ofrecidos. Esto puede incluir la realización de transacciones, la personalización de la experiencia del usuario, la mitigación de fraudes y el fortalecimiento de la seguridad de la plataforma.

Compartir información: YAPE puede compartir información personal de los usuarios con proveedores de servicios externos, instituciones financieras y organismos gubernamentales, cumpliendo con la legislación vigente, con el objetivo de asegurar la seguridad de las transacciones y para otros propósitos comerciales válidos.

Seguridad de los datos: YAPE aplica medidas de seguridad técnicas, administrativas y físicas para proteger la información personal de los usuarios, utilizando cifrado, firewalls y autenticación. Además, los usuarios tienen derechos sobre sus datos, incluyendo acceso, rectificación, eliminación y portabilidad de la información.

Las políticas de privacidad de YAPE suelen incluir información sobre cómo ejercer estos derechos permiten a los usuarios conocer cómo acceder a la plataforma para recibir asistencia.

Es fundamental que los usuarios consulten las políticas de privacidad y protección de datos de YAPE para entender mejor sus derechos y opciones disponibles., así como cualquier actualización o cambio en las mismas, para comprender cómo se recopila, utiliza y protege su información personal en la plataforma. (Yape, 2024).

2.1.6.6. Educación y concienciación. La educación y la conciencia sobre la seguridad de las plataformas de pago móvil son aspectos fundamentales en la actualidad, dada la creciente adopción de estas tecnologías y los riesgos asociados con su uso. A continuación, se analizan estos puntos:

Educación sobre seguridad: Es crucial proporcionar a los usuarios información detallada sobre cómo utilizar de manera segura las plataformas de pago móvil. Esto incluye instrucciones sobre cómo configurar medidas de seguridad, como contraseñas fuertes y autenticación de dos factores, así como también sobre cómo identificar posibles amenazas, como el phishing o el malware.

Conciencia sobre riesgos: Los usuarios deben estar al tanto de los riesgos potenciales asociados con el uso de plataformas de pago móvil, como el robo de información financiera, el fraude y el acceso no autorizado a las cuentas. La conciencia sobre estos riesgos puede ayudar a los usuarios a tomar medidas preventivas y a estar alerta ante posibles amenazas.

Formación en buenas prácticas: Además de la educación sobre seguridad, es importante proporcionar formación en buenas prácticas de uso de plataformas de pago móvil. Esto puede incluir consejos sobre la protección de datos personales, la verificación de la autenticidad de las transacciones y la actualización regular de la aplicación y del dispositivo móvil.

Responsabilidad compartida: Tanto los proveedores de servicios de pago móvil como los usuarios tienen un papel que desempeñar en la seguridad de estas plataformas. Los proveedores deben implementar medidas robustas de seguridad y proporcionar actualizaciones regulares para proteger a los usuarios, mientras que los usuarios deben seguir las recomendaciones de seguridad y estar atentos a cualquier actividad sospechosa en sus cuentas (García, 2021).

2.1.7. Plataforma de pago móvil

El sistema de pagos móviles basado en SMS emplea un protocolo de telecomunicaciones que facilita el intercambio de mensajes de texto cortos entre dos dispositivos móviles (Zhang, 2020).

El tercer modelo de pagos móviles se fundamenta en el uso de códigos QR. Un código QR es un sistema que almacena información en dos dimensiones y puede ser impreso o

exhibido en una pantalla, permitiendo su lectura a través de un software especializado (Zhang, 2020).

2.1.8. Protección de datos personas y financiero

La preservación de la información personal ha sido crucial en tanto en las prácticas comerciales como en las disposiciones gubernamentales durante un período considerable, debido a la necesidad de salvaguardar los datos de personas, instituciones y entidades en el entorno digital.

Sin embargo, a día de hoy, los datos personales continúan expuestos a riesgos como la filtración, el robo y la explotación indebida (SYDLE, 2023).

2.1.9. Phishing

El phishing representa una estrategia empleada por criminales cibernéticos con el propósito de engañar a los usuarios y adquirir datos sensibles, tales como contraseñas o información de tarjetas de crédito.

En el contexto de las plataformas de pago móvil, los delincuentes a menudo envían correos electrónicos o mensajes de texto falsificados que simulan ser originados por la entidad legítima, solicitando datos personales o financieros. Una vez que los usuarios comparten dicha información, los estafadores la utilizan con fines fraudulentos. (IBM, 2024).

III. MÉTODO

3.1. Tipo de investigación

La investigación es de tipo aplicada es un enfoque que tiene como objetivo solucionar problemas prácticos y concretos utilizando conocimientos teóricos. A diferencia de la investigación básica, que se enfoca en crear nuevas teorías o conocimientos sin un uso inmediato, la investigación aplicada se dirige a implementar soluciones en contextos específicos (Valderrama, 2019).

El nivel es correlacional se refiere a un tipo de diseño de investigación que tiene como objetivo identificar y analizar la relación entre dos o más variables. En este enfoque, no se determina una relación de causa y efecto, sino que se estudia cómo las variables cambian en conjunto (Valderrama y Jaimes, 2019).

3.2. Población y muestra

3.2.1. Población

La población fue conformada por 200 alumnos de la de la facultad de administración de la universidad Nacional Mayor de San Marcos.

3.2.2. Muestra

Para la muestra se procederá a tomar toda la población, convirtiéndose en una muestra de tipo censal. La muestra queda conformada por 200 estudiantes de la Facultad de administración (Hernández y Mendoza, 2018).

3.3 Operacionalización de variables

Matriz de Operacionalización de las Variables					
Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medida
SEGURIDAD DE LAS PLATAFORMAS DE PAGO MÓVIL	La seguridad de las plataformas de pago móvil se refiere al conjunto de medidas, políticas y tecnologías diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información y transacciones realizadas a través de aplicaciones y servicios de pago móvil (Ciberseguridad, 2024)	La seguridad de las plataformas de pago móvil puede operacionalizarse mediante la implementación de diversas medidas y controles, que pueden incluir: Encriptación de datos, Autenticación multifactor, Monitoreo de seguridad y Actualizaciones de seguridad.	Seguridad de la transacción	Autenticación multifactor Tokenización de datos Detección de fraudes en tiempo real.	Ordinal Totalmente en desacuerdo (1) En desacuerdo (2) Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)
			Protección de datos personales	Nombres Direcciones Números de teléfono Detalles de las tarjetas de crédito	Totalmente en desacuerdo (1) En desacuerdo (2) Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)
			Seguridad del dispositivo	Implementación de medidas de seguridad Bloqueo de pantalla detección de malware Actualizaciones regulares del sistema operativo Protección contra el rooteo o jailbreaking	
			Autenticación segura	Autenticación biométrica Contraseñas robustas Códigos de verificación únicos.	Totalmente en desacuerdo (1) En desacuerdo (2)

			Protección contra fraudes	-Monitoreo de patrones de comportamiento sospechoso - Análisis de datos en tiempo real y Colaboración con redes de tarjetas.	Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)

Matriz de Operacionalización de las Variables:					
Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medida
CONOCIMIENTO SOBRE LA PROTECCIÓN DE LOS DATOS FINANCIEROS Y PERSONALES	El conocimiento sobre la protección de los datos financieros y personales es la comprensión profunda y completa de los principios, normativas, tecnologías, prácticas y medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información financiera y personal de los individuos.	Evaluar el grado en que un individuo conoce y comprende cada Una de las dimensiones como es la gestión de riesgo, la tecnología y seguridad de la información, la legislación y regulación, así como la educación y conciencia sobre protección de datos financieros y personales.	Gestión de Riesgos	- Frecuencia y gravedad de incidentes de seguridad de datos. - Eficacia de los controles de seguridad implementados (por ejemplo, tasa de detección de amenazas). - Tiempo medio para detectar y responder a incidentes de seguridad. - Evaluaciones periódicas de riesgos y vulnerabilidades.	Totalmente en desacuerdo (1) En desacuerdo (2) Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)
			Tecnología y seguridad de la información	- Nivel de cumplimiento con los estándares de seguridad de la información (por ejemplo, ISO 27001). - Eficiencia de los sistemas de detección y prevención de intrusiones. - Tasa de actualización y parcheo de sistemas y software. - Evaluación de la efectividad de la encriptación de datos. - Nivel de cumplimiento con las mejores prácticas de seguridad de la información.	Totalmente en desacuerdo (1) En desacuerdo (2) Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)
			Legislación y regulación	- Nivel de cumplimiento con las normativas de protección de datos aplicables (por ejemplo, RGPD, CCPA).	Totalmente en desacuerdo (1) En desacuerdo (2)

				- Frecuencia y gravedad de las infracciones de datos y sanciones asociadas.	Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)
			Educación y concienciación	- Participación en programas de formación sobre seguridad de la información. - Concienciación sobre seguridad de datos. - Nivel de comprensión de los usuarios sobre políticas y procedimientos de seguridad de datos. - Conocimiento sobre incidentes de seguridad y mejores prácticas. - Nivel de implicación y responsabilidad de los usuarios en la protección de datos.	Totalmente en desacuerdo (1) En desacuerdo (2) Ni de acuerdo ni en desacuerdo (3) De acuerdo (4) Totalmente de acuerdo (5)

3.4. Instrumentos

El tipo de instrumento utilizado en esta investigación es un cuestionario y la técnica es la encuesta.

Este instrumento se emplea para recopilar datos sobre el nivel de conocimiento sobre vulnerabilidad de la plataforma móvil y protección de datos financieros y personales, entre los participantes de la UNMSM (Gamarra et al., 2015).

El cuestionario constará de una serie de preguntas estructuradas, diseñadas específicamente para medir las variables de interés en la investigación.

Las preguntas incluirán ítems sobre el de los participantes en relación con la protección de datos, su experiencia previa con plataformas de pago móvil, la frecuencia con la que utilizan estos servicios, y su percepción sobre la seguridad y privacidad de los mismos.

El instrumento incluirá preguntas cerradas, que ofrecen opciones de respuesta predeterminadas, así como preguntas abiertas, que permiten a los participantes proporcionar respuestas más detalladas y personales (Hernández, 2021).

Esta combinación facilitará una comprensión más profunda de las actitudes, percepciones y experiencias de los participantes respecto al tema de estudio.

3.5. Procedimientos

Preparación del Instrumento: Antes de aplicar el instrumento, se debe asegurar que esté correctamente diseñado y validado.

Esto implica revisar las preguntas para garantizar su claridad, relevancia y adecuación a los objetivos de la investigación.

Además, se debe establecer un sistema de codificación para facilitar el análisis posterior de los datos.

Administración del Instrumento: El instrumento se administró a los participantes de manera presencial y en línea, teniendo en cuenta la logística y las preferencias de los sujetos.

Se proporcionará instrucciones claras sobre cómo completar el instrumento y se asegurará de que los participantes tengan tiempo suficiente para responder a todas las **preguntas.**

3.6. Análisis de datos

Las tablas de frecuencias son herramientas estadísticas que organizan y resumen datos, mostrando cuántas veces aparece cada valor o categoría en un conjunto específico (Sánchez, 2019).

Cada fila incluye la categoría o valor analizado, la frecuencia absoluta que indica cuántas veces se presenta, y la frecuencia relativa que muestra su proporción respecto al total.

Por otro lado, un gráfico de barras es una representación visual que utiliza barras rectangulares para ilustrar la frecuencia de diversas categorías.

En este gráfico, el eje vertical representa la frecuencia y el eje horizontal las categorías, con cada barra reflejando la frecuencia correspondiente y separadas para destacar que representan grupos distintos. Estas herramientas son efectivas para comparar grupos y visualizar tendencias en los datos (Sánchez et al., 2023).

El coeficiente de correlación de Spearman, se emplea para evaluar la fuerza y dirección de la relación entre dos variables ordinales o cuando los datos no cumplen los requisitos de normalidad del coeficiente de Pearson (Otzen y Manterola, 2017).

Resulta particularmente útil para datos ordinales, ya que permite clasificar las variables en un orden sin requerir que las distancias entre los rangos sean constantes.

3.7. Consideraciones éticas (de ser necesario)

Consentimiento Informado: Se obtendrá el consentimiento informado de todos los participantes, a quienes se les explicarán claramente los objetivos, procedimientos y posibles riesgos de su participación.

Los participantes podrán retirarse del estudio en cualquier momento sin enfrentar consecuencias negativas.

Además, se asegurará la confidencialidad de la información recopilada, protegiendo la identidad de los participantes y utilizando códigos numéricos o pseudónimos en lugar de datos personales en los informes y análisis.

Se tomarán medidas para asegurar la protección de los datos financieros y personales recopilados durante el estudio.

Beneficencia y No Maleficencia: Se asegurará de que el estudio beneficie a la comunidad universitaria y contribuya al avance del conocimiento en el campo de la protección de datos financieros y personales.

Se minimizarán los riesgos para los participantes y se tomarán medidas para evitar cualquier forma de daño o perjuicio.

Imparcialidad y Rigor Científico: Se mantendrá la imparcialidad en la recopilación y análisis de datos, evitando cualquier sesgo o conflicto de intereses.

Se seguirán estándares éticos y metodológicos rigurosos en todas las etapas del estudio se busca asegurar la validez y fiabilidad de los resultados.

En cuanto a la divulgación de los hallazgos, estos se presentarán de manera clara, precisa y accesible, tanto a los participantes del estudio como a la comunidad científica y al público en general.

Se promoverá la transparencia y la responsabilidad en la divulgación de los hallazgos, evitando la distorsión o exageración de los mismos.

Supervisión Ética: Se establecerá un comité de ética o se obtendrá la aprobación de un comité de ética existente para supervisar y evaluar la conducta ética del estudio, así como para abordar cualquier preocupación ética que pueda surgir durante su realización.

IV. RESULTADOS

En el contexto actual, la utilización de plataformas de pago móvil ha crecido exponencialmente, convirtiéndose en una parte integral de las transacciones financieras diarias. Sin embargo, este aumento en la adopción también ha traído consigo preocupaciones significativas sobre la seguridad de los datos y las transacciones realizadas a través de estas plataformas. Con el objetivo de comprender mejor el comportamiento de los usuarios y sus percepciones respecto a la seguridad en el uso de estas herramientas, se llevó a cabo una encuesta que analiza diferentes aspectos relacionados con la seguridad de las transacciones en línea.

Los resultados presentados a continuación ofrecen una visión integral sobre la frecuencia de uso de las plataformas de pago móvil, el nivel de preocupación de los usuarios en relación con la seguridad de sus transacciones, las medidas de seguridad que consideran más relevantes, así como su experiencia con incidentes de fraude o actividad sospechosa. Estos hallazgos son fundamentales para identificar áreas de mejora y diseñar estrategias que fortalezcan la confianza de los usuarios en el uso de estas plataformas, promoviendo así una cultura de seguridad en el entorno digital. A continuación, se detallan los resultados obtenidos en la encuesta.

4.1. Análisis descriptivo de resultados

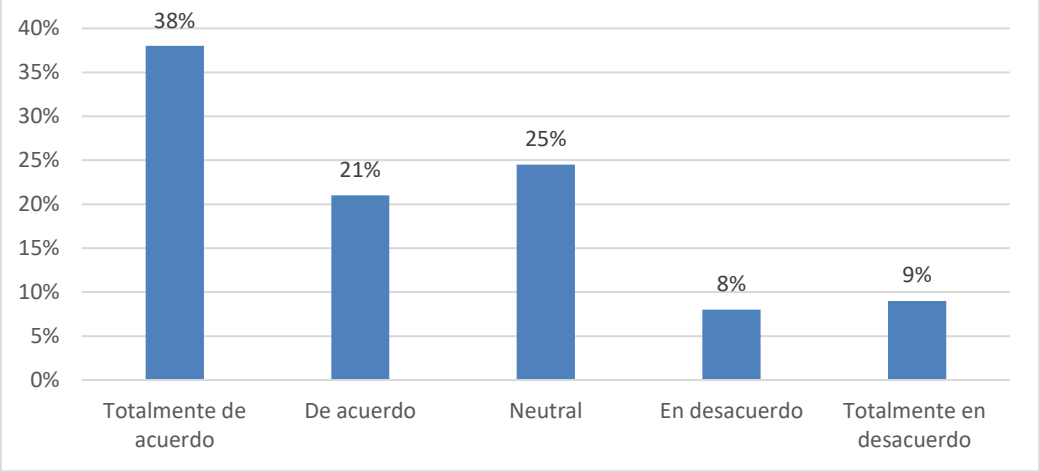
Tabla 1

Plataforma de pago móvil

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	76	38
	De acuerdo	42	21
	Neutral	49	25
	En desacuerdo	16	8
	Totalmente en desacuerdo	17	9
	Total	200	100

Figura 1

Plataforma de pago móvil



Nota. La tabla indica que el 38% de los encuestados se siente "totalmente de acuerdo" en que las plataformas de pago móvil son seguras, mientras que un 21% está "de acuerdo". Sin embargo, un 25% permanece neutral y un 17% manifiesta desacuerdo, lo que sugiere una falta de confianza general en su seguridad. A pesar de las preocupaciones sobre fraudes y la protección de datos personales, muchos consideran cruciales medidas como la autenticación de dos factores y la encriptación. También se reconoce que Yape y Plin podrían fortalecer su defensa contra la suplantación de identidad mediante una mayor educación y sensibilización.

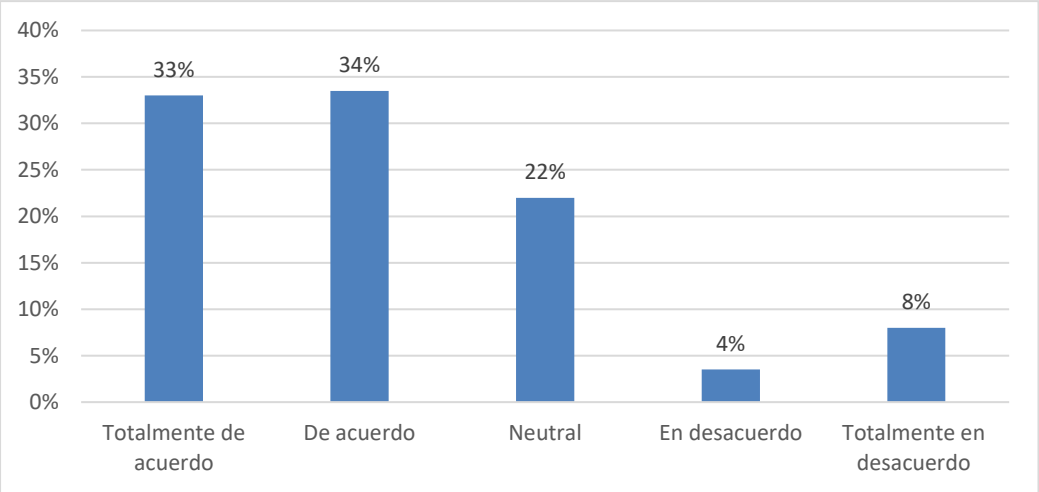
Tabla 2

Seguridad de la Transacción

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	66	33
	De acuerdo	67	34
	Neutral	44	22
	En desacuerdo	7	4
	Totalmente en desacuerdo	16	8
	Total	200	100

Figura 2

Seguridad de la Transacción



Nota. Los datos indican que un 33% de los encuestados se siente "totalmente de acuerdo" y un 34% "de acuerdo" con la afirmación sobre la seguridad de las plataformas de pago móvil, lo que sugiere una percepción mayormente positiva. Sin embargo, un 22% se muestra neutral y un 12% expresa algún grado de desacuerdo (4% en desacuerdo y 8% totalmente en desacuerdo), lo que revela ciertas inquietudes sobre la vulnerabilidad de estas plataformas. A pesar de estas preocupaciones, muchos reconocen la importancia de medidas de seguridad como la autenticación de dos factores, la encriptación de datos y la educación sobre prácticas seguras.

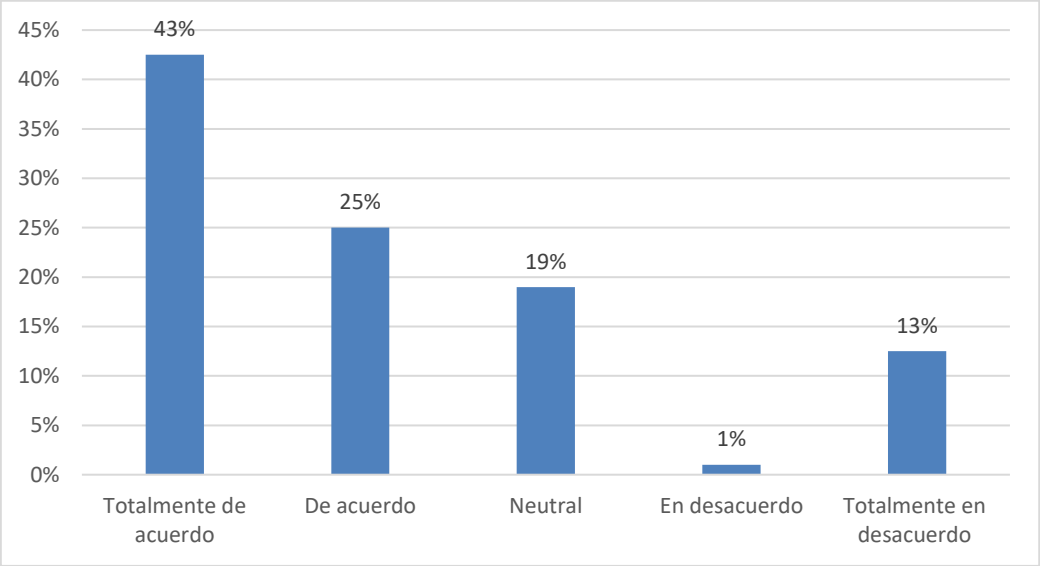
Tabla 3

Protección de Datos Personales

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	85	43
	De acuerdo	50	25
	Neutral	38	19
	En desacuerdo	2	1
	Totalmente en desacuerdo	25	13
	Total	200	100

Figura 3

Protección de Datos Personales



Nota. La tabla indica que un 43% de los encuestados está "totalmente de acuerdo" y un 25% "de acuerdo" en que toman medidas para proteger sus datos personales en línea, lo que sugiere una actitud generalmente positiva hacia la privacidad y la seguridad. Un 19% se muestra neutral, mientras que solo un 14% expresa desacuerdo (1% en desacuerdo y 13% totalmente en desacuerdo), lo que implica que, aunque la mayoría está comprometida con la protección de su información, hay un pequeño grupo que podría no estar tomando las precauciones adecuadas.

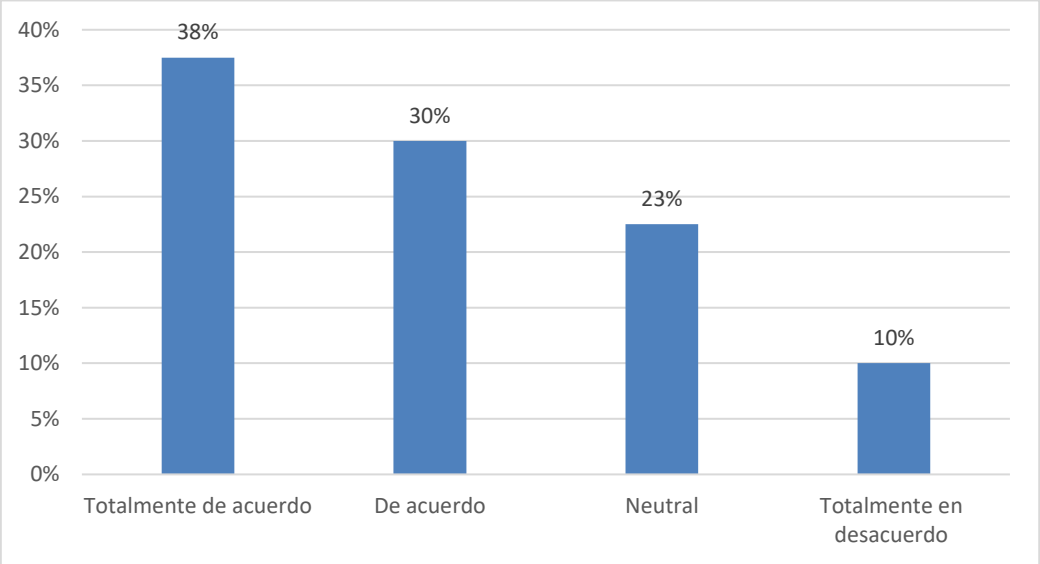
Tabla 4

Seguridad del Dispositivo

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	75	38
	De acuerdo	60	30
	Neutral	45	23
	Totalmente en desacuerdo	20	10
	Total	200	100

Figura 4

Porcentaje Seguridad del Dispositivo



Nota. La tabla revela que un 38% de los encuestados está "totalmente de acuerdo" y un 30% "de acuerdo" en la importancia de la seguridad de sus dispositivos, lo que indica una percepción positiva hacia la protección de su información. Un 23% se muestra neutral, mientras que un 10% expresa desacuerdo, lo que sugiere que, aunque la mayoría valora la seguridad, existe un porcentaje que podría no estar completamente comprometido.

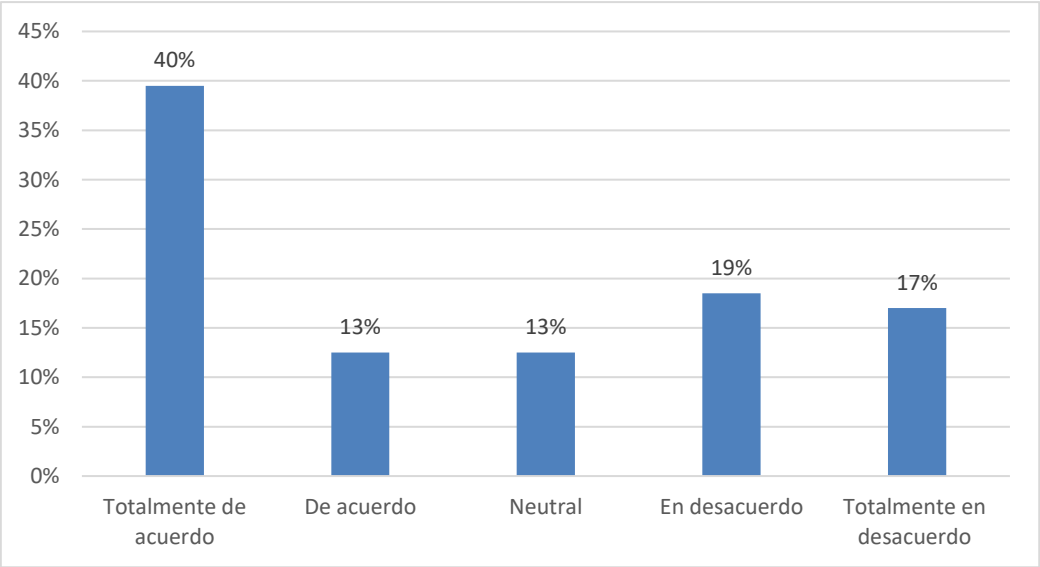
Tabla 5

Autenticación

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	79	40
	De acuerdo	25	13
	Neutral	25	13
	En desacuerdo	37	19
	Totalmente en desacuerdo	34	17
	Total	200	100

Figura 5

Porcentaje de Autenticación



Nota. La tabla indica que un 40% de los encuestados está "totalmente de acuerdo" y un 13% "de acuerdo" en que la autenticación de dos factores brinda una protección efectiva para sus cuentas en línea. Un 13% se muestra neutral, mientras que un 36% tiene algún nivel de desacuerdo (19% en desacuerdo y 17% totalmente en desacuerdo).

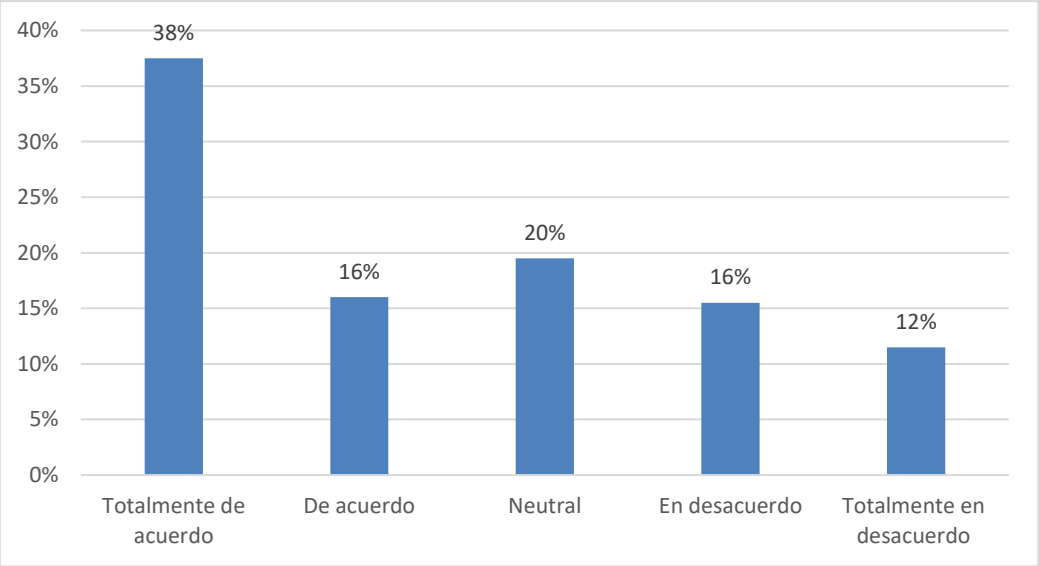
Tabla 6

Protección contra Fraudes

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	75	38
	De acuerdo	32	16
	Neutral	39	20
	En desacuerdo	31	16
	Totalmente en desacuerdo	23	12
	Total	200	100

Figura 6

Porcentajes Protección contra Fraudes



Nota. La tabla indica que un 38% de los encuestados está "totalmente de acuerdo" y un 16% "de acuerdo" en que han recibido información útil sobre cómo reconocer y evitar intentos de suplantación de identidad al usar Yape y Plin. Un 20% se muestra neutral, mientras que un 28% expresa algún grado de desacuerdo (16% en desacuerdo y 12% totalmente en desacuerdo). Esto sugiere que, aunque una parte significativa se siente bien informada, hay un porcentaje notable que cuestiona la efectividad de la protección que ofrecen estas plataformas.

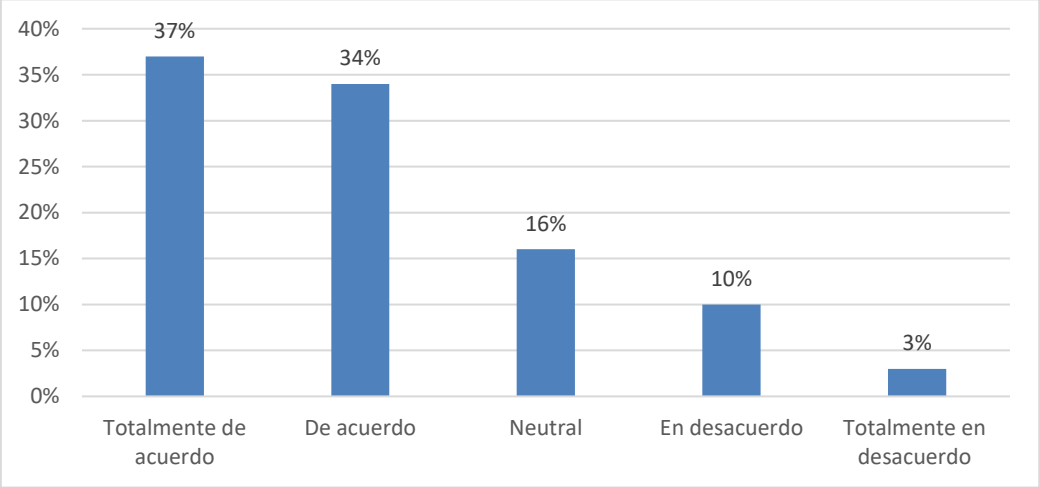
Tabla 7

Nivel de conocimiento sobre la protección de datos financieros y personales

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	74	37
	De acuerdo	68	34
	Neutral	32	16
	En desacuerdo	20	10
	Totalmente en desacuerdo	6	3
	Total	200	100

Figura 7

Nivel de protección de datos financieros y personales



Nota. La tabla muestra que un 37% de los encuestados se siente "totalmente de acuerdo" y un 34% "de acuerdo" en que poseen un adecuado conocimiento sobre la protección de datos financieros y personales. Un 16% se mantiene neutral y un 13% expresa desacuerdo. Esto sugiere que, aunque la mayoría se siente segura sobre su conocimiento en seguridad de datos, hay un porcentaje notable que podría no estar tan informado. Los encuestados realizan evaluaciones de riesgo y confían en sus medidas de seguridad, pero también reconocen la importancia de mantenerse actualizados sobre amenazas y participar en programas de formación, reflejando una responsabilidad personal en la protección de sus datos.

4.2. Contraste de las hipótesis

4.2.1. Hipótesis general

Ha. Existe relación positiva entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 8

Contraste de la hipótesis general

			Plataforma de pago móvil (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Plataforma de pago móvil (agrupado)	Coeficiente de correlación	1,000	,812
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,812	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se encuentra un coeficiente de correlación de Spearman de 0.812, indicando una fuerte relación positiva entre las variables. La significancia bilateral de 0.000 respalda la relevancia estadística de esta correlación. Por lo tanto, se rechaza la hipótesis nula (Ho) y se confirma la relación entre el uso de plataformas de pago móvil y el conocimiento sobre protección de datos.

4.2.2. Hipótesis específica 1

Ha. Existe relación positiva entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 9

Contraste de la hipótesis específica 1

			Seguridad de la transacción (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Seguridad de la transacción (agrupado)	Coeficiente de correlación	1,000	,768
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,768	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se observa un coeficiente de correlación de Spearman de 0.768, indicando una relación positiva significativa entre las variables. La significancia bilateral de 0.000 respalda su relevancia estadística. Así, se rechaza la hipótesis nula (Ho) y se confirma la relación entre la seguridad de transacciones y el conocimiento sobre protección de datos.

4.2.3. Hipótesis específica 2

Ha. Existe relación positiva entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 10

Contraste de la hipótesis específica 2

			Protección de datos personales (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Protección de datos personales (agrupado)	Coeficiente de correlación	1,000	,762
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,762	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se encuentra un coeficiente de correlación de Spearman de 0.762, sugiriendo una relación positiva significativa entre las variables. La significancia bilateral de 0.000 confirma su relevancia estadística. Así, se rechaza la hipótesis nula (Ho) y se concluye que hay una relación positiva entre la protección de datos y el conocimiento sobre este tema.

4.2.4. Hipótesis específica 3

Ha. Existe relación positiva entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 11

Contraste de la hipótesis específica 3

			Seguridad del dispositivo (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Seguridad del dispositivo (agrupado)	Coeficiente de correlación	1,000	,767
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,767	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se reporta un coeficiente de correlación de Spearman de 0.767, indicando una relación positiva significativa entre las variables. La significancia bilateral de 0.000 respalda su relevancia estadística. Por lo tanto, se rechaza la hipótesis nula (Ho) y se concluye que existe una relación positiva entre la seguridad del dispositivo y el conocimiento sobre protección de datos.

4.2.5. Hipótesis específica 4

Ha. Existe relación positiva entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 12

Contraste de la hipótesis específica 4

			Autenticación segura (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Autenticación segura (agrupado)	Coeficiente de correlación	1,000	,758
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,758	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se presenta un coeficiente de correlación de Spearman de 0.758, sugiriendo una relación positiva significativa entre las variables. La significancia bilateral de 0.000 respalda su validez estadística. Así, se rechaza la hipótesis nula (Ho) y se concluye que hay una relación positiva entre la autenticación segura y el conocimiento sobre protección de datos.

4.2.6. Hipótesis específica 5

Ha. Existe relación positiva entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Ho. No existe relación positiva entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.

Tabla 13

Contraste de la hipótesis específica 5

			Protección contra fraudes (agrupado)	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)
Rho de Spearman	Protección contra fraudes (agrupado)	Coeficiente de correlación	1,000	,680
		Sig. (bilateral)	.	,000
		N	200	200
	Nivel de conocimiento sobre protección de datos financieros y personales (agrupado)	Coeficiente de correlación	,680	1,000
		Sig. (bilateral)	,000	.
		N	200	200

Nota. Se encuentra un coeficiente de correlación de Spearman de 0.680, lo que sugiere una relación positiva considerable entre las variables. La significancia bilateral de 0.000 confirma su relevancia estadística. Así, se rechaza la hipótesis nula (Ho) y se concluye que hay una relación positiva entre la protección contra fraudes y el conocimiento sobre protección de datos.

V. DISCUSIÓN DE RESULTADOS

Los resultados asociados con la teoría de la adopción de tecnología (TAM) pueden indicar que la facilidad de uso y la utilidad percibida son factores clave en la adopción de plataformas de pago móvil por los estudiantes.

Si los encuestados consideran que estas plataformas son fáciles de usar y mejoran la eficiencia en sus transacciones diarias, esto puede explicar una alta tasa de adopción. Sin embargo, si se encuentran obstáculos en términos de complejidad o falta de funcionalidad, esto sugiere que es necesario implementar estrategias de capacitación para aumentar su aceptación.

En relación con la teoría de la seguridad de la información, los hallazgos pueden mostrar que la percepción de seguridad impacta significativamente la confianza de los estudiantes en las plataformas de pago.

Si muchos participantes expresan preocupación por la seguridad de sus datos financieros, esto señala una falta de comunicación sobre las medidas de protección que las plataformas ofrecen.

Por lo tanto, es fundamental que las instituciones educativas y las empresas tecnológicas colaboren en la educación y la transparencia respecto a las prácticas de seguridad para fortalecer la confianza del usuario.

La teoría de la privacidad de la información también puede reflejarse en los resultados. Si los estudiantes muestran un bajo nivel de conocimiento sobre sus derechos de privacidad y el control sobre sus datos personales, esto pone de manifiesto la necesidad de desarrollar programas educativos que informen sobre la gestión de la privacidad en el entorno digital.

La falta de comprensión sobre el manejo de sus datos podría estar limitando su disposición a usar las plataformas de pago, a pesar de que las perciban como útiles.

Finalmente, al aplicar la teoría del riesgo y la confianza, los resultados pueden indicar que los estudiantes evalúan los riesgos asociados al uso de plataformas de pago móvil y, en función de esta evaluación, forman su nivel de confianza.

Si los hallazgos revelan que los participantes tienden a evitar estas plataformas por temor a fraudes o pérdidas de información, es crucial implementar campañas que informen sobre los riesgos y, al mismo tiempo, resalten las medidas de seguridad y los beneficios de su uso.

La primera discusión, señala que es significativo que un 38% de los encuestados se siente "totalmente de acuerdo" en que estas plataformas son seguras, mientras que un 21% se declara "de acuerdo". Sin embargo, el 25% que se mantiene neutral y el 17% que expresa desacuerdo indican una percepción general de inseguridad que podría limitar la adopción plena de estas herramientas.

Este fenómeno está alineado con lo señalado por Castro (2019), quien enfatiza la necesidad de abordar los desafíos relacionados con la protección de datos en entornos automatizados.

La preocupación por el acceso no autorizado y el uso indebido de la información es evidente entre los usuarios, lo que resalta la importancia de implementar medidas sólidas como la autenticación de dos factores y la encriptación.

Estas estrategias son consideradas fundamentales por los encuestados, lo que sugiere que, a pesar de la desconfianza, existe un reconocimiento de la necesidad de acciones efectivas para mitigar riesgos.

El análisis estadístico, que muestra un coeficiente de correlación de Spearman de 0.812. Este hallazgo se alinea con las observaciones de Juli (2024) sobre la relevancia de la inclusión financiera, donde el conocimiento se presenta como un habilitador crucial para acceder a servicios financieros.

Además, se hace evidente la necesidad de aumentar la educación y sensibilización en torno a las plataformas de pago móvil.

Las respuestas indican que iniciativas similares a las de Action Bank, enfocadas en promover la inclusión financiera, podrían ser útiles en el contexto de las aplicaciones de pago.

La formación y capacitación de los usuarios en temas de privacidad y seguridad de la información son vitales, no solo para fomentar una mayor confianza en estas plataformas, sino también para promover un uso responsable y seguro de las tecnologías.

En la segunda discusión, un 33% de los encuestados se siente "totalmente de acuerdo" con que estas plataformas son seguras.

Sin embargo, un 22% mantiene una postura neutral y un 12% manifiesta algún grado de desacuerdo.

Esto sugiere que, aunque la mayoría confía en las plataformas de pago móvil, también existen preocupaciones sobre su vulnerabilidad.

A pesar de estas inquietudes, es alentador que muchos participantes reconozcan la importancia de adoptar medidas de seguridad, como la autenticación de dos factores, la encriptación de datos y la educación en prácticas seguras.

Estos hallazgos indican que, aunque hay una confianza general, también hay una creciente conciencia sobre los riesgos asociados y la necesidad de salvaguardar la información personal y financiera.

El análisis estadístico muestra un coeficiente de correlación de Spearman de 0.768. Estos resultados son coherentes con los hallazgos de García y Soto (2022), quienes destacan la importancia de la inclusión financiera en contextos de crecimiento constante y dificultades en el acceso a servicios financieros formales.

Su estudio, que identifica un impacto significativo del financiamiento de campañas en la inclusión financiera, sugiere que una mayor educación y sensibilización sobre la seguridad

en el uso de plataformas de pago móvil podría no solo fortalecer la confianza de los consumidores, sino también promover la inclusión financiera en áreas como Lima Norte.

Sobre la tercera discusión, un 43% se siente "totalmente de acuerdo" y un 25% "de acuerdo" en que toman medidas para resguardar su información, lo que refleja un compromiso notable con la privacidad y la seguridad.

Sin embargo, un 19% se muestra neutral y un 14% expresa desacuerdo. Esto sugiere que, aunque la mayoría está preocupada por la protección de sus datos, hay un pequeño grupo que podría no estar tomando las precauciones adecuadas.

El análisis estadístico revela un coeficiente de correlación de Spearman de 0.762, lo que indica una relación positiva significativa entre el nivel de conocimiento sobre protección de datos y las medidas que los usuarios adoptan para proteger su información personal.

La significancia bilateral de 0.000 respalda la relevancia estadística de esta correlación, lo que permite rechazar la hipótesis nula (Ho) y confirmar que efectivamente hay una relación positiva entre ambas variables en este contexto.

Estos resultados son coherentes con las conclusiones de Balarezo y Gálvez (2020), quienes destacan que existe una relación moderadamente positiva entre el uso de métodos de pago digitales y la satisfacción del cliente.

Al igual que en este estudio, enfatizan la importancia de evaluar la atención al usuario y de establecer una cultura de datos dentro de las organizaciones. Esto sugiere que la educación sobre protección de datos es fundamental no solo para empoderar a los usuarios, sino también para mejorar la satisfacción general en el uso de plataformas digitales.

Por lo tanto, es esencial implementar programas de educación y sensibilización sobre la protección de datos, con el objetivo de fortalecer el compromiso de todos los usuarios en la adopción de medidas de seguridad adecuadas.

Esto no solo beneficiará a los individuos al proteger su información personal, sino que también fomentará un entorno más seguro y confiable en el uso de plataformas de pago móvil. En resumen, al mejorar el conocimiento y la comprensión sobre la protección de datos, se puede aumentar la confianza en estas tecnologías y, por ende, mejorar la inclusión financiera y la satisfacción del usuario.

La cuarta discusión, señala que un 38% de los encuestados se declara "totalmente de acuerdo" y un 30% "de acuerdo" en que consideran importante la seguridad de sus dispositivos. Se aprecia que gran parte de los participantes valora la protección de su información personal. Sin embargo, un 23% mantiene una postura neutral y un 10% expresa desacuerdo, lo que sugiere que, aunque muchos reconocen la importancia de la seguridad, hay un grupo que podría no estar plenamente comprometido con este aspecto.

El análisis estadístico muestra un coeficiente de correlación de Spearman de 0.767. Estos hallazgos son consistentes con el trabajo de Rayo (2020), quien adaptó cuestionarios relacionados con el financiamiento de campañas, la confianza y la inclusión financiera para evaluar sus hipótesis.

Su análisis, realizado mediante regresión lineal, reveló un impacto significativo del financiamiento en la inclusión financiera. Esta información es valiosa para empresas e instituciones financieras, ya que sugiere que la educación y la sensibilización sobre la seguridad de los dispositivos podrían ser herramientas efectivas para fomentar la inclusión financiera en Lima Norte y en otras regiones del país.

Sobre la quinta discusión, un 40% se siente "totalmente de acuerdo" y un 13% "de acuerdo" en que la autenticación de dos factores proporciona una protección efectiva para sus cuentas en línea. Sin embargo, un 13% se muestra neutral y un 36% expresa algún nivel de desacuerdo.

Esto sugiere que, aunque una parte considerable de los encuestados valora esta medida de seguridad, hay un grupo significativo que no está convencido de su eficacia.

El análisis estadístico revela un coeficiente de correlación de Spearman de 0.758. Estos hallazgos son coherentes con el estudio de Arrunátegui (2020), quien menciona la escasez de investigaciones empíricas en el ámbito peruano sobre la inclusión financiera y la adopción de pagos móviles.

Mediante un análisis detallado de la literatura, se ha desarrollado un marco analítico que examina los factores que afectan la adopción de tecnologías de pago y su influencia en el crecimiento de negocios como las bodegas, así como en el desarrollo de sus propietarios.

Sobre la sexta discusión, un 37% de los encuestados se siente "totalmente de acuerdo" y un 34% "de acuerdo" en que tienen un conocimiento adecuado sobre el tema. Esto sugiere que una parte significativa de los participantes confía en su comprensión sobre la seguridad de los datos.

No obstante, un 16% se muestra neutral y un 13% expresa desacuerdo, lo que revela que existe un grupo notable que podría no estar completamente informado o seguro sobre sus conocimientos.

Los encuestados realizan evaluaciones de riesgo y confían en las medidas de seguridad que han implementado.

Sin embargo, también reconocen la necesidad de mantenerse al tanto de las amenazas y participar en programas de formación, lo que demuestra un compromiso personal con la protección de sus datos.

Este aspecto es esencial, ya que la educación continua es clave en un entorno digital que está en constante evolución.

El análisis estadístico presenta un coeficiente de correlación de Spearman de 0.680. Estos resultados son coherentes con lo señalado por Pacheco (2019), quien destaca que los

servicios financieros han experimentado una evolución notable en los últimos años gracias a los avances tecnológicos, con un enfoque particular en la banca móvil.

A nivel global, se han implementado con éxito modelos que han facilitado esta transformación. Aunque en Perú el número de bancos es limitado, se están explorando estrategias para aumentar la actividad bancaria, priorizando la banca móvil como una solución fundamental.

VI. CONCLUSIONES

6.1. Al obtener los resultados se pudo demostrar que “El nivel de seguridad de la transacción en las plataformas de pago móvil está positivamente relacionado con el nivel de conocimiento sobre la gestión de riesgos en seguridad de datos” la implementación de controles de seguridad complejos en las transacciones puede reducir la exposición a riesgos y vulnerabilidades, las organizaciones que priorizan la seguridad en sus transacciones, por lo tanto, están mejor preparadas para mitigar riesgos globales en la seguridad de datos.

6.2. Los hallazgos de la Protección de Datos Personales y Educación en Seguridad de la Información, permiten concluir que existe una relación positiva por lo que es de gran importancia la formación en la mejora de la protección de datos, la educación y la concienciación son cruciales para reducir los riesgos de violaciones de datos. Invertir en programas educativos permite que cada usuario pueda entender mejor las amenazas y aplicar prácticas seguras.

6.3. Respecto a la dimensión sobre Seguridad del Dispositivo y Cumplimiento de Normativas: La correlación que se encontró fue significativa entre ambas lo que subraya que los dispositivos con mayores estándares de seguridad están asociados con un mejor cumplimiento de las regulaciones de protección de datos. Este resultado está en consonancia con el principio de que la seguridad tecnológica es un pilar fundamental para cumplir con las normativas legales, la implementación de medidas de seguridad adecuadas en los dispositivos es esencial no solo para proteger la información, sino también para garantizar el cumplimiento normativo.

6.4.La relación entre la autenticación y el cumplimiento de normativas refuerza la idea de que sistemas de autenticación complejas son esenciales para asegurar el cumplimiento con las

regulaciones de protección de datos, una autenticación efectiva previene el acceso no autorizado y reduce el riesgo de fraudes. Esto es fundamental para cumplir con las exigencias normativas que buscan proteger la integridad y la confidencialidad de la información.

6.5. En la dimensión, Protección contra Fraudes y Tecnología en Seguridad de la Información, se encontró que si están correlacionadas por lo que la integración de tecnologías avanzadas demuestra que se puede mejorar significativamente la capacidad de protección contra fraudes.

6.5. Finalmente, respecto a la Plataforma de Pago Móvil y Nivel de Conocimiento sobre protección de datos financieros y personales, se encontró una fuerte correlación por lo que los estudiantes con mayor conocimiento sobre protección de datos utilizan las plataformas de pago móvil de manera más segura y efectiva, el conocimiento y la educación influyen significativamente en la adopción de prácticas seguras. La educación sobre protección de datos es, por lo tanto, un factor clave para fomentar el uso seguro de tecnologías financieras.

VII. RECOMENDACIONES

7.1. Fortalecer las Medidas de Seguridad en Transacciones: Las organizaciones deben seguir invirtiendo en la mejora de la seguridad de sus transacciones. Implementar tecnologías de encriptación, monitoreo en tiempo real y sistemas de autenticación multifactor puede ayudar a gestionar mejor los riesgos de seguridad de datos.

7.2. Desarrollar Programas de Capacitación en Seguridad de la Información: Es crucial implementar programas de educación y concienciación sobre la seguridad de la información dirigidos tanto a empleados como a usuarios. Estos programas deben incluir formación en buenas prácticas para la protección de datos personales, así como en el uso seguro de plataformas digitales.

7.3. Invertir en Seguridad Tecnológica de los Dispositivos: Las organizaciones deben asegurarse de que todos los dispositivos utilizados para acceder a datos sensibles cumplan con altos estándares de seguridad. Esto incluye el uso de software de protección actualizado, configuraciones de seguridad adecuadas y protocolos de autenticación sólidos.

7.4. Reforzar los Sistemas de Autenticación: La implementación de sistemas de autenticación multifactor y otras medidas avanzadas de verificación debe ser prioritaria para garantizar el cumplimiento normativo y proteger los datos sensibles de las organizaciones.

7.5. Adoptar Tecnologías Avanzadas para la Protección contra Fraudes: Es aconsejable que las organizaciones incorporen tecnologías como la inteligencia artificial en sus sistemas de seguridad para optimizar la detección y prevención de fraudes. Esta implementación no solo resguardará a los usuarios, sino que también reforzará la confianza en las plataformas digitales.

7.6. Promover la Educación en Protección de Datos entre los Usuarios de Plataformas de Pago Móvil: Las organizaciones deben desarrollar campañas educativas dirigidas a los usuarios de plataformas de pago móvil, enfocándose en la importancia de la protección de datos y el uso seguro de estas tecnologías. Esto puede incluir guías prácticas, seminarios en línea y soporte técnico accesible.

VIII. REFERENCIAS

Arrunategui, R. (2020). *Efectos de la adopción y uso de aplicaciones bancarias de pagos y transferencias en el crecimiento empresarial y la inclusión financiera de las bodegas de Lima Metropolitana*. [Tesis de grado, Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/19433/ARRUNATEGUI_RAVELLO_TOLENTINO_CHUJUTALLI.pdf?sequence=1&isAllowed=y

Balarezo, A., y Gálvez, A. (2020). *El uso medio de Pagos Digitales y la Satisfacción de los Clientes de Luz Del Sur SAA, 2020.* [Tesis de grado, Universidad San Ignacio de Loyola]. https://repositorio.usil.edu.pe/server/api/core/bitstreams/120d7082-992b-4fdf-9fb1-cc552af6624d/content

Buenapepa, R. (2023). *Estafas por Yape y Plin: Policía reporta más de 600 denuncias por transferencias falsas*. Buena Pepa. https://buenapepa.pe/aumentan-estafas-por-transferencias-de-yape-y-plin/

Cárdenas, L. (2022). *Efecto de las fusiones de Plataformas (Two-Sided Markets) En Bienestar*. [Tesis de grado, Universidad del Pacífico]. https://repositorio.up.edu.pe/bitstream/handle/11354/3481/Cardenas%2C%20Pedro_Trabajo%20de%20suficiencia%20profesional_Economia_2022.pdf?sequence=1&isAllowed=y

Castro, I. (2019). *Protección de datos personales a través de herramientas de procesamiento automatizado de datos: desafíos y recomendaciones*. Infotec Centro de Investigación e Innovación En Tecnologías de la Información y Comunicación. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/462/1/INFOTEC_MDTIC_MICR_07122020.pdf

Ciberseguridad. (2024). Infosecuritymexico.com. https://www.infosecuritymexico.com/es/ciberseguridad.html

Espinoza, A. (2023). *Aumentan estafas con Yape y Plin: 609 denuncias por falsas transferencias de dinero*. infobae. https://www.infobae.com/peru/2023/11/10/aumentan-estafas-con-yape-y-plin-609-denuncias-por-falsas-transferencias-de-dinero/#:~:text=En%20lo%20que%20va%20del,suplantan%20a%20ambas%20billeteras%20digitales.

Garcia, J., y Soto, M. (2022). Dinero móvil y su impacto en la inclusión financiera en los residentes de los distritos de Lima Norte en el 2021. [Tesis de grado, Universidad Peruana de Ciencias Aplicadas].. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/667550/García_BE.pdf?sequence=13&isAllowed=y

García, M. (2021). Seguridad en plataformas de pago móvil: Educación y conciencia como medidas preventivas. Revista de Tecnología Financiera., 7(2), 45-60.

Gamarra, G., Wong , F., Rivera , T., y Pujay , O. (2015). *Estadistica e investigacion con aplicacion de SPSS.* San Marcos.

Hernández, O. (2021). *Aproximación a los distintos tipos de muestreo no probabilístico que existen*. Rev Cubana Med Gen Integr, 37(3). 1-3. http://scielo.sld.cu/pdf/mgi/v37n3/1561-3038-mgi-37-03-e1442.pdf.

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* Mc Graw Hill Interamericana Editores, S.A. de C.V.

Hernández Botero, J., y Londoño Sepúlveda, N. R. (2020). La Responsabilidad de las Entidades Financieras por Fraudes Electrónicos. (Tesis de maestría, Universidad Pontificia Bolivariana). https://repository.upb.edu.co/bitstream/handle/20.500.11912/6161/La%20responsabili

dad%20de%20las%20entidades%20financieras%20por%20fraudes%20electrónicos.pdf?sequence=1

International Business Machines Corporation. (2024). Entrenamiento de usuarios y mejores prácticas. IBM. https://www.ibm.com/es-es/topics/phishing

International Business Machines Corporation. (2024). IBM. https://www.ibm.com/es-es/topics/phishing.

Juli Quispe, E. N. (2024). *La Banca Móvil y su Relación con la Inclusión Financiera de los Estudiantes De la Universidad Nacional del Altiplano Puno, Periodo 2022*. [Tesis de grado, Universidad Nacional del Altiplano]. http://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/21415/Juli_Quispe_Eymi_Naomy.pdf?sequence=1&isAllowed=y

Kobra. (2024). Cumplimiento Normativo en Perú: Seguridad Financiera. https://kobra.red/blog/cumplimiento-normativo-en-peru-seguridad-financiera.

Leguizamón, M. S. (2019). *El Phishing*. [Tesis de Grado, Universidad Jaume-I]. https://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizamón_Mayra.pdf?sequence=1

López, L y López, J. (2011). Modelos de adopción de tecnologías de la información desde el paradigma actitudinal. *Cad. 9 (1),* 176-196. https://doi.org/10.1590/S1679-39512011000100011

Malwarebytes. (2024). ¿Cómo protegerse del phishing? https://es.malwarebytes.com/phishing/

Mercantil, D. (2024). *Apertura en las transferencias digitales entre Yape y Plin: Los nuevos retos de la interoperabilidad financiera en torno al desarrollo del derecho a la libre competencia y derechos conexos*. Dimensión mercantil.

https://dimensionmercantil.pe/apertura-en-las-transferencias-digitales-entre-yape-y-plin

Otzen, T., y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Int. J. Morphol., 35(81)*, 227-232. https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf.

Pacheco, M. (2019). *Impacto de la Banca Móvil en el Proceso de Bancarización para Una Entidad Financiera Estatal en Lima Norte en El 2017*. [Tesis de grado, Universidad Privada del Norte]. https://repositorio.upn.edu.pe/bitstream/handle/11537/24716/Pacheco%20Alarcón%2C%20Flor%20de%20María.pdf?sequence=2&isAllowed=n

Parada, A. y Gómez, U. (2018). Analysis of the Components of Security from a Systemic System Dynamics Perspective. *Inf. tecnol., 29(1),* 27-38. http://dx.doi.org/10.4067/S0718-07642018000100027

Ramírez, S. (2023). *Estafas a usuarios de Plin y Yape: la nueva modalidad que afecta a comerciantes y cómo protegerse*. El Comercio Perú. https://elcomercio.pe/pasa-en-la-calle/estafas-a-usuarios-de-plin-y-yape-la-nueva-modalidad-con-capturas-de-pantallas-falsas-y-como-protegerse-inseguridad-ciudadana-ciberdelincuencia-noticia/?ref=ecr#google_vignette

Rapimán, M. y Chibey, T. (2022). Privacy of information in qualitative social research: the transition to the digital world. *Acta bioeth. 28(2),* 197-203. http://dx.doi.org/10.4067/S1726-569X2022000200197

Rayo, A. (2020). *Prototipo de Detección de Fraudes Con Tarjetas de Crédito Basado en Inteligencia Artificial Aplicado a un Banco Peruano*. [Tesis de grado, Universidad de Lima]. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/15294/Trabajo.pdf?sequence=1&isAllowed=y

Sánchez, A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Rev. Digit. Invest. Docencia Univ., 13(1)*, 1-21. http://dx.doi.org/10.19083/ridu.2019.644.

Sànchez, M., Velasco, M., Espinoza, R., Gonzales, A., Romero, R., & Mory, W. (2023). *Metodología y estadística en la investigación científica.* Puerto Madero Editorial Académica. https://doi.org/10.55204/PMEA.17

Sánchez, M. (2024). Participación ciudadana en la gestión de la política pública contra la violencia familiar. Lima Metropolitana. *Revista de Climatología, 24*, 1441-1454. https://rclimatol.eu/wp-content/uploads/2024/03/Articulo-RCLIMCS24_0156-Mario-Sanchez.pdf.

Sganderla, J., Aguiar, C. y Fagundes, M. (2014). Aproximación de las teorías del riesgo en un estudio de caso en el sur de Brasil. *Ambient. soc., 17 (1),* 133-150. https://www.scielo.br/j/asoc/a/Vs8F5m4FcrRLFJRGrwsBmcf/?lang=es

SYDLE. (2023). Protección de datos personales en el sector financiero. https://www.sydle.com/es/blog/proteccion-de-datos-personales-en-el-sector-financiero-64b574331b980e466f1eb4df

Valderrama, S. (2019). *Pasos para elaborar proyectos de investigacion cientifica* (10 ed.). Editorial San Marcos.

Valderrama, S., y Jaimes, C. (2019). *El desarrollo de la tesis. Descriptiva - comparativa, correlacional y cuasiexperimental.* Editorial San Marcos.

Vallejos, M. (2023). *Yape y Plin: ¿Qué tan seguras son estas aplicaciones de interoperabilidad?* UPC. https://puntoseguido.upc.edu.pe/yape-y-plin-que-tan-seguras-son-estas-aplicaciones-de-interoperabilidad/

Vergara, M. (2023). *Pagos digitales: Una tendencia que avanza a buen ritmo en el Perú*. ESAN. https://www.esan.edu.pe/conexion-esan/pagos-digitales-una-tendencia-que-avanza-a-buen-ritmo-en-el-peru

Yape, B. (2024). *Política de privacidad y datos personales*. YAPE. https://www.yape.com.pe/politica-privacidad-datos/yape

Zhang, J. (2020). *Métodos de pago móvil: desarrollo y estudio comparativo*. [Tesis de grado, Universidad Politécnica de Cartagena]. https://repositorio.upct.es/bitstream/handle/10317/8787/tfg-zha-met.pdf?sequence=1&isAllowed=y

IX ANEXOS

Anexo A. Matriz de consistencia

<table>
<tr><th colspan="4">PLATAFORMA DE PAGO MÓVIL Y NIVEL DE CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES EN UNA UNIVERSIDAD DE LIMA, 2024</th></tr>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th></tr>
<tr>
<td>Problema General
¿Cuál es la relación entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?
Problemas específicos
¿Cuál es la relación entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?
¿Qué relación existe entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales en una</td>
<td>Objetivo General
Determinar la relación entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
Objetivos específicos
Determinar la relación entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
Establecer la relación entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales</td>
<td>Hipótesis General
Existe relación positiva entre la plataforma de pago móvil y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
Hipótesis específicas
Existe relación positiva entre la seguridad de la transacción y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.
Existe relación positiva entre la protección de datos personales y el nivel de conocimiento sobre protección de datos financieros y personales</td>
<td>Variable independiente.
<table>
<tr><th>Dimensiones</th><th>Indicadores</th><th>Escala</th></tr>
<tr><td rowspan="3">Seguridad de la transacción</td><td>Autenticación multifactor</td><td rowspan="10">Ordinal:
(1) Totalmente en desacuerdo.
(2) En desacuerdo.
(3)Neutral.
(4)De acuerdo.
(5)Totalmente de acuerdo.</td></tr>
<tr><td>Tokenización de datos</td></tr>
<tr><td>Detección de fraudes en tiempo real.</td></tr>
<tr><td rowspan="2">Protección de datos personales</td><td></td></tr>
<tr><td></td></tr>
<tr><td rowspan="2">Seguridad del dispositivo</td><td>Bloqueo de pantalla</td></tr>
<tr><td>Protección contra el rooteo o jailbreaking</td></tr>
<tr><td rowspan="2">Autenticación segura</td><td>Autenticación biométrica</td></tr>
<tr><td>Códigos de verificación únicos</td></tr>
<tr><td rowspan="2">Protección contra fraudes</td><td>Monitoreo de patrones de comportamiento sospechoso</td></tr>
<tr><td>Análisis de datos en tiempo real y Colaboración con redes de tarjetas.</td></tr>
</table>
Variable dependiente.</td>
</tr>
</table>

Universidad de Lima, 2024? ¿Qué relación existe entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024? ¿Cuál es la relación entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024? ¿Cuál es la relación entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024?	en una Universidad de Lima, 2024. Establecer la relación entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024. Determinar la relación entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024. Establecer la relación entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.	en una Universidad de Lima, 2024. Existe relación positiva entre la seguridad del dispositivo y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024. Existe relación positiva entre la autenticación segura y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024. Existe relación positiva entre la protección contra fraudes y el nivel de conocimiento sobre protección de datos financieros y personales en una Universidad de Lima, 2024.	**Dimensiones**	**Indicadores**	**Escala**
			Gestión de Riesgos	Frecuencia y gravedad de incidentes de seguridad de datos	Ordinal: (1)Totalmente en desacuerdo. (2) En desacuerdo. (3)Neutral. (4)De acuerdo. (5)Totalmente de acuerdo.
				Eficacia de los controles de seguridad implementados	
				Tiempo medio para detectar y responder a incidentes de seguridad.	
				Evaluaciones periódicas de riesgos y vulnerabilidades	
			Tecnología y seguridad de la información	Nivel de cumplimiento con los estándares de seguridad de la información	
				Eficiencia de los sistemas de detección y prevención de intrusiones	
				Tasa de actualización y parcheo de sistemas y software	
				Evaluación de la efectividad de la encriptación de datos	
				Nivel de cumplimiento con las mejores prácticas de seguridad de la información	
			Legislación y regulación	Nivel de cumplimiento con las normativas de protección de datos aplicables	
				Frecuencia y gravedad de las infracciones de datos y sanciones asociadas	

			Educación y concienciación	Participación en programas de formación sobre seguridad de la información	
				Concienciación sobre seguridad de datos	
				Nivel de comprensión de los usuarios sobre políticas y procedimientos de seguridad de datos	
				Conocimiento sobre incidentes de seguridad y mejores prácticas	
				Nivel de implicación y responsabilidad de los usuarios en la protección de datos	
METODOLOGÍA Enfoque. Cuantitativo Tipo de investigación. Aplicada Nivel de investigación. Correlacional Diseño: No experimental – transversal Población: 200 Muestra: 200 Muestreo: Censal					

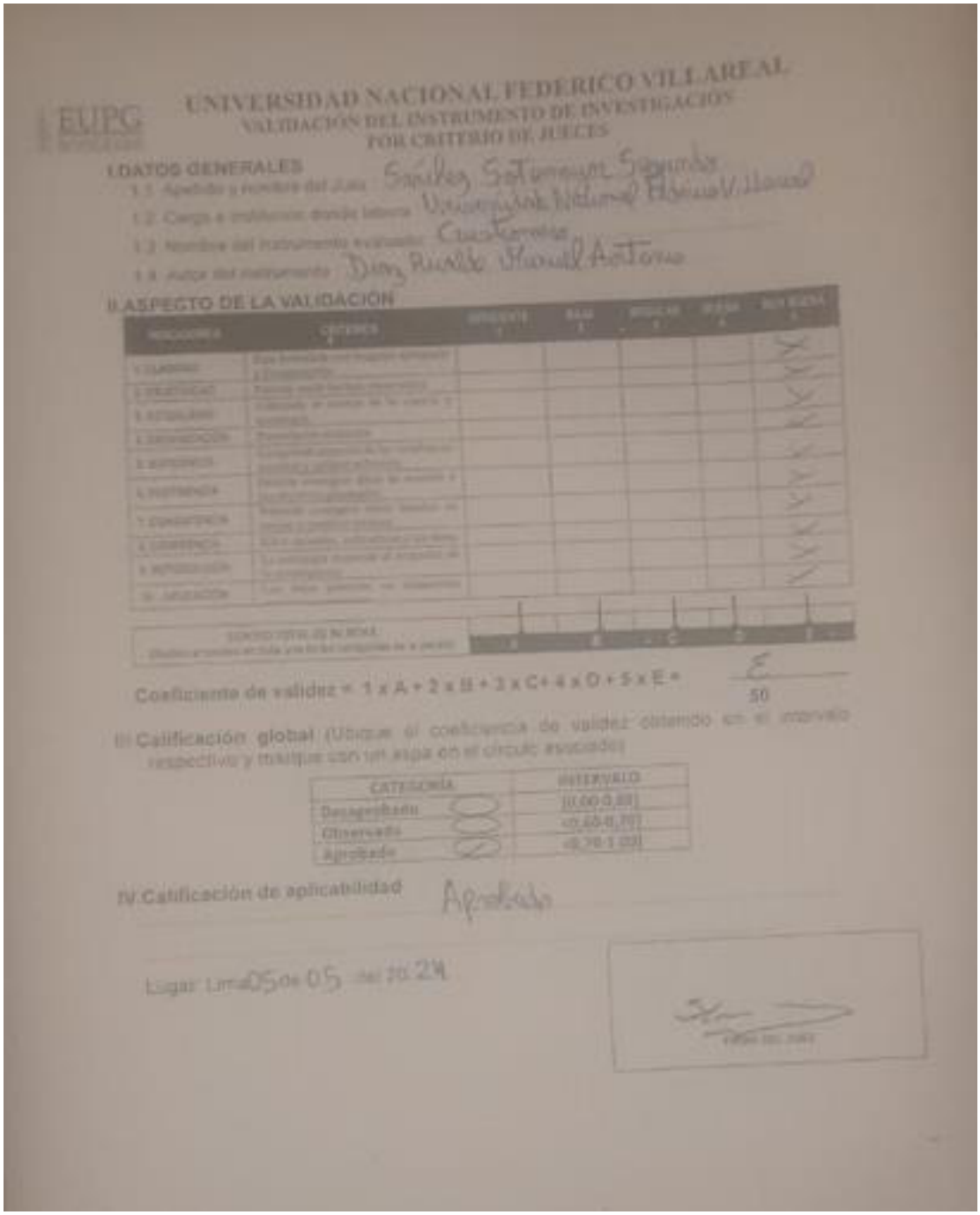
Anexo B. Validación de instrumentos

Tabla 14

Expertos durante la evaluación de los instrumentos

Experto	Decisión
Sánchez Sotomayor, Segundo	Si existe suficiencia
Bazán Briceño José Luis	Si existe suficiencia
Sánchez Camargo Mario	Si existe suficiencia

Certificado de validación de instrumentos



UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
POR CRITERIO DE JUECES

I.DATOS GENERALES

I.1. Apellido y nombre del Juez: Sánchez Salamanca Segundo

I.2. Cargo e institución donde labora: Universidad Nacional Federico Villarreal

I.3. Nombre del instrumento evaluado: Cuestionario

I.4. Autor del instrumento: Díaz Ruelas Manuel Antonio

II.ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Está formulado con lenguaje apropiado y comprensible.					X
2. OBJETIVIDAD	Permite medir hechos observables.					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					X
4. ORGANIZACIÓN	Presentación adecuada.					X
5. SUFICIENCIA	Comprende aspectos de cantidad y calidad suficientes para medir la variable.					X
6. INTENCIONALIDAD	Permite analizar datos de acuerdo a los objetivos propuestos.					X
7. CONSISTENCIA	Responde a fundamentos técnicos y científicos propios.					X
8. COHERENCIA	Existe relación entre variables e indicadores.					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación.					X
10. OPORTUNIDAD	Los datos permiten un tratamiento estadístico.					X
SUMATORIA TOTAL DE LA HOJA (Sumar el puntaje de cada ítem calificado en la escala)						

Coeficiente de validez = 1 x A + 2 x B + 3 x C + 4 x D + 5 x E = $\frac{E}{50}$

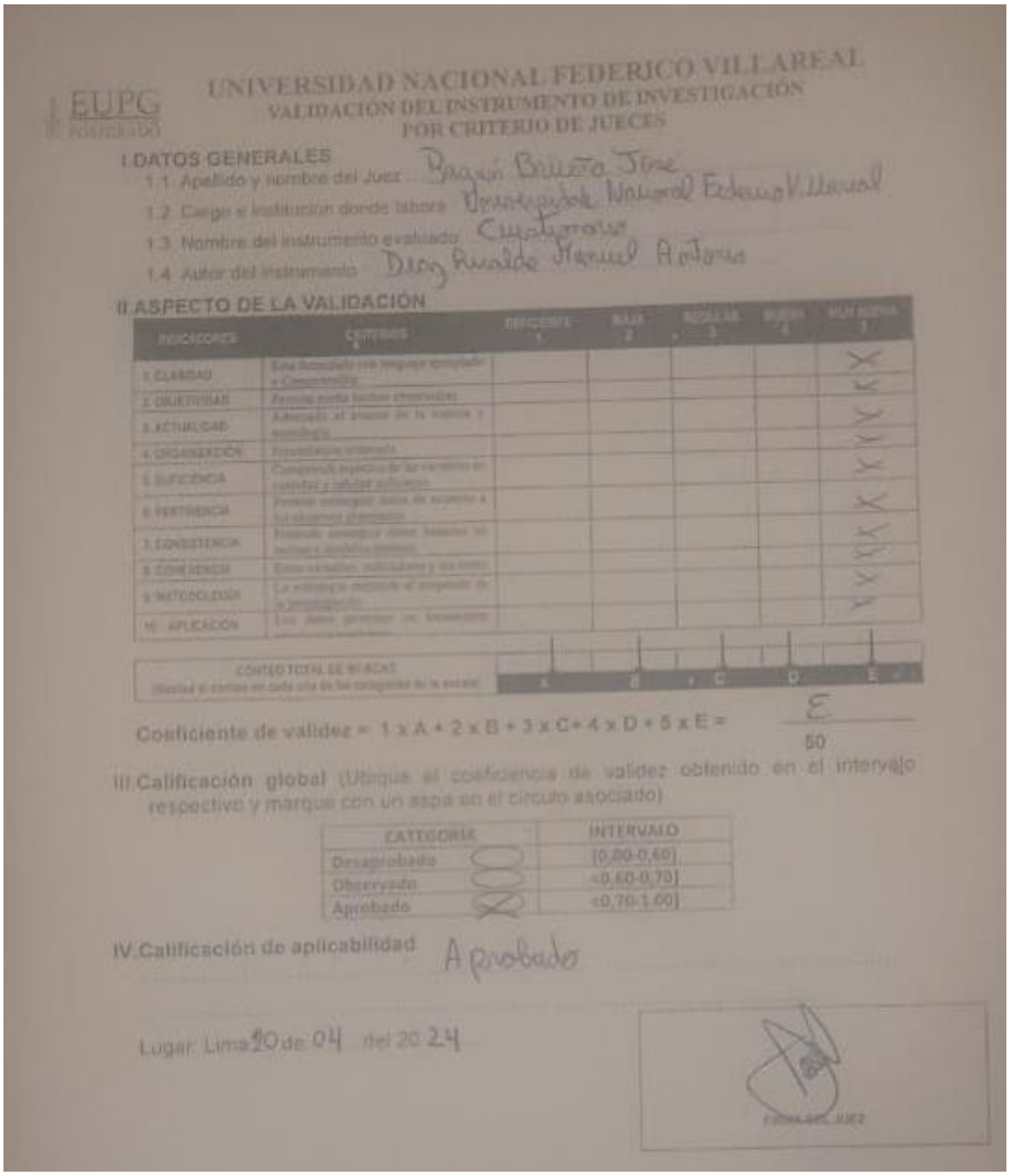
III. Calificación global (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo evaluado)

CATEGORÍA	INTERVALO
Desaprobado	[0.00-0.59]
Observado	<0.60-0.79]
Aprobado	<0.79-1.00]

IV.Calificación de aplicabilidad: Aprobado

Lugar: Lima 05 de 05 del 20 24

Firma del Juez



EUPG
POSTGRADO

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellido y nombre del Juez: Bazán Bullón José
1.2. Cargo e institución donde labora: Docente/Jefe Maestría Federico V. Manuel
1.3. Nombre del instrumento evaluado: Cuestionario
1.4. Autor del instrumento: Diaz Rivalde Manuel Antonio

II. ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Está formulado con lenguaje apropiado y Comprensible					X
2. OBJETIVIDAD	Permite darle buena interpretación					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Presentación ordenada					X
5. SUFICIENCIA	Comprende aspectos de la variable en cantidad y calidad suficiente					X
6. PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados					X
7. CONSISTENCIA	Presenta consigna clara basada en teorías y modelos teóricos					X
8. COHERENCIA	Entre variables, indicadores y los ítems					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					X
10. APLICACIÓN	Los datos permiten un tratamiento estadístico pertinente					X

CUADRO TOTAL DE RESPUESTAS (Escribir el número en cada una de las categorías de la escala)	A	B	C	D	E

Coeficiente de validez = 1 x A + 2 x B + 3 x C + 4 x D + 5 x E = $\frac{E}{50}$

III. Calificación global (Ubique el coeficiencia de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA	INTERVALO
Desaprobado ( )	[0,00-0,69]
Observado ( )	<0,60-0,70]
Aprobado (X)	<0,70-1,00]

IV. Calificación de aplicabilidad: Aprobado

Lugar: Lima 20 de 04 del 20 24

FIRMA DEL JUEZ

EUPG
POSTGRADO

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
POR CRITERIO DE JUECES

I.DATOS GENERALES

1.1. Apellido y nombre del Juez: Sánchez Camargo Hugo

1.2. Cargo e institución donde labora: Universidad Nacional Federico Villarreal

1.3. Nombre del instrumento evaluado: Cuestionario

1.4. Autor del instrumento: Díaz Rivalla Manuel Antonio

II.ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Está redactado con lenguaje apropiado y comprensible					X
2. OBJETIVIDAD	Permite medir hechos observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Presentación ordenada					X
5. SUFICIENCIA	Comprende aspectos de los factores en cantidad y calidad suficiente					X
6. PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados					X
7. CONSISTENCIA	Permite conseguir datos basados en teorías o modelos teóricos					X
8. COHERENCIA	Entre variables, indicadores y las dimensiones					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					X
10. APLICACIÓN	Los datos permiten un tratamiento estadístico pertinente					X

CONTEO TOTAL DE MARCAS (Escriba el conteo en cada una de las categorías de la escala)	A	B	C	D	E

Coeficiente de validez = 1 x A + 2 x B + 3 x C + 4 x D + 5 x E = $\frac{\Sigma}{50}$

III Calificación global (Ubique el coeficiencia de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA		INTERVALO
Desaprobado	( )	[0,00-0,60]
Observado	( )	<0,60-0,70]
Aprobado	(X)	<0,70-1,00]

IV.Calificación de aplicabilidad Aprobado

Lugar: Lima 06 de 06 del 2024

FIRMA DEL JUEZ

Anexo C. Confiabilidad de Instrumentos

En la confiabilidad del instrumento por ser variables de escala ordinal se utilizo el Alfa de Cronbach.

La confiabilidad es la precisión del instrumento para medir la variable de interés. A mayor fiabilidad sera menor la cantidad de errores aleatorios e impredecibles que apareceran al utilizarlo.

Tabla 15

Resumen de procesamientos de casos

		N	%
Casos	Válido	200	100,0
	Excluido[a]	0	,0
	Total	200	100,0

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

Nota. Según la tabla 15, los resultados de las 200 encuestas que fueron procesadas mediante el SPSS, no presenta casos de exclusion, el 100% fueron aceptados.

Tabla 16

Confiabilidad del instrumento de la variable 1

Alfa de Cronbach	N de elementos
,938	20

Nota. Mediante el SPSS se obtuvo un coeficiente de fiabilidad de 0.938, se interpreta como una alta fiabilidad.

Tabla 17

Confiabilidad del instrumento de la variable 2

Alfa de Cronbach	N de elementos
,895	20

Nota. Mediante el SPSS se obtuvo un coeficiente de fiabilidad de 0.895, se interpreta como una alta fiabilidad.

Anexo D. Instrumento de medición

TÍTULO: PLATAFORMA DE PAGO MÓVIL Y NIVEL DE CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES EN UNA UNIVERSIDAD DE LIMA, 2024.

I. DATOS GENERALES

Sexo: Femenino ( ) Masculino ( )
Edad: …….
Nivel de Estudios: ……

INSTRUCCIONES (CONSENTIMIENTO INFORMADO):
El presente cuestionario es de naturaleza anónima y tiene por objetivo medir la vulnerabilidad en plataformas de pago móvil y el nivel de conocimiento por parte de los estudiantes.
Lea cuidadosamente cada pregunta y marque con un aspa (X) sólo una alternativa, la que mejor refleje su punto de vista. Conteste todas las proposiciones y le solicitamos responda con sinceridad las alternativas, la información será utilizada con fines únicamente académicos.

Dimensión: Seguridad de la Transacción

1. Cree que el uso de plataformas de pago móvil está siendo vulnerables en hacer transacciones financieras.

   1: Totalmente en desacuerdo (1)
   2: En desacuerdo (2)
   3: Neutral (3)
   4: De acuerdo (4)
   5: Totalmente de acuerdo (5)

2. Estoy preocupado por la seguridad de mis transacciones cuando utilizo plataformas de pago móvil.

   1: Totalmente en desacuerdo (1)
   2: En desacuerdo (2)
   3: Neutral (3)
   4: De acuerdo (4)
   5: Totalmente de acuerdo (5)

3. Las siguientes medidas de seguridad son importantes para proteger mis transacciones en plataformas de pago móvil:

   (Califica cada medida en la escala de 1 a 5)

   Autenticación de dos factores
   Totalmente en desacuerdo (1)
   En desacuerdo (2)
   Neutral (3)
   De acuerdo (4)
   Totalmente de acuerdo (5)

Encriptación de datos
Totalmente en desacuerdo (1)
En desacuerdo (2)
Neutral (3)
De acuerdo (4)
Totalmente de acuerdo (5)

Verificación biométrica (por ejemplo, huella dactilar o reconocimiento facial)
Totalmente en desacuerdo (1)
En desacuerdo (2)
Neutral (3)
De acuerdo (4)
Totalmente de acuerdo (5)
Monitoreo de actividad sospechosa

Totalmente en desacuerdo (1)
En desacuerdo (2)
Neutral (3)
De acuerdo (4)
Totalmente de acuerdo (5)
Educación sobre prácticas seguras de uso de la plataforma

Totalmente en desacuerdo (1)
En desacuerdo (2)
Neutral (3)
De acuerdo (4)
Totalmente de acuerdo (5)

4. He experimentado intentos de fraude o actividad sospechosa al realizar transacciones en plataformas de pago móvil.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

Dimensión: Protección de Datos Personales

5. Estoy preocupado por la seguridad de mis datos personales en línea.
1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

6. Reviso y actualizo regularmente la configuración de privacidad en mis cuentas en línea (redes sociales, correo electrónico, etc.).

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

7. He experimentado una violación de datos personales (por ejemplo, robo de identidad, acceso no autorizado a cuentas en línea, etc.).

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

8. Tomo medidas para proteger mis datos personales en línea, como usar contraseñas seguras y activar la autenticación de dos factores.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

Dimensión: Seguridad del Dispositivo

9. Estoy preocupado por la seguridad de mis dispositivos electrónicos (por ejemplo, computadora, teléfono inteligente, tablet, etc.).

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

10. He implementado medidas de seguridad en mis dispositivos para protegerlos contra amenazas cibernéticas, como el uso de contraseñas fuertes y la instalación de software antivirus.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

11. He experimentado una violación de seguridad en mis dispositivos (por ejemplo, virus informáticos, malware, piratería, etc.).

    1: Totalmente en desacuerdo (1)

2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

12. Realizo copias de seguridad de mis datos importantes en mis dispositivos regularmente.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

Dimensión: Autenticación

13. Considero que la autenticación en línea es importante para proteger mis cuentas y datos personales.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

14. Prefiero utilizar métodos de autenticación como contraseñas, autenticación de dos factores o reconocimiento biométrico para acceder a mis cuentas en línea.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

15. He experimentado intentos de acceso no autorizado a alguna de mis cuentas en línea.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

16. Creo que la autenticación de dos factores proporciona una capa adicional de seguridad efectiva para proteger mis cuentas en línea.

1: Totalmente en desacuerdo (1)
2: En desacuerdo (2)
3: Neutral (3)
4: De acuerdo (4)
5: Totalmente de acuerdo (5)

Dimensión: Protección contra Fraudes

17. Estoy familiarizado con las medidas de seguridad proporcionadas por las plataformas de pago móvil Yape y Plin para proteger contra la suplantación de identidad.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

18. He recibido información sobre cómo reconocer y evitar intentos de suplantación de identidad al utilizar Yape y Plin.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

19. Creo que Yape y Plin podrían mejorar la protección contra la suplantación de identidad mediante más educación y concientización para los usuarios, mejoras en la tecnología de seguridad de la plataforma, y colaboración con autoridades y entidades de seguridad cibernética.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

20. Me siento seguro utilizando Yape y Plin en términos de protección contra la suplantación de identidad.

    1: Totalmente en desacuerdo (1)
    2: En desacuerdo (2)
    3: Neutral (3)
    4: De acuerdo (4)
    5: Totalmente de acuerdo (5)

CUESTIONARIO

NIVEL CONOCIMIENTO SOBRE PROTECCIÓN DE DATOS FINANCIEROS Y PERSONALES

Dimensión: Gestión de Riesgos en Seguridad de Datos

1. Realiza evaluaciones periódicas de riesgos en su dispositivos y cuentas personales para identificar vulnerabilidades de seguridad.

   - Totalmente en desacuerdo (1)
   - En desacuerdo (2)
   - Ni de acuerdo ni en desacuerdo (3)
   - De acuerdo (4)
   - Totalmente de acuerdo (5)

2. Toma medidas inmediatas para mitigar los riesgos una vez que identifico una amenaza a la seguridad de sus datos.

   - Totalmente en desacuerdo (1)
   - En desacuerdo (2)
   - Ni de acuerdo ni en desacuerdo (3)
   - De acuerdo (4)
   - Totalmente de acuerdo (5)

3. Confía en que los controles de seguridad que tiene implementado son suficientes para proteger sus datos personales.

   - Totalmente en desacuerdo (1)
   - En desacuerdo (2)
   - Ni de acuerdo ni en desacuerdo (3)
   - De acuerdo (4)
   - Totalmente de acuerdo (5)

4. Se asegura de mantenerme informado sobre las últimas amenazas y vulnerabilidades en seguridad de datos.

   - Totalmente en desacuerdo (1)
   - En desacuerdo (2)
   - Ni de acuerdo ni en desacuerdo (3)
   - De acuerdo (4)
   - Totalmente de acuerdo (5)

Dimensión: Tecnología y Seguridad de la Información

5. Tiene un conocimiento adecuado sobre los estándares de seguridad de la información, como ISO 27001.

   - Totalmente en desacuerdo (1)
   - En desacuerdo (2)
   - Ni de acuerdo ni en desacuerdo (3)
   - De acuerdo (4)

- Totalmente de acuerdo (5)

6. Entiende cómo funcionan los sistemas de detección y prevención de intrusiones para proteger sus dispositivos y redes contra amenazas cibernéticas.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

7. Actualiza regularmente sus sistemas y software para protegerlos contra vulnerabilidades conocidas.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

8. Comprende la importancia de la encriptación de datos para proteger la privacidad y seguridad de la información.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

9. Sigue las mejores prácticas de seguridad de la información, como el uso de contraseñas seguras y la autenticación de dos factores.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

Dimensión: Cumplimiento y Sanciones en Protección de Datos

10. Está bien informado sobre las normativas de protección de datos aplicables al uso de plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

11. Cree que las plataformas de pago móvil cumplen adecuadamente con las normativas de protección de datos.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

12. ¿Has sido afectado directa o indirectamente por una infracción de datos relacionada con una plataforma de pago móvil que haya resultado en sanciones para la empresa?

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

13. Las sanciones por incumplimiento de normativas de protección de datos en plataformas de pago móvil son lo suficientemente severas para disuadir futuras infracciones.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

14. Considera que necesita una mayor vigilancia y aplicación por parte de las autoridades para garantizar el cumplimiento de las normativas de protección de datos en plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

Dimensión: Educación y Concienciación en Seguridad de la Información

15. Participa regularmente en programas de formación sobre seguridad de la información.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

16. Se siento bien informado sobre la seguridad de datos y los riesgos asociados al uso de plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (4)

17. Entiende claramente las políticas y procedimientos de seguridad de datos establecidos por las plataformas de pago móvil que utilizo.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

18. Está al tanto de los incidentes de seguridad de datos ocurridos en plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

19. Se considera responsable de proteger sus propios datos personales al utilizar plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)

20. Cree que la educación y concienciación sobre seguridad de la información deben ser una prioridad para los usuarios de plataformas de pago móvil.

- Totalmente en desacuerdo (1)
- En desacuerdo (2)
- Ni de acuerdo ni en desacuerdo (3)
- De acuerdo (4)
- Totalmente de acuerdo (5)