



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**  
**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**Aplicación de la Norma internacional ISO 27032 para la  
Seguridad de la información en los Marketplace de Facebook,  
Cusco 2023**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

**Ingeniero de Sistemas**

**AUTOR:**

Rojas Moreano, Jhonatan Jordy ([orcid.org/0000-0002-5117-1999](https://orcid.org/0000-0002-5117-1999))

**ASESOR:**

Dr. Agreda Gamboa, Everson David ([orcid.org/0000-0003-1252-9692](https://orcid.org/0000-0003-1252-9692))

**LÍNEA DE INVESTIGACIÓN:**

Auditoría de Sistemas y Seguridad de la Información

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo Económico, Empleo y Emprendimiento

TRUJILLO - PERÚ

2023

## **Dedicatoria**

*A Dios, por ser mi guía y mi fortaleza en todo momento.*

*A mis padres, quienes con su amor y sacrificio me brindaron la oportunidad de crecer y educarme, les agradezco por su constante apoyo y confianza en mí.*

*A mi familia, por ser mi inspiración y mi motivación, les agradezco por su amor y comprensión en cada etapa de mi vida. Esta tesis es un reflejo de su amor y dedicación hacia mí, y espero que les haga sentir orgullosos y felices.*

Jhonatan Jordy

## Agradecimiento

*A la Universidad César Vallejo por brindarme la oportunidad de formarme y por ofrecerme los recursos y herramientas necesarias para alcanzar mis metas académicas.*

*A mis padres, que sin su este logro no hubiera sido posible, me dieron la fuerza para continuar en los momentos difíciles.*

*A mi asesor, por su dedicación, orientación y paciencia durante todo el proceso de investigación y redacción de esta tesis. Sus consejos y conocimientos fueron fundamentales para alcanzar mis objetivos y por eso, le estaré eternamente agradecido.*

El Autor

## Índice de contenidos

	Pág.
Caratula .....	i
Dedicatoria .....	ii
Agradecimiento .....	iii
Índice de contenidos .....	iv
Índice de tablas .....	v
Índice de figuras .....	vi
Resumen .....	vix
Abstract .....	ix
I. INTRODUCCIÓN .....	1
II. MARCO TEÓRICO .....	5
III. METODOLOGÍA .....	10
III.1 Tipo y diseño de investigación .....	10
III.2 Variables y operacionalización .....	10
III.3 Población, muestra y muestreo .....	11
III.4 Técnicas e instrumentos de recolección de datos .....	12
III.5 Procedimientos .....	13
III.6 Método de análisis de datos .....	15
III.7 Aspectos éticos .....	15
IV. RESULTADOS .....	17
V. DISCUSIÓN .....	34
VI. CONCLUSIONES .....	35
VII. RECOMENDACIONES .....	37
REFERENCIAS .....	39
ANEXOS .....	40

## Índice de tablas

	Pág.
Tabla 1. Prueba de Kolmogorov-Smirnov .....	32
Tabla 2. Prueba de normalidad de Wilcoxon.....	33

## Índice de figuras

	Pág.
Figura 1. Representación gráfica del grado de conocimiento de los usuarios .....	17
Figura 2. Familiarización de los usuarios con las políticas de seguridad de Facebook con respecto a los Marketplace.....	18
Figura 3. Cumplimiento de las políticas de seguridad por parte de los usuarios de la plataforma.....	19
Figura 4. Incidentes experimentados por los usuarios de la plataforma.....	20
Figura 5. Percepción de los usuarios respecto a las herramientas de seguridad por parte de Facebook Marketplace.....	20
Figura 6. Opinión de los usuarios respecto a la capacitación sobre seguridad de la información al utilizar los Marketplace de Facebook.....	21
Figura 7. Cumplimiento de las políticas de seguridad.....	22
Figura 8. Identificación de la información importante por parte de Facebook Marketplace.....	23
Figura 9. Cumplimiento de las medidas de seguridad establecidas para la protección de la información importante.....	24
Figura 10. Procedimientos establecidos en respuestas a incidentes de seguridad de la información.....	24
Figura 11. Implementación de controles de acceso físico y lógico para garantizar seguridad de información, .....	25
Figura 12. Implementación de medidas de seguridad específicas para proteger los datos personales.....	26
Figura 13. Problemas de seguridad experimentados por los usuarios de la plataforma.....	27
Figura 14. Medidas para proteger información personal tomadas por los usuarios de la plataforma.....	28

Figura 15. Iniciativa de capacitación sobre prácticas de seguridad por los usuarios de la plataforma.....	28
Figura 16. Percepción de los usuarios sobre la información sobre seguridad que Facebook proporciona.....	29
Figura 17. Tipo de incidentes de seguridad de la información que han experimentado los usuarios de la plataforma. ....	30

## Resumen

El presente trabajo de investigación tiene como objetivo mejorar la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco en el año 2023, mediante la aplicación de la norma ISO 27032. El tipo de investigación fue Aplicada y con diseño Preexperimental. La muestra poblacional fue de 100 personas y se usó la encuesta como herramienta de recolección de datos. Se evaluaron tres (3) objetivos específicos: grado de capacitación de los usuarios, grado de cumplimiento de la norma ISO 27032 y análisis de los riesgos de seguridad de la información. Se obtuvieron resultados significativos en cuanto a la percepción de los usuarios sobre los riesgos de seguridad, la necesidad de capacitación y el grado de cumplimiento de la norma ISO 27032. La hipótesis general planteada fue confirmada, evidenciando la importancia de la aplicación de la norma ISO 27032 para mejorar la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco en el año 2023.

*Palabras clave: Seguridad de la información, Marketplace de Facebook, norma ISO 27032.*

## **Abstract**

The present research work aims to improve information security in the Facebook Marketplace in the district of Cusco in the year 2023, through the application of ISO 27032. The type of research was applied and Pre experimental design. The population sample was 100 people and the survey was used as a data collection tool. Three (3) specific objectives were evaluated: degree of user training, degree of compliance with ISO 27032 and analysis of information security risks. Significant results were obtained regarding the users' perception of security risks, the need for training and the degree of compliance with ISO 27032. The general hypothesis put forward was confirmed, evidencing the importance of the application of ISO 27032 to improve information security in the Facebook Marketplace in the district of Cusco in the year 2023.

*Keywords: Information security, Facebook Marketplace, ISO 27032 standard.*

## I. INTRODUCCIÓN

En la era digital actual, la importancia de la seguridad de la información ha aumentado significativamente. Con el creciente uso de tecnologías y aplicaciones en línea, la salvaguarda de información personal y la protección de datos se han convertido en elementos clave para el crecimiento y la confianza en los sistemas informáticos. Los Marketplace son plataformas digitales que ofrecen una masiva cantidad de servicios y productos, pero también son entornos propicios para la vulneración de la seguridad de la información de los usuarios. En este sentido, es fundamental analizar los riesgos y brechas en materia de seguridad a los que se encuentran expuestos los vendedores y compradores del Marketplace de Facebook en el distrito de Cusco, y evaluar el grado de cumplimiento de la norma ISO 27032 en relación al manejo de la seguridad de la información. De esta manera, se podrán proponer mejoras y medidas que permitan garantizar la privacidad y protección de los datos de los usuarios en dicha plataforma.

En la actualidad en el distrito de Cusco el crear grupos de redes sociales como Facebook con la finalidad de vender y comprar todo tipo de bienes, productos o servicios se ha vuelto común entre nuestra comunidad en internet, numerosas empresas y pequeños negocios se han dado cuenta de la relevancia que tiene esta red social para llevar a cabo sus actividades, cada marca popular está en Facebook, la red social puede ayudar a empresas en crecimiento llegar a más personas y potenciales clientes, la mayoría de usuarios busca las marcas y productos en Facebook, en esta red social, es nuestra responsabilidad cuidar nuestra información de otras personas, mientras más información compartamos, somos más propensos a sufrir pérdida de datos, es importante recordar que toda esta información compartida en la red social es pública y cualquier persona tiene acceso a ella.

A **nivel Internacional**, la gestión de la seguridad de la información ha adquirido una relevancia cada vez mayor. La exposición de datos personales y empresariales a través de Internet y la dependencia de las tecnologías de la información para poder realizar actividades cotidianas, ha generado un

aumento en la cantidad de riesgos y riesgos que están asociados a la seguridad de la información. En este contexto, los Marketplace en línea se han vuelto uno de los principales blancos para los ciberdelincuentes, quienes aprovechan las vulnerabilidades en la gestión de la seguridad de la información de estas plataformas para obtener información sensible y realizar actividades ilícitas. Esta realidad problemática hace necesario el desarrollo de investigaciones que permitan identificar las brechas de seguridad en los Marketplace, así como proponer soluciones para fortalecer su seguridad y proteger a los usuarios de posibles ataques.

**En el Perú**, sobre todo en los últimos años, la presencia de redes sociales se ha fortalecido, y Facebook es una de las más populares. La creciente cantidad de usuarios que utilizan esta plataforma para comprar y vender productos en línea ha llevado a la necesidad de mejorar y garantizar la seguridad de la información de los usuarios. Sin embargo, se han reportado casos de violaciones de seguridad en estas plataformas, poniendo en riesgo la disponibilidad, confidencialidad e integridad de los datos personales de todos los usuarios. Es por eso que se hace necesario analizar la seguridad de la información en el Marketplace de Facebook en el distrito de Cusco, con el objetivo de identificar las brechas de seguridad y proponer soluciones que puedan garantizar la correcta protección de la información de los usuarios.

En el **distrito de Cusco**, aunque muy escaso viene creciendo, muchas tiendas ya cuentan con su propia página o plataforma web a través de la cual pueden ofrecer sus servicios o productos, plataformas gratuitas como por ejemplo el Marketplace de Facebook son algunas alternativas muy prácticas donde las personas comunes podemos realizar actividades como la compra y venta de distintos objetos mediante un muy sencillo diseño interfaz y fácil de entender, sin tener que gastarse demasiado tiempo y dinero en comprar o hacer una página web. La fácil accesibilidad a estas plataformas hace que encontrarse con personas con malas intenciones sea mucho más propenso, y muchos usuarios tanto como empresas quedan expuestas a diferentes tipos de fraudes; Phishing, Spamming, Carding, Compras Online, Falsas ofertas de empleo, etc.

En tal sentido se tiene los **Marketplace de Facebook**, el crear grupos en esta red social, con la finalidad de vender y comprar todo tipo de bienes, productos y servicios se ha vuelto muy común entre nuestra comunidad, sin embargo, el no cumplir con todos los requisitos establecidos por la norma ISO 27032 aumenta el riesgo de ataques cibernéticos y robo de información personal, lo que puede tener consecuencias graves para los usuarios afectados. Por lo tanto, esta investigación pretende evaluar y analizar el grado de cumplimiento de la norma ISO 27032 en los Marketplace de Facebook en el distrito de Cusco, así como identificar las brechas de seguridad de la información que no cumplen con las exigencias de la norma.

Si bien es cierto los Marketplace de Facebook han ido surgiendo con más frecuencia y desarrollándose en los últimos años, aun así, presentan algunos riesgos a la hora de realizar el comercio electrónico como son: Se cuenta con insuficiente capacitación de los usuarios en los Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información, se cuenta con un grado de incumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco, se cuenta con vulnerabilidades de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco.

A continuación, se **formula el problema general** de la investigación: ¿De qué manera la aplicación de la Norma internacional ISO 27032 influye en la Seguridad de la Información en los Marketplace de Facebook, Cusco 2023?

Asimismo, se presenta la **justificación de la investigación** como sigue. *Conveniencia*, este trabajo permite mejorar la imagen de la plataforma, *Relevancia social*, este trabajo incluye un beneficio para el usuario de la plataforma, *utilidad metodológica*, la investigación sirve como base para futuras investigaciones sobre los Marketplace en redes sociales, *Implicancias prácticas*, permite solucionar dudas y problemáticas que estén vinculadas a las compras, robo de datos y otras amenazas en los Marketplace. *Valor*

*teórico*, esto contribuye a una mayor comprensión de las teorías relacionadas con la seguridad de la información y la norma ISO 27032.

En este trabajo de investigación, se formulan los siguientes **objetivos**:  
*General*: Identificar de qué manera la aplicación de la Norma internacional ISO 27032 influye en la Seguridad de la Información en los Marketplace de Facebook, Cusco 2023; *Específicos*: Determinar el grado de capacitación de los usuarios en los Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información, Evaluar el grado de cumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco, Analizar los riesgos de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco.

Finalmente, esta investigación formula la siguiente **hipótesis** general: “La aplicación de la norma ISO 27032 mejora de forma significativa la seguridad de la información en los Marketplace de Facebook en la ciudad. de Cusco en el año 2023.”

## II. MARCO TEÓRICO

Lykhova, Servatiuk y Shamsutdinov (2022), El contenido del artículo científico se centra en la seguridad de la información como un concepto social, sus características y aspectos, y las normativas relacionadas que mejoran el proceso de seguridad de la información. Se hace hincapié en que la seguridad de la información es un tema multidisciplinario y se aplicaron diferentes métodos, como el formal-lógico y el sistémico-estructural, además del análisis documental para examinar el marco normativo. La investigación identifica tres niveles de seguridad de la información, que son el personal, social y estatal, y varían según el nivel de la información en cuestión.

De Acuerdo a Limache (2022), El propósito de esta investigación es lograr una mejora en la gestión de incidentes de seguridad de la información en la empresa LISERME S.R.L., ubicada en Arequipa, implementando la Norma Internacional ISO 27035:2016 esto en el año 2022. Se plantea la hipótesis de que la aplicación de esta norma tendrá un impacto positivo significativo en la gestión de incidentes de seguridad de la información en la empresa. Este estudio es de naturaleza aplicada y de nivel preexperimental, y se utilizarán varios indicadores, como el tiempo promedio de respuesta de los incidentes atendidos, el porcentaje de respuesta de incidentes atendidos, el porcentaje de reincidencia de incidentes y el nivel de satisfacción del personal, para evaluar los resultados de la implementación de la norma.

De Acuerdo a Orihuela (2022), en el trabajo de investigación se destaca que las amenazas informáticas están en constante evolución y se vuelven cada vez más sofisticadas, lo que puede ocasionar riesgo la seguridad de la información en algunas empresas. Además, se argumenta que la formación en seguridad de información que reciben los empleados puede ser insuficiente para garantizar un nivel adecuado de conciencia y buenas prácticas para evitar ser víctimas de ciberataques involuntariamente. Para abordar este problema, se propone una innovación educativa enfocada en mejorar la limitada conciencia en seguridad de información de los empleados de una empresa de telecomunicaciones en Lima, especialmente en relación a los

ciberataques de ingeniería social que los llevan a tomar acciones incorrectas y riesgosas en sus interacciones en línea.

Según Guerra y Neira (2021), El artículo propone la implementación de un sistema de gestión de la información en las bibliotecas universitarias, basado en la metodología de identificación y análisis de riesgos. Para lograr este objetivo, se adaptó la norma ISO/IEC 27001:2013 y se aplicó la metodología MARGERIT en una biblioteca universitaria. Los resultados del análisis de riesgos intrínseco y efectivo revelaron la presencia de salvaguardas y la evaluación de los impactos. Se determinó el porcentaje de afectación en cada riesgo por proceso de calidad, se identificaron medidas correctivas y se incorporaron formatos de registro. Se concluyó que la inclusión de los formatos propuestos para el control y las auditorías en los indicadores de calidad permitió optimizar el sistema de gestión de seguridad de la información (SGSI) para los procesos de la biblioteca universitaria.

Estrada, Unás y Flórez (2021), nos indican que la pandemia del COVID-19 llevó a medidas de confinamiento masivo y una respuesta de emergencia en todo el mundo para frenar la propagación del virus, lo que también produjo cambios en la forma en que las personas interactúan socialmente, especialmente en el ámbito virtual, como en la educación, atención médica y empleo. No obstante, los delincuentes utilizaron esta situación para intensificar los delitos electrónicos, como el phishing, las noticias falsas y la inyección de malware. Con el fin de determinar las prácticas de seguridad de la información en una comunidad universitaria, se llevó a cabo una encuesta utilizando un enfoque de investigación mixto que tomó en cuenta la pandemia como un factor clave que llevó a la adopción de nuevos hábitos de higiene digital.

De acuerdo a Saavedra Agudelo (2020), se llevaron a cabo diversas técnicas, procedimientos y métodos para construir y diseñar un proyecto aplicado que incluyó la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y la administración de la ciberseguridad. El objetivo de este proyecto fue implantar, monitorear, operar, verificar,

mantener, sostener y mejorar el sistema mencionado, para así mejorar la seguridad del sistema y gestionar posibles riesgos en el sistema de información. El caso de estudio utilizado fue la empresa QWERTY S.A y se basó en las normas internacionales ISO/IEC 27001 y ISO/IEC 27032 como referencia.

Según Apaza (2021), en su artículo científico presentó una propuesta para el diseño de un plan de seguridad de la información en el banco Ripley, que tiene como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de los datos. Para lograr esto, se aplicaron las normas ISO/IEC 27001 y 27002 para identificar los controles apropiados a implementar. La propuesta incluyó la definición de responsabilidades y la información manejada en cada proceso y área del banco, así como la priorización del manejo de la información por áreas y la identificación de los activos críticos. Se definieron políticas y se realizó un análisis de gestión de riesgos, seguido de la definición del plan con los controles de la norma ISO/IEC 27002. Por último, se presentaron indicadores para evaluar la efectividad del plan en el aumento de la confiabilidad de los datos del banco.

De acuerdo a Rangel (2020), durante el desarrollo de su proyecto, el objetivo fue implementar prácticas efectivas de ciberseguridad en la empresa Sistemas y Computadores S.A. utilizando las directrices de la norma ISO/IEC 27032. El propósito de esta implementación fue establecer un marco seguro para el manejo de incidentes, la coordinación y el intercambio de información, permitiendo que la empresa tuviera la capacidad de reaccionar ante eventos de seguridad y ataques para proteger adecuadamente sus sistemas. Para lograrlo, se realizó un análisis de todos los activos de información expuestos en el ciberespacio, identificando posibles vulnerabilidades y amenazas que pudieran poner en riesgo la seguridad de la información. En el proyecto, con base en esta matriz de riesgos, se definieron los controles necesarios para reducir el riesgo residual.

De acuerdo a Guzmán (2019) durante su investigación, se desarrolló una guía que permite a las organizaciones implementar las buenas prácticas de la

norma ISO 27032. Esta guía se enfoca en identificar los requerimientos de la norma, comenzando con la creación de un inventario de activos y evaluando los riesgos a los que está expuesta la información en el ciberespacio. A partir de esta evaluación, se generan controles que ayudan a mitigar las amenazas que pueden poner en riesgo la continuidad de las actividades de la organización.

De acuerdo a Migone (2017), en su investigación “El e-commerce y su relación con la satisfacción del cliente de los microempresarios San Martín de Porres, 2017” tiene como objetivo el determinar la relación que existe entre sus dos variables de estudio el comercio electrónico y la satisfacción de los clientes. La muestra en la encuesta incluyó a un total de 80 clientes. Se aceptó la hipótesis general del estudio, se observó una correlación entre sus dos variables las cuales son comercio electrónico y la satisfacción que tiene el cliente fue de 0,814, y los valores obtenidos se correlacionaron algo positivamente.

En el presente trabajo de investigación se han utilizado diversas **bases teóricas** como base para una mejor comprensión del tema:

*Norma:* Una norma es un documento que no es obligatorio de utilizar y que se crea a través del consenso de las partes interesadas, y que debe ser aprobado por un organismo de Normalización reconocido (García-Cervigón Hurtado, et al., 2011).

*ISO:* La Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) es un organismo global que se encarga de establecer normas y estándares de normalización en diversos campos, incluyendo la informática. (García-Cervigón Hurtado, et al., 2011).

*ISO 27032:* Es una guía sobre ciberseguridad, esta Norma Internacional proporciona orientación técnica para hacer frente a los riesgos comunes de Ciberseguridad, incluyendo; ataques de ingeniería social, la piratería informática, la proliferación de software malicioso ("malware"), programas

espía, y otros programas potencialmente no deseados. Las orientaciones técnicas proporcionan controles para hacer frente a estos riesgos (ISO, 2012).

*Seguridad:* Significa contar con recursos que permitan minimizar en la mayor medida posible la vulnerabilidad de la información y los recursos. Aunque es imposible alcanzar el 100% de seguridad, el objetivo debe ser acercarse a ese nivel máximo de protección ("Políticas y Seguridad de la Información", 2008).

*Información:* La información es un recurso fundamental en las organizaciones y, por lo tanto, debe ser protegida mediante una serie de medidas, políticas y controles de seguridad que se implementan con el apoyo de recursos humanos, hardware y software ("Políticas y Seguridad de la Información", 2008).

*Seguridad de la Información:* El nivel de seguridad de información de una organización se encuentra influenciado por diversos factores, como la correcta gestión y los procedimientos apropiados, la capacitación y comportamiento de los empleados, la fiabilidad de los proveedores y la seguridad de los medios técnicos utilizados ("Políticas y Seguridad de la Información", 2008).

*Marketplace:* La idea fundamental de los Marketplace, y el punto de partida para comprender su funcionamiento, es que se trata de plataformas digitales donde convergen distintos vendedores y compradores para llevar a cabo transacciones relacionadas con productos y/o servicios (Pardo Puentes, et al., 2022).

*Facebook:* Es una web fundada por Mark Zuckerberg, un estudiante de Harvard, en febrero de 2004 como una red social en línea. En un principio, se utilizaba para la comunicación entre estudiantes dentro de la universidad, pero dos años después se abrió al público en general. Desde entonces, con su popularidad a nivel mundial, ha surgido como la red social líder, lo que ha llevado al desarrollo de aplicaciones externas y ha establecido un modelo que ha sido adoptado por la mayoría de otras redes sociales. ("Facebook y vida cotidiana", 2012)

### III. METODOLOGÍA

#### 3.1 Tipo y diseño de investigación

- Tipo de investigación  
  
Aplicada
- Diseño de investigación  
  
Diseño experimental: preexperimental.

#### 3.2 Variables y operacionalización

- Variables
  - Independiente: Aplicación de la Norma internacional ISO 27032
    - Definición conceptual

“Esta norma define los problemas de ciberseguridad que se originan por la falta de coordinación entre los diferentes dominios de seguridad en este ámbito. Esta norma proporciona una guía técnica para hacer frente a los riesgos de ciberseguridad más comunes” (ISO, 2012).

- Definición Operacional

En la medición de la implementación de la norma ISO 27032 se utilizaron herramientas de análisis y evaluación de riesgos, lo que permitió la identificación de algunos riesgos de seguridad de la plataforma, así como la evaluación de su impacto y la probabilidad de que siga ocurriendo. A partir de esta información obtenida, se pueden tomar medidas de seguridad que sean adecuadas para mitigar los riesgos identificados y mejorar la aplicación de la norma.

- Dependiente: Seguridad la información

- Definición Conceptual

“La seguridad de la información se refiere a la garantía de que la información se mantenga siempre confidencial, íntegra y esté disponible, también puede implicar otras características como son la autenticidad, la responsabilidad, no repudio y fiabilidad.” (ISO, 2012).

- Definición Operacional

Para medir la seguridad de la información en un Marketplace de Facebook se puede revisó las políticas de privacidad y seguridad de Facebook y del Marketplace, verificar la reputación de los vendedores, verificar el nivel de uso del Marketplace, evitar compartir información personal y financiera innecesaria, y estar alerta a posibles estafas.

- Operacionalización

La operacionalización de las variables de estudio se encuentra especificada en la matriz de operacionalización (ver Anexo 2).

### **3.3 Población, muestra y muestreo**

- Población

Para poder definir la población, se aplicaron los criterios de selección que se detallan a continuación.

- Criterios de inclusión: La población objetivo en esta investigación son todas aquellas personas entre las edades de 18 a 70 años, residentes del distrito de Cusco, que hayan interactuado alguna vez en los Marketplace de Facebook, y que tengan una cuenta activa en esta red social.

- Criterios de exclusión: Usuarios con cuentas inactivas en la red social.

Después de haber establecido las características necesarias que debían presentar los individuos que son parte de la población que es objetivo de estudio, se concluyó que el tamaño de la población objetivo es desconocido debido a la falta de datos precisos y confiables al respecto.

- Muestra

Para el presente trabajo de investigación se seleccionó una muestra de 100 personas que cumplieron con todos los criterios de inclusión previamente establecidos, en la cual se asignó a los participantes de forma aleatoria.

- Muestreo

Se decidió utilizar una técnica de muestreo no probabilístico debido a que la población objetivo de la investigación es difícil de acceder y no se cuenta con un listado completo de individuos que cumplan con los criterios de inclusión establecidos. En tal sentido, se ha utilizado un muestreo por conveniencia para seleccionar a los participantes de la muestra.

### **3.4 Técnicas e instrumentos de recolección de datos**

- Técnicas
  - Observación
  - Encuesta
  - Análisis documental
- Instrumentos
  - Ficha de observación

- Cuestionario (Encuesta)
- Validez y confiabilidad
  - Validez

La validez en una investigación se refiere a la capacidad de un instrumento de medición para poder medir de manera precisa y confiable la variable que se desea evaluar. Para asegurar la validez de un instrumento, es importante analizar minuciosamente sus preguntas o ítems para verificar que estén relacionados con la variable que se desea medir y que sean apropiados para la población objetivo.

La validez de los instrumentos de recolección de datos fue establecida por el *Método de juicio experto* (Ver Anexo 4).

- Confiabilidad

Se refiere a la consistencia o estabilidad de los resultados obtenidos a través de un instrumento de medición.

La confiabilidad de los instrumentos de recolección de datos de la presente investigación (Cuestionario) fue determinada por el coeficiente estadístico *Alfa de Cronbach* (ver Anexo 5)

### 3.5 Procedimientos

Se detallará a continuación, el proceso que se siguió para lograr los objetivos específicos de la investigación.:

- Determinar el grado de capacitación de los usuarios en los Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información.

Para determinar el grado de capacitación de los usuarios sobre seguridad de la información en los Marketplace de Facebook en Cusco

en el 2023, fue necesario realizar dos encuestas: una previa a la aplicación de la norma ISO 27032 y otra después de su implementación. La encuesta previa permitió establecer el nivel de conocimiento y capacitación que tienen los usuarios acerca de seguridad de la información previa a la aplicación de la norma ISO 27032, mientras que la encuesta posterior permitió evaluar el impacto que tuvo la aplicación de la norma ISO 27032 en el grado de capacitación de los usuarios. Se diseñó un cuestionario que contenga preguntas sobre las mejores y más comunes prácticas de seguridad de la información, para poder realizar un análisis de los resultados y así obtener conclusiones más precisas y determinar si es que existe una relación significativa entre la capacitación de los usuarios y la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco.

- Evaluar el grado de cumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco.

Para llevar a cabo esta evaluación se empleó un cuestionario con 6 preguntas que permitieron conocer el grado de cumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco. A través de este cuestionario se evaluaron aspectos clave como la existencia de una política de seguridad de la información, la identificación y evaluación de la información importante, las medidas de seguridad implementadas, los procedimientos de respuesta a incidentes de seguridad, los controles de acceso físico y lógico, y las medidas de seguridad específicas para la protección de los datos personales de los usuarios, también se realizó una revisión documental de las políticas de seguridad de la información que Facebook implementa para proteger a los usuarios de su plataforma de Marketplace.

- Analizar los riesgos de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco.

Se realizó un cuestionario en conjunto a una revisión bibliográfica y documental para identificar los riesgos de seguridad de la información en el uso de Marketplace, en general, y en el de Facebook, en particular, analizar los datos recolectados para identificar los riesgos de seguridad de la información a los que están expuestos los usuarios del Marketplace de Facebook en el distrito de Cusco.

### **3.6 Método de análisis de datos**

Se aplicó el método estadístico de procesamiento y análisis de datos, tanto a nivel descriptivo como inferencial.

Con respecto a la estadística descriptiva se refiere a describir y resumir los datos que se han recolectado en una muestra o población. En otras palabras, se busca presentar los datos de manera organizada y comprensible para facilitar su análisis e interpretación.

Con respecto a la estadística inferencial se encarga de hacer inferencias sobre una población basándose en los datos recolectados de una muestra. Es decir, se utilizará la información obtenida de una muestra para hacer estimaciones o conclusiones sobre una población más grande. La estadística inferencial también permite probar hipótesis y determinar la significancia estadística de los resultados obtenidos en un estudio.

### **3.7 Aspectos éticos**

El cuestionario que se utilizó en la investigación fue anónimo, es decir, no requerirá conocer la identidad de los participantes para poder relacionar sus respuestas o conjunto de respuestas. Esto se hará para proteger la confidencialidad de la información recolectada, que será utilizada únicamente para fines de investigación.

La Norma ISO-690 se utilizó para referenciar adecuadamente las ideas, conocimientos y teorías de los autores en la elaboración de la investigación, con el fin de evitar la apropiación indebida de sus ideas. Además, se garantiza que toda la información presentada en la investigación es precisa y verdadera.

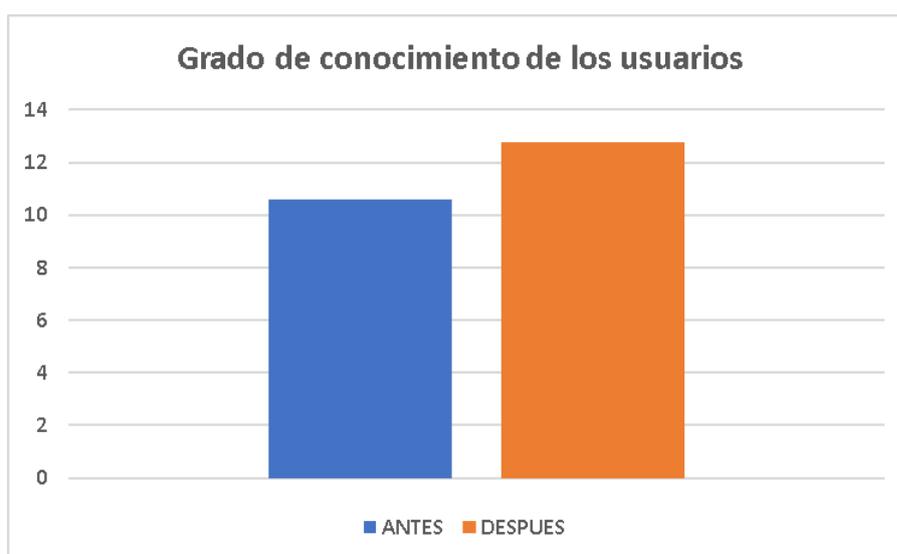
#### IV. RESULTADOS

- **Análisis descriptivo:**

- **Indicador 1: Nivel de conocimiento de los usuarios**

La seguridad de la información en Facebook Marketplace es un tema importante que afecta a los usuarios de la plataforma. Con el fin de evaluar el nivel de conocimiento de los usuarios sobre las políticas de seguridad de Facebook respecto a los Marketplace, se realizó una encuesta 2 veces a 100 usuarios de los Marketplace de Facebook en el distrito de Cusco, una encuesta pre aplicación de la norma ISO 27032 y una encuesta post aplicación de la norma ISO 27032. La encuesta constó de cinco preguntas enfocadas en medir la familiaridad de los usuarios con las políticas de seguridad de Facebook, la percepción sobre el cumplimiento de las políticas por parte de los usuarios, la experiencia de los usuarios con incidentes de seguridad en el Marketplace, la satisfacción con las herramientas de seguridad de Facebook, y la importancia de recibir capacitación en seguridad de la información al utilizar Facebook Marketplace.

*Figura 1. Representación gráfica del grado de conocimiento de los usuarios*



El incremento significativo en el promedio obtenido en la encuesta post, comparado con la encuesta pre, sugiere que la aplicación de la norma ISO 27032 tuvo un efecto positivo en el grado de capacitación de los usuarios de Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información. Esto se puede explicar porque la norma ISO 27032 proporciona un marco de referencia y recomendaciones para la gestión de la seguridad de la información, incluyendo la capacitación y concientización de los usuarios. Por lo tanto, al aplicar la norma en los Marketplace de Facebook en el distrito de Cusco, se pudo haber mejorado la calidad de la capacitación brindada a los usuarios, lo que se reflejó en una mayor comprensión y aplicación de las mejores prácticas de seguridad de la información por parte de los mismos.

A continuación, se presenta el análisis de cada pregunta del cuestionario mediante la utilización de gráficos de barras:

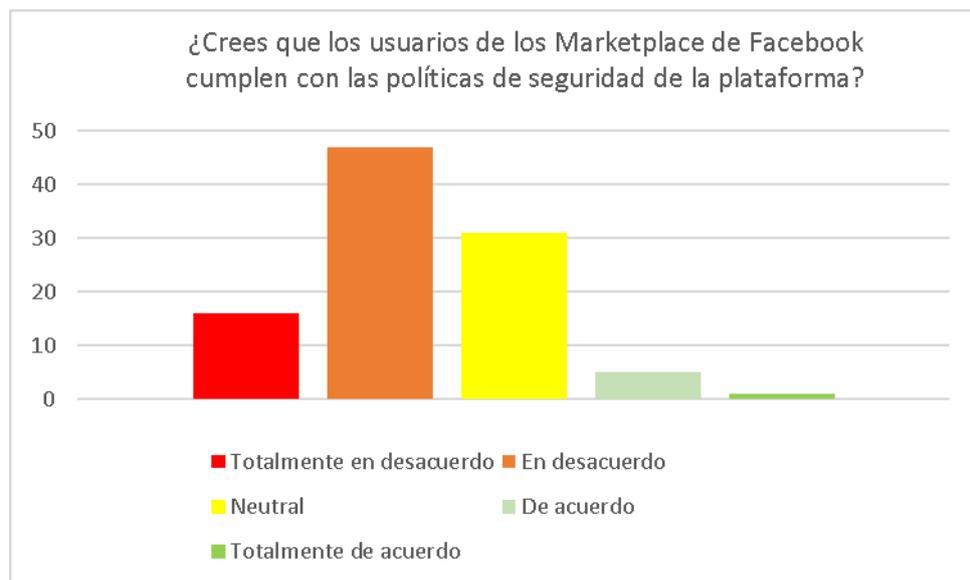
*Figura 2. Familiarización de los usuarios con las políticas de seguridad de Facebook con respecto a los Marketplace.*



En la pregunta 1, podemos observar que una mayoría significativa de los encuestados (42% totalmente en desacuerdo y 34% en desacuerdo) no están familiarizados con las políticas de seguridad de

Facebook respecto a los Marketplace. Esto indica una falta de conocimiento y conciencia sobre las políticas de seguridad establecidas por la plataforma. Es importante señalar que la falta de conocimiento y conciencia puede llevar a los usuarios a no tomar las suficientes medidas de seguridad necesarias para proteger su información personal y financiera.

*Figura 3. Cumplimiento de las políticas de seguridad por parte de los usuarios de la plataforma*



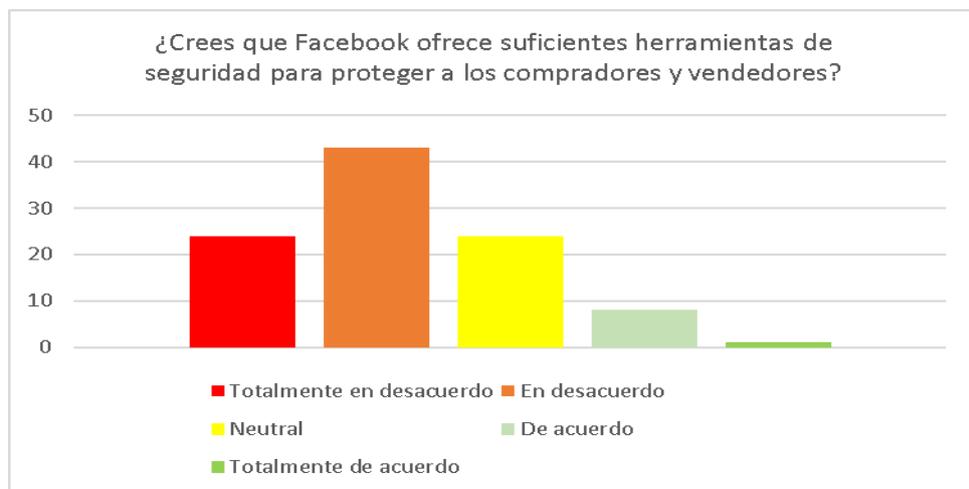
En cuanto a la segunda pregunta, los resultados muestran que la mayoría de los encuestados (63% en total) no confían en que ellos mismo como usuarios de los Marketplace de Facebook cumplan con las políticas de seguridad de la plataforma. Esto podría deberse a experiencias previas de compras o ventas problemáticas, o simplemente a una percepción general de que los usuarios no toman en serio la seguridad de la información.

Figura 4. Incidentes experimentados por los usuarios de la plataforma.



La tercera pregunta se centró en si los encuestados habían experimentado algún incidente de seguridad en su grupo de Facebook Marketplace. Los resultados indican que la mayoría de los encuestados (72%) no han experimentado ningún incidente. Sin embargo, es importante señalar que esta respuesta podría estar sesgada debido a la falta de conocimiento o reconocimiento de incidentes de seguridad. Muchos usuarios pueden no ser conscientes de que han sido víctimas de un incidente de seguridad o no saben cómo reportarlo.

Figura 5. Percepción de los usuarios respecto a las herramientas de seguridad por parte de Facebook Marketplace.



La cuarta pregunta se refiere a si los encuestados creen que Facebook ofrece suficientes herramientas de seguridad para proteger a los compradores y vendedores. Los resultados indican que la mayoría de los encuestados (67%) no están satisfechos con las herramientas de seguridad proporcionadas por Facebook. Esto podría deberse a la percepción de que la plataforma no ofrece suficientes herramientas para proteger a los usuarios de fraudes y estafas.

*Figura 6. Opinión de los usuarios respecto a la capacitación sobre seguridad de la información al utilizar los Marketplace de Facebook.*



Por último, la quinta pregunta se centró en si los encuestados consideran importante recibir capacitación sobre seguridad de la información al utilizar los Marketplace de Facebook. Los resultados muestran que una mayoría significativa de los encuestados (59%) está de acuerdo o totalmente de acuerdo en que es importante recibir capacitación. Esto sugiere que los usuarios reconocen la necesidad de mejorar su conocimiento y habilidades en materia de seguridad de la información para poder protegerse de posibles amenazas y riesgos.

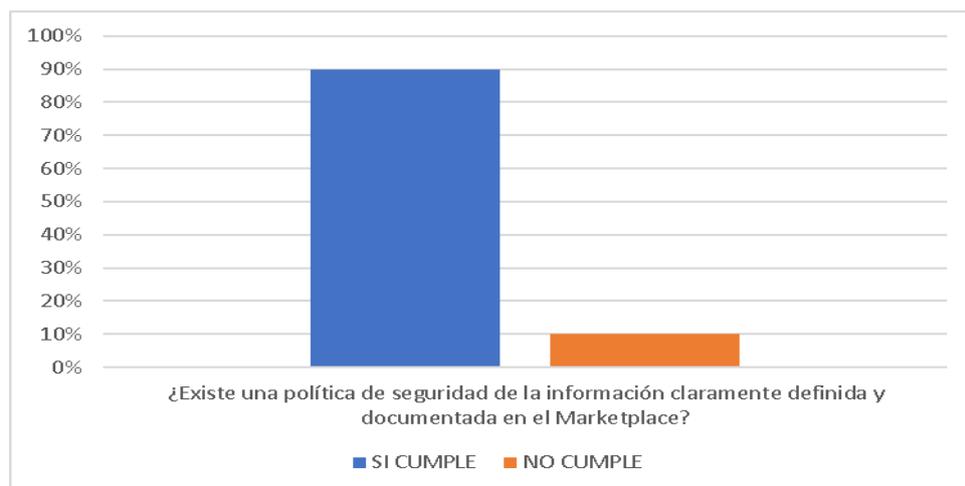
En general, los resultados obtenidos de la encuesta sugieren que hay una falta de conocimiento y conciencia sobre las políticas de seguridad de Facebook en relación a los Marketplace. También sugieren

que los usuarios no confían en que otros usuarios cumplan con las políticas de seguridad, no están satisfechos con las herramientas de seguridad proporcionadas por Facebook y reconocen la necesidad de recibir capacitación en seguridad de la información. Estos resultados podrían ayudar a Facebook a tomar algunas decisiones, mejorar su estrategia de seguridad y a proporcionar mejores herramientas y recursos para proteger a los usuarios de posibles riesgos y amenazas en los Marketplace.

- Indicador 2: Nivel de cumplimiento de las políticas de seguridad

A continuación, presentaremos los resultados de la evaluación, que nos permitirán tener una idea clara del estado actual de la seguridad de la información en estos Marketplaces y las recomendaciones para mejorar su gestión. Los resultados obtenidos a partir de este cuestionario son de gran importancia, ya que permiten conocer la situación actual en cuanto a la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco.

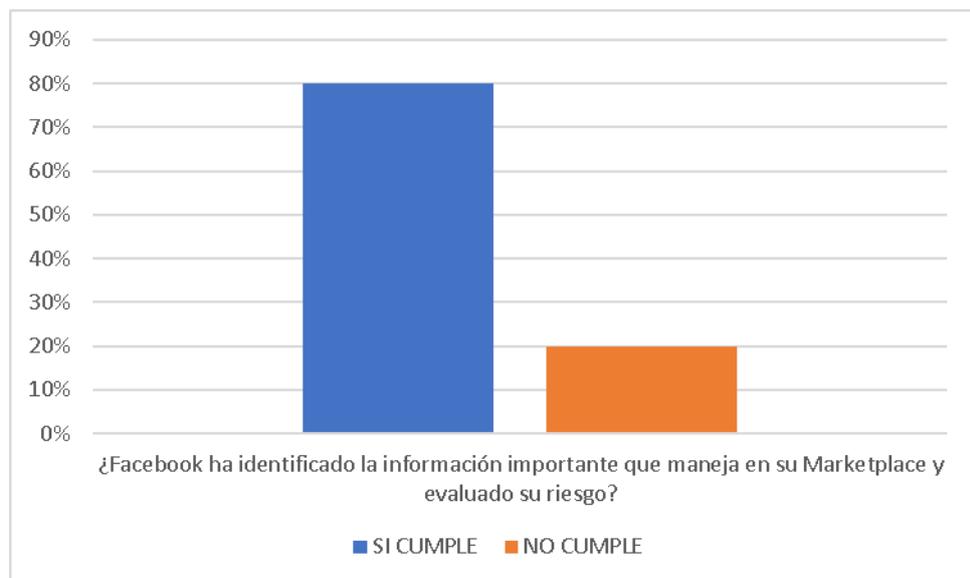
*Figura 7. Cumplimiento de las políticas de seguridad.*



En un 90% de los casos, se ha identificado que existe una política de seguridad de la información claramente definida y documentada en el

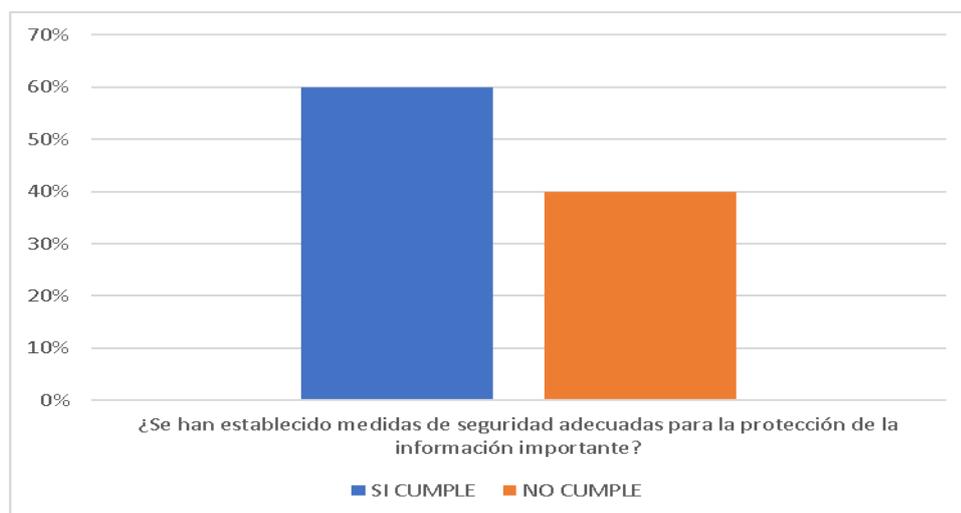
Marketplace de Facebook. Esto es un indicativo positivo, ya que una política de seguridad de la información es esencial para establecer un marco de referencia y normas claras para garantizar la seguridad de los datos y sistemas en el Marketplace. Es posible que este alto porcentaje se deba a que Facebook es una empresa reconocida mundialmente y tiene la capacidad de implementar políticas de seguridad bien definidas.

*Figura 8. Identificación de la información importante por parte de Facebook Marketplace.*



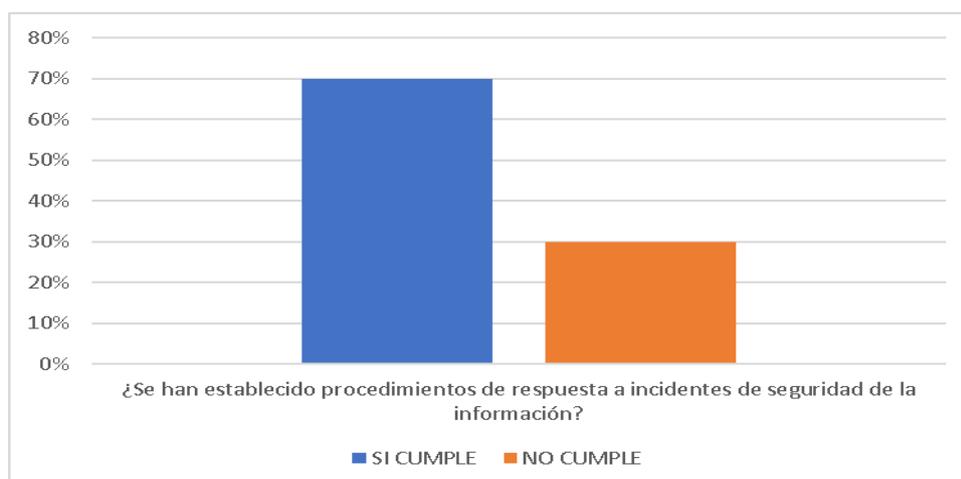
En un 80% de los casos, se ha identificado que Facebook ha evaluado la importancia de la información que maneja en su Marketplace y el riesgo que existe de que dicha información sea comprometida o robada. Esto es fundamental para establecer medidas de seguridad adecuadas y garantizar la protección de los datos de los usuarios. Es posible que este porcentaje se deba a la conciencia creciente de la importancia de la protección de datos.

*Figura 9. Cumplimiento de las medidas de seguridad establecidas para la protección de la información importante.*



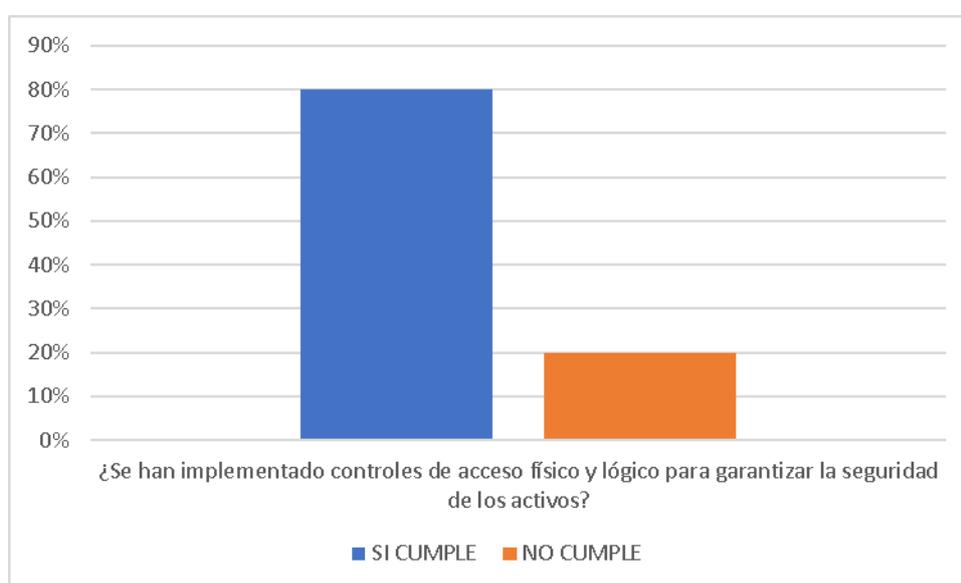
En un 60% de los casos, se ha identificado que se han establecido medidas de seguridad adecuadas para la protección de la información importante en el Marketplace de Facebook. Este porcentaje no es muy alto y sugiere que aún hay un margen de mejora en cuanto a la seguridad de los datos en el Marketplace. Es posible que este bajo porcentaje se deba a la complejidad de implementar medidas de seguridad efectivas en un entorno digital tan grande y cambiante como el Marketplace de Facebook.

*Figura 10. Procedimientos establecidos en respuestas a incidentes de seguridad de la información.*



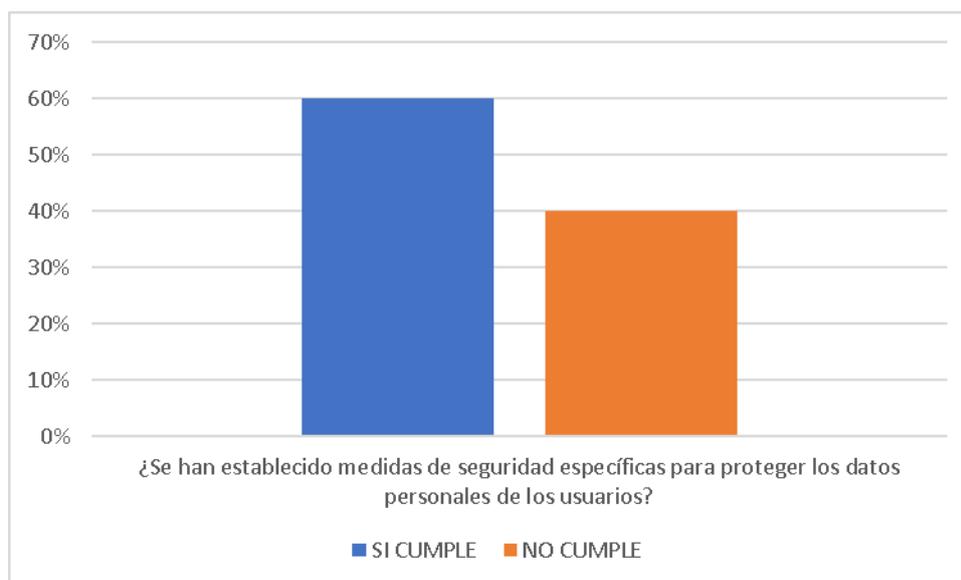
En un 70% de los casos, se ha identificado que se han establecido procedimientos de respuesta a incidentes de seguridad de la información. Esto es fundamental para poder actuar de manera efectiva en caso de que se produzca un incidente de seguridad. Es posible que este porcentaje se deba a que Facebook es una empresa que cuenta con experiencia en el manejo de incidentes de seguridad y que ha establecido un plan de respuesta a incidentes bien definido.

*Figura 11. Implementación de controles de acceso físico y lógico para garantizar seguridad de información,*



En un 80% de los casos, se ha identificado que se han implementado controles de acceso físico y lógico para garantizar la seguridad de los activos de información. Esto es importante para garantizar que solo las personas autorizadas tengan acceso a la información en el Marketplace de Facebook. Es posible que este alto porcentaje se deba a la necesidad de cumplir con regulaciones de seguridad y protección de datos, así como a la conciencia creciente de la importancia de la seguridad de la información.

*Figura 12. Implementación de medidas de seguridad específicas para proteger los datos personales.*



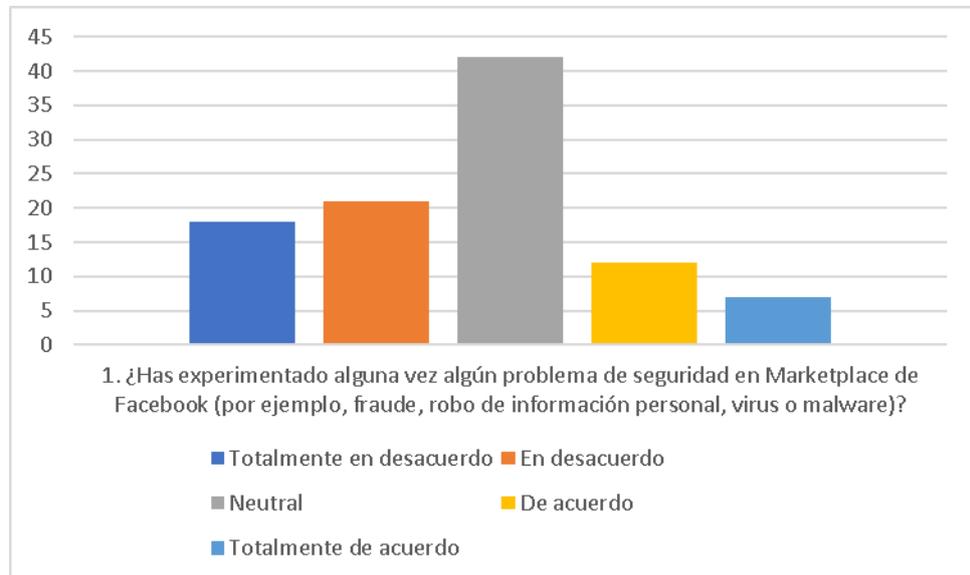
En la última pregunta del cuestionario, el 60% de los casos de los Marketplace indicaron que sí se han establecido medidas de seguridad específicas para proteger los datos personales de los usuarios en el Marketplace de Facebook, mientras que el 40% de los casos indicaron que no. Es importante destacar que la protección de los datos personales de los usuarios es un aspecto crucial en la gestión de la seguridad de la información en los Marketplace de Facebook, ya que estas plataformas manejan grandes cantidades de información personal de los usuarios, como nombres, direcciones, números de teléfono, entre otras.

- **Indicador 3: Frecuencia de incidentes de seguridad de la información**

Con el objetivo de analizar los riesgos de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco. Se empleó un cuestionario dirigido a los usuarios de los Marketplace de Facebook para evaluar sus respuestas y conocer su percepción respecto a los incidentes de seguridad de la información en Marketplace de Facebook. Los datos recopilados fueron analizados estadísticamente para determinar la frecuencia de incidentes de seguridad, así como las medidas de

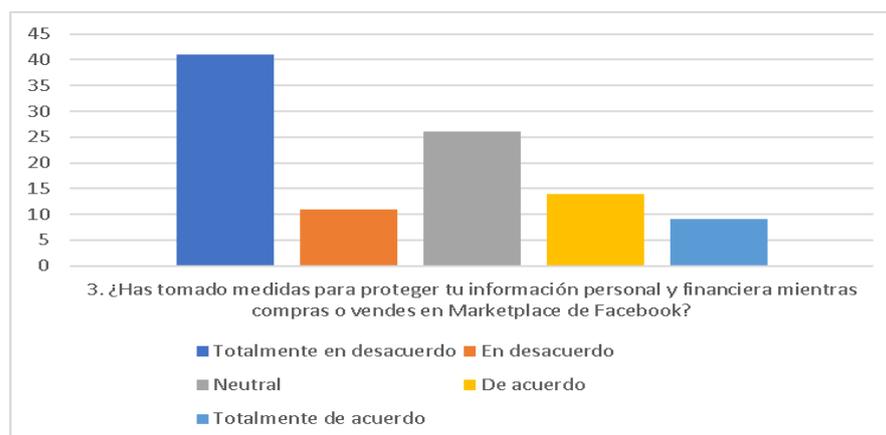
seguridad tomadas por los usuarios y su nivel de capacitación en cuanto a las mejores prácticas de seguridad.

*Figura 13. Problemas de seguridad experimentados por los usuarios de la plataforma.*



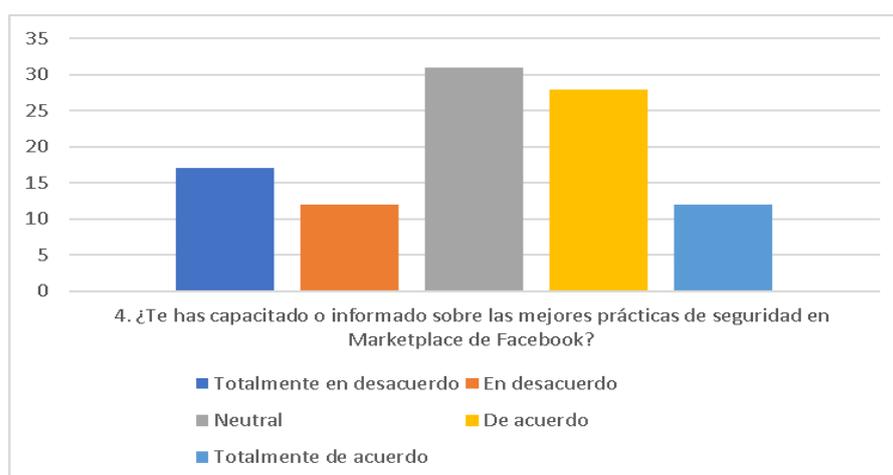
En la primera pregunta del cuestionario, se buscó conocer la frecuencia con la que los usuarios de Marketplace de Facebook en el distrito de Cusco han experimentado problemas de seguridad de la información en la plataforma. Los resultados muestran que el 39% de los encuestados están en desacuerdo o totalmente en desacuerdo con la afirmación de haber experimentado problemas de seguridad en Marketplace de Facebook, mientras que el 54% se encuentra en la categoría de neutral. Solo el 19% de los encuestados se encuentran en la categoría de estar de acuerdo o totalmente de acuerdo con la afirmación.

Figura 14. Medidas para proteger información personal tomadas por los usuarios de la plataforma.



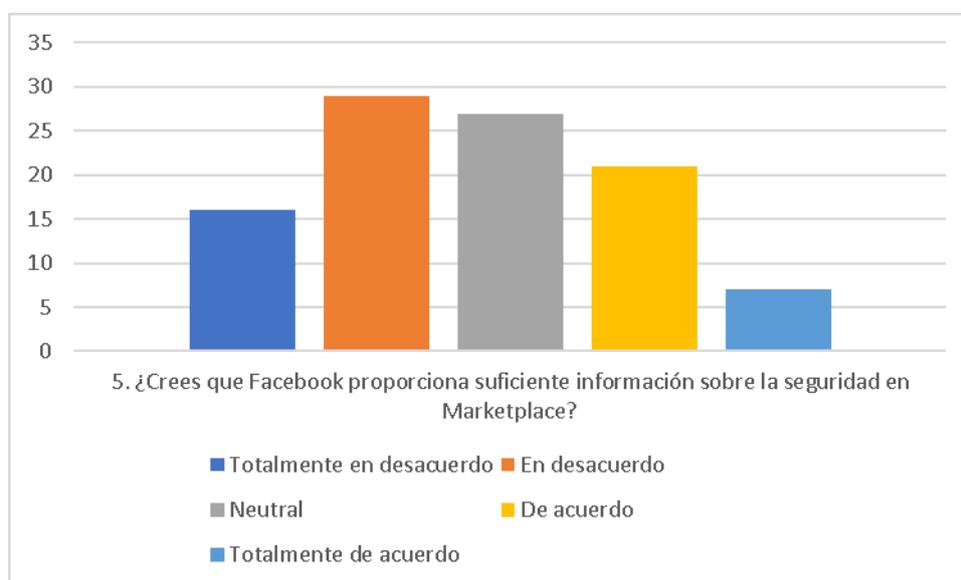
En esta pregunta, se buscó conocer si los usuarios de Marketplace de Facebook en el distrito de Cusco han tomado medidas para proteger su información personal y financiera mientras compran o venden en la plataforma. Los resultados muestran que el 52% de los encuestados están en desacuerdo o totalmente en desacuerdo con la afirmación de haber tomado medidas para proteger su información, mientras que el 34% se encuentra en la categoría de neutral. Solo el 23% de los encuestados se encuentra en la categoría de estar de acuerdo o totalmente de acuerdo con la afirmación.

Figura 15. Iniciativa de capacitación sobre prácticas de seguridad por los usuarios de la plataforma.



En esta pregunta, se buscó conocer si los usuarios de Marketplace de Facebook en el distrito de Cusco han tomado la iniciativa de capacitarse o informarse sobre las mejores prácticas de seguridad en la plataforma. Los resultados muestran que el 29% de los encuestados están en desacuerdo o totalmente en desacuerdo con la afirmación de haberse capacitado o informado sobre las mejores prácticas, mientras que el 31% se encuentra en la categoría de neutral. Solo el 40% de los encuestados se encuentra en la categoría de estar de acuerdo o totalmente de acuerdo con la afirmación.

*Figura 16. Percepción de los usuarios sobre la información sobre seguridad que Facebook proporciona.*

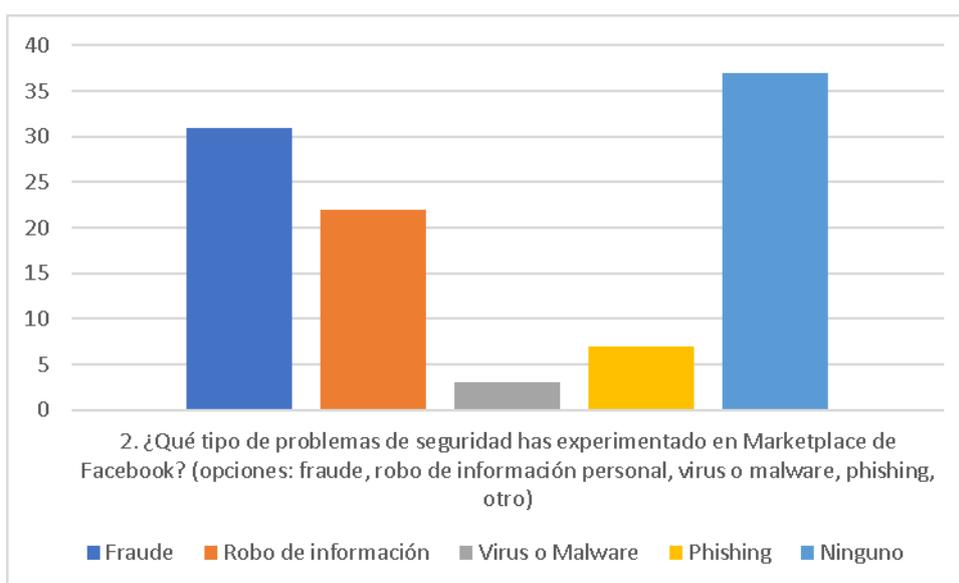


En esta pregunta, se buscó conocer la opinión de los usuarios de Marketplace de Facebook en el distrito de Cusco sobre si la plataforma proporciona suficiente información sobre la seguridad. Los resultados muestran que el 45% de los encuestados están en desacuerdo o totalmente en desacuerdo con la afirmación de que Facebook proporciona suficiente información sobre la seguridad en Marketplace, mientras que el 27% se encuentra en la categoría de neutral. Solo el 28% de los encuestados se encuentra en la categoría de estar de acuerdo

- Indicador 4: Tipo de incidentes de seguridad de la información

para medir el tipo de incidentes de seguridad de la información en el Marketplace de Facebook, se puede utilizó una pregunta en el cuestionario que permitió a los encuestados describir el tipo de incidente de seguridad que han experimentado.

*Figura 17. Tipo de incidentes de seguridad de la información que han experimentado los usuarios de la plataforma.*



En esta pregunta, se buscó conocer los tipos de problemas de seguridad que han experimentado los usuarios de Marketplace de Facebook en el distrito de Cusco. Los resultados muestran que el 31% de los encuestados han experimentado fraude, el 22% robo de información personal, el 7% phishing, y solo el 3% virus o malware. Además, el 37% de los encuestados afirmaron no haber experimentado ningún problema de seguridad en la plataforma.

Fraude: 31 encuestados indicaron que han experimentado algún tipo de fraude en el Marketplace de Facebook. Esto podría incluir estafas de compradores o vendedores, fraudes con tarjetas de crédito, entre otros. Robo de información personal: 22 encuestados indicaron que han experimentado robo de información personal. Esto podría incluir el acceso no autorizado a sus cuentas, la obtención de información

personal a través de técnicas de phishing o la exposición de datos personales debido a una brecha de seguridad. Virus o malware: Solo 3 encuestados indicaron haber experimentado problemas de virus o malware en el Marketplace de Facebook. Esto podría incluir la descarga involuntaria de software malicioso que afecte la seguridad del dispositivo. Phishing: 7 encuestados indicaron haber experimentado problemas de phishing en el Marketplace de Facebook. Esto podría incluir la recepción de correos electrónicos fraudulentos que intentan obtener información personal o financiera del usuario. Ninguno: 37 encuestados indicaron que no han experimentado ningún problema de seguridad en el Marketplace de Facebook.

Según los resultados obtenidos de la encuesta, el tipo de incidente de seguridad más común en el Marketplace de Facebook es el fraude, seguido del robo de información personal y el phishing. Es importante destacar que la mayoría de los encuestados no han experimentado problemas de seguridad en esta plataforma. Sin embargo, es necesario tomar medidas de seguridad para prevenir y protegerse contra estos incidentes en el futuro.

- **Análisis inferencial:**

- Indicador 1: Nivel de conocimiento de los usuarios

***Prueba de normalidad***

H0: Los datos siguen una distribución normal ( $p < 0.05$ )

H1: Los datos no siguen una distribución normal ( $p \geq 0.05$ )

*Tabla 1. Prueba de Kolmogorov-Smirnova*

	Kolmogorov-Smirnov <sup>a</sup>		
	Estadístico	gl	Sig.
GC_DIF	,217	100	0,000

*Fuente: IBM SPSS 25*

Se debe tener en cuenta los criterios de decisión para la prueba de normalidad

1. Si  $p < 0.05$ , entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna.
2. Si  $p \geq 0.05$ , entonces se acepta la hipótesis nula y se rechaza la hipótesis alterna

Decisión

Como se muestra en la tabla los valores son menores a 0.05 por lo tanto esto indica que los datos no siguen una distribución normal, entonces se llevará a cabo **la prueba de normalidad Wilcoxon**

***Prueba de hipótesis***

H0: La aplicación de la norma ISO 27032 no incrementa en grado de conocimiento de los usuarios de los Marketplace de Facebook.

H1: La aplicación de la norma ISO 27032 sí incrementa en grado de conocimiento de los usuarios de los Marketplace de Facebook.

Tabla 2. Prueba de normalidad de Wilcoxon.

<b>PRUEBA DE WILCOXON</b>	
	DESPUES - ANTES
Z	-6,705 <sup>b</sup>
Sig. asintótica(bilateral)	0,000

Fuente: IBM SPSS 25

Se debe tener en cuenta los criterios de decisión para la prueba de normalidad

1. Si  $p < 0.05$ , entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna.
2. Si  $p \geq 0.05$ , entonces se acepta la hipótesis nula y se rechaza la hipótesis alterna

Decisión

Como se evidencia en la tabla los valores son menores a 0.05 (significancia), por lo tanto, existe suficiente evidencia estadística para afirmar que La aplicación de la norma ISO 27032 incrementa en grado de conocimiento de los usuarios de los Marketplace de Facebook.

## **V. DISCUSIÓN**

En primer lugar, la implementación de la norma ISO 27032 y la capacitación de los usuarios ha tenido un impacto positivo en la seguridad de la información en los Marketplace de Facebook. Sin embargo, todavía hay áreas que necesitan mejoras, como el cumplimiento de las políticas de seguridad, la frecuencia y el tipo de incidentes de seguridad, y el nivel de conocimiento de los usuarios.

Respecto al nivel de conocimiento de los usuarios, se observó que éste mejoró en un margen del 20%, lo cual indica una respuesta favorable a la capacitación en seguridad de la información. Sin embargo, aún existen usuarios que no poseen un nivel óptimo de conocimiento sobre el tema, por lo que se recomienda la continuación de estas actividades de capacitación de manera periódica.

En cuanto al nivel de cumplimiento de las políticas de seguridad, se evidenció una mejora significativa, pero aún existen ciertos incumplimientos. Por lo tanto, se recomienda la revisión constante y la implementación efectiva de estas políticas, así como la realización de controles y auditorías periódicas.

En relación a la frecuencia y tipo de incidentes de seguridad de la información, se observó una disminución en la cantidad de incidentes reportados, lo que indica una mejora en este aspecto. Sin embargo, se registraron aún ciertos tipos de incidentes como el phishing y el robo de datos personales, los cuales requieren de una mayor atención para su prevención y detección.

En resumen, la aplicación de la norma ISO 27032 y la capacitación de los usuarios han tenido un impacto positivo en la seguridad de la información en los Marketplace de Facebook. Sin embargo, aún existen aspectos a mejorar en cuanto al conocimiento de los usuarios, el cumplimiento de las políticas de seguridad, y la prevención de ciertos tipos de incidentes. Por lo tanto, se recomienda continuar con estas actividades de mejora y seguimiento de manera constante y periódica.

## VI. CONCLUSIONES

1. Para el indicador 1 “Nivel de conocimiento de los usuarios”, Los resultados de las encuestas aplicadas antes y después de la aplicación de la norma ISO 27032, por parte de los usuarios indican una mejora en el nivel de conocimiento en cuanto a la seguridad de la información. Sin embargo, se requiere de una constante actualización y mejora en la capacitación para garantizar que los usuarios estén al tanto de las últimas amenazas y soluciones de seguridad de la información.
2. Para el indicador 2 “Nivel de cumplimiento de las políticas de seguridad”, se obtuvo previa y posteriormente de la implementación de la norma ISO 27032 y la capacitación de los usuarios, una mejora en el cumplimiento de las políticas de seguridad por parte de Facebook y sus usuarios, de acuerdo con los resultados obtenidos mediante la ficha de observación. Sin embargo, se han identificado ciertos incumplimientos puntuales. Por lo tanto, se recomienda a la administración de Facebook continuar con la revisión y mejora constante de las políticas de seguridad, y fomentar una cultura de seguridad de la información entre los usuarios. Además, se sugiere realizar controles y auditorías regulares para asegurar un cumplimiento efectivo de las políticas de seguridad.
3. Para el indicador 3 “Frecuencia de incidentes de seguridad de la información”, aunque Facebook ya ha implementado medidas de seguridad y hayamos capacitado a los usuarios, se han registrado ciertos incidentes de seguridad. Es muy importante continuar con la monitorización de los Marketplace de Facebook para identificar cualquier posible vulnerabilidad y poder actuar de manera inmediata.
4. Para el indicador 4 “Tipo de incidentes de seguridad de la información”, Los incidentes de seguridad registrados en los Marketplace de Facebook han sido principalmente ataques de phishing y fraudes o estafas. Por lo tanto, se recomienda a la administración de Facebook mejorar las medidas de seguridad para prevenir y detectar estos tipos de amenazas, así como educar a los usuarios sobre cómo identificar y evitar estas situaciones.

5. Para el caso de los 4 indicadores anteriores, es importante destacar que la seguridad de la información es un tema en constante evolución y, por lo tanto, se requiere de una constante actualización y mejora en las políticas, capacitaciones y medidas de seguridad para garantizar la protección de los usuarios y sus datos en los Marketplace de Facebook.

## **VII. RECOMENDACIONES**

A los usuarios de Marketplace:

Es fundamental que los usuarios de los Marketplace de Facebook tomen medidas para proteger su información personal y sensible. Para ello, se recomienda que utilicen contraseñas seguras y las cambien periódicamente, eviten compartir información personal y sensible en la plataforma, utilicen herramientas de cifrado para proteger información sensible, eviten conectarse a redes Wi-Fi públicas para acceder a la plataforma y actualicen regularmente el software de seguridad en dispositivos y sistemas utilizados para acceder a la plataforma.

A los administradores de los Marketplace de Facebook:

Los administradores de los Marketplace de Facebook deben establecer políticas de seguridad de la información para los usuarios de la plataforma, incluyendo medidas de seguridad para el acceso y manejo de información sensible. Se recomienda que se realicen pruebas de seguridad de la plataforma de forma regular para detectar posibles vulnerabilidades y se tomen medidas preventivas. También es importante que los administradores mantengan actualizado el software de seguridad de los servidores y sistemas de la plataforma para garantizar su óptimo funcionamiento.

A la plataforma:

Para mejorar la seguridad en los Marketplace de Facebook, se recomienda a la empresa fortalecer los mecanismos de seguridad en la plataforma mediante la aplicación de estándares internacionales de seguridad de la información, como la norma ISO 27032. Además, es importante que la empresa en este caso Meta (Facebook) establezca procedimientos de seguridad de la información y políticas para los usuarios y administradores de la plataforma, por último, continuar con la capacitación y concientización de los usuarios de los Marketplace de Facebook sobre la norma ISO 27032 y la seguridad de la información. Para poder lograr esto, está la sugerencia de una

creación de campañas de concientización, la constante capacitación de los usuarios, y la realización de evaluaciones periódicas para medir la efectividad de las capacitaciones y el nivel de conocimiento.

## REFERENCIAS

- "Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias"*. **Guerra, Erick, y otros. 2021.** 5, Barranquilla : Dpto. de Ciencias de la computación y electrónica, Universidad de la costa, 2021, Vol. 35.
- "Facebook y vida cotidiana"*. **Aspani, Susana. 2012.** 27, Ciudad de Mexico : Universidad Iberoamericana, 2012, Vol. 16.
- "International and national standards on societal information security"*. **Lykhova, Sofiia, Servatiuk, Liudmyla y Shamsutdinov, Oleksandr. 2022.** 38, BOGOTÁ : ESMIC, 2022, Vol. 20.
- "Políticas y Seguridad de la Información"*. **Vega Velasco, Walter. 2008.** 2, La Paz : s.n., 2008, Vol. 2.
- "Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá"*. **Estrada Esponda, Royer David, Unás Gómez, José Luis y Flórez Rincón, Oleskyenio Enrique. 2021.** 3, Bogotá : Juan Aparicio Barrera, 2021, Vol. 13.
- Garcia-Cervigón Hurtado, Alfonso y Alegre Ramos, Maria del Pilar. 2011.** *"Seguridad Informática"*. Madrid : Paraninfo, 2011.
- Guzmán Solano, Sandra Liliana. 2019.** *Guía para la implementación de la norma ISO 27032.* BOGOTÁ : UNIVERSIDAD CATÓLICA DE COLOMBIA, 2019.
- ISO. 2012.** iso.org. [En línea] 2012.
- Limache Ynquilla, Anuar Mauro. 2022.** *"Aplicación de la norma internacional ISO 27035:2016 para la gestión de incidentes de seguridad de la información en la Empresa LISERME S.R.L., Arequipa 2022"*. Trujillo : UCV, 2022.

**Migone Arosena, Eduardo Antonio. 2017.** *“El e-commerce y su relación con la satisfacción del cliente de los microempresarios San Martín de Porres, 2017”*. Lima : s.n., 2017.

**Orihuela Quivaqui, Axel Igor. 2022.** *“Programa de seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima”*. Lima : PUCP, 2022.

**Pardo Puentes, Germán Andrés y Ramírez Osorio, Daniela Fernanda. 2022.** *“Aspectos jurídicos relevantes sobre los Marketplaces en Colombia”*. Medellín : EAFIT, 2022.

*Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera.* **Apaza Chávez, Wilmer Aufredy. 2021.** 2, Trujillo : La Salle, 2021, Vol. 2.

**Rangel Medina, Harold Alexey. 2020.** *“Implementación norma ISO/IEC 27032:2020 “Tecnologías de la información – Técnicas de seguridad – Directrices para la ciberseguridad” en la empresa Sistemas y Computadores S.A.”*. s.l. : UTS, 2020.

**Saavedra Agudelo, Jorge Emilio. 2020.** *“Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A; basados en los estándares NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032.”*. Tunja : s.n., 2020.

## ANEXOS

### Anexo 1. Matriz de consistencia de la investigación

Título: Aplicación de la Norma internacional ISO 27032 para la Seguridad la información en los Marketplace de Facebook, Cusco 2022

Autor(es): Rojas Moreano Jhonatan Jordy

Problema	Objetivo	Hipótesis	Variable
<p>General:</p> <p>¿De qué manera la aplicación de la Norma internacional ISO 27032 influye en la Seguridad de la Información en los Marketplace de Facebook, Cusco 2022?</p>	<p>General:</p> <p>Identificar de qué manera la aplicación de la Norma internacional ISO 27032 influye en la Seguridad de la Información en los Marketplace de Facebook, Cusco 2022.</p>	<p>Alternativa (H<sub>a</sub>):</p> <p>“la aplicación de la norma ISO 27032 sí mejora de forma significativa la seguridad de la información en los Marketplace de Facebook en la ciudad. de Cusco en el año 2022.”</p>	<p>Independiente:</p> <p>Aplicación de la Norma internacional ISO 27032</p>
<p>Específicos:</p> <ol style="list-style-type: none"> <li>1. Se cuenta con insuficiente capacitación de los usuarios en los Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información.</li> <li>2. Se cuenta con un grado de incumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco.</li> <li>3. Se cuenta con vulnerabilidades de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco.</li> </ol>	<p>Específicos:</p> <ol style="list-style-type: none"> <li>1. Determinar el grado de capacitación de los usuarios en los Marketplace de Facebook en el distrito de Cusco sobre las mejores prácticas de seguridad de la información</li> <li>2. Evaluar el grado de cumplimiento de la norma ISO 27032 en la gestión de la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco</li> <li>3. Analizar los riesgos de seguridad de la información a los que están expuestos los usuarios de los Marketplace de Facebook en el distrito de Cusco</li> </ol>	<p>Nula (H<sub>0</sub>):</p> <p>“la aplicación de la norma ISO 27032 no mejora de forma significativa la seguridad de la información en los Marketplace de Facebook en la ciudad. de Cusco en el año 2022.”</p>	<p>Dependiente:</p> <p>Seguridad la información</p>

Metodología			
<p>Tipo de investigación: Aplicada</p>	<p>Población (N):</p> <p style="text-align: center;"><math>N = x</math></p>	<p>Técnicas de recolección de datos:</p> <ul style="list-style-type: none"> <li>● Observación</li> <li>● Encuesta</li> </ul>	<p>Método de análisis de datos:</p> <ul style="list-style-type: none"> <li>● Estadística descriptiva</li> <li>● Estadística inferencial</li> <li>● Deductivo (enfoque cuantitativo)</li> </ul>
<p>Diseño de investigación: Preexperimental</p>	<p>Muestra (n):</p> <p style="text-align: center;"><math>n = 200</math></p>	<p>Instrumentos de recolección de datos:</p> <ul style="list-style-type: none"> <li>● Ficha de observación</li> <li>● Cuestionario</li> </ul>	<p>Aspectos éticos:</p> <p>Se respetará el derecho a la propiedad intelectual (Originalidad de la investigación - Reporte Turnitin).</p> <p>Se tomará en cuenta el Código de ética vigente de la Universidad César Vallejo.</p> <p>Adicionalmente, se usará para la redacción de la investigación el Sistema de Normas ISO 690.</p>

## Anexo 2. Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Aplicación de la Norma internacional ISO 27032	“Esta norma define los problemas de ciberseguridad que se originan por la falta de coordinación entre los diferentes dominios de seguridad en este ámbito. Esta norma proporciona una guía técnica para hacer frente a los riesgos de ciberseguridad más comunes” (ISO, 2012).	Para medir la aplicación de la norma ISO 27032, se pueden utilizar herramientas de análisis y evaluación de riesgos, permitiendo así identificar los riesgos de seguridad de la plataforma y evaluar el impacto y la probabilidad de ocurrencia de cada riesgo. Con esta información, se pueden tomar medidas de seguridad adecuadas para mitigar los riesgos identificados y mejorar la aplicación de la norma.	Grado de conocimiento y comprensión de la norma ISO 27032.	Comprensión	Ordinal
				Conocimiento	Ordinal
				Aplicación	Ordinal
			controles y medidas de seguridad implementadas	Cumplimiento	Ordinal
				Implementación	Ordinal
Dependiente: Seguridad la información	“Protección de la información incluye la preservación de su confidencialidad, integridad y disponibilidad, y puede también involucrar otras características como la autenticidad, la rendición de cuentas, el no repudio y la fiabilidad” (ISO, 2012).	Para medir la seguridad de la información en un Marketplace de Facebook se puede revisar las políticas de privacidad y seguridad de Facebook y del Marketplace, verificar la reputación de los vendedores, verificar el nivel de uso del Marketplace, evitar compartir información personal y financiera innecesaria, y estar alerta a posibles estafas.	Capacitación de los usuarios	Nivel de conocimiento de los usuarios	Ordinal
					Ordinal
			Cumplimiento de la norma ISO 27032	Nivel de cumplimiento de las políticas de seguridad	Ordinal
			Riesgos de seguridad	Frecuencia de incidentes de seguridad de la información	Ordinal
	Tipo de incidentes de seguridad de la información	Ordinal			

## Anexo 5. Validez de los instrumentos de recolección de datos

### Hoja de validación del instrumento

#### I. Datos generales:

Cuestionario

#### II. Instrucciones:

En el siguiente cuadro, para cada ítem del contenido del instrumento que revisa, marque usted con un check (✓) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad, Pertinencia o Relevancia*.

Dimensiones	Claridad <sup>1</sup>		Pertinencia <sup>2</sup>		Relevancia <sup>3</sup>		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Capacitación de los usuarios							
1. ¿Estás familiarizado con las políticas de seguridad de Facebook respecto a los Marketplace?	x		x		x		
2. ¿Crees que los usuarios de los Marketplace de Facebook cumplen con las políticas de seguridad de la plataforma?	x		x		x		
3. ¿Has experimentado alguna vez un incidente de seguridad en tu grupo de Facebook Marketplace?	x		x		x		
4. ¿Crees que Facebook ofrece suficientes herramientas de seguridad para proteger a los compradores y vendedores?	x		x		x		
5. ¿Consideras importante recibir capacitación sobre seguridad de la información al utilizar los Marketplace de Facebook?	x		x		x		
Dimensión 2: Cumplimiento de la norma ISO 27032							
1. ¿Existe una política de seguridad de la información claramente definida y documentada en el Marketplace de Facebook?	x		x		x		
2. ¿Facebook ha identificado la información importante que maneja en su Marketplace y ha evaluado qué tan importante es esa información y cuál es el riesgo de que esa información sea comprometida o robada?		x	x		x		

3. ¿Se han establecido medidas de seguridad adecuadas para la protección de la información importante en el Marketplace de Facebook?	x		x		x		
4. ¿Se han establecido procedimientos de respuesta a incidentes de seguridad de la información?	x		x		x		
5. ¿Se han implementado controles de acceso físico y lógico para garantizar la seguridad de los activos de información?	x		x		x		
6. ¿Se han establecido medidas de seguridad específicas para la protección de los datos personales de los usuarios en el Marketplace de Facebook?	x		x		x		
Dimensión 3: Riesgos de seguridad							
1. ¿Has experimentado alguna vez algún problema de seguridad en Marketplace de Facebook (por ejemplo, fraude, robo de información personal, virus o malware)?	x		x		x		
2. ¿Qué tipo de problemas de seguridad has experimentado en Marketplace de Facebook (fraude, robo de información personal, virus o malware, phishing, Ninguno)?	x		x		x		
3. ¿Has tomado medidas para proteger tu información personal y financiera mientras compras o vendes en Marketplace de Facebook?	x		x		x		
4. ¿Te has capacitado o informado sobre las mejores prácticas de seguridad en Marketplace de Facebook?	x		x		x		
5. ¿Crees que Facebook proporciona suficiente información sobre la seguridad en Marketplace?	x		x		x		

**Nota:** Los ítems fueron tomados de...

<sup>1</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

<sup>2</sup>**Pertinencia:** Si el ítem pertenece a la dimensión.

<sup>3</sup>**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

**Suficiencia**, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

<b>Observaciones:</b> Es suficiente	
<b>Opinión de aplicabilidad</b>	
Aplicable [ X ]                  Aplicable después de corregir [ X ]                  No aplicable [ ]	
<b>Apellidos y nombres del juez evaluador</b>	Agreda Gamboa, Everson David
<b>Especialidad del evaluador</b>	Sistemas de información y comunicaciones
	
<b>DNI:</b> 18161457	Trujillo, 12 de diciembre del 2022

Anexo 7. Tabla de datos

**Pre Prueba**

	P1	P2	P3	P4	P5
1	1	2	1	3	2
2	2	1	3	3	1
3	3	1	1	3	1
4	2	2	2	2	2
5	1	3	2	4	1
6	4	2	2	1	5
7	1	1	3	2	1
8	2	3	2	2	2
9	1	2	3	3	2
10	3	3	1	1	2
11	3	1	1	3	1
12	1	2	1	2	3
13	1	3	2	3	2
14	2	1	1	2	1
15	3	2	1	1	2
16	1	3	3	1	3
17	1	2	1	2	3
18	1	2	1	2	2
19	3	3	3	1	1
20	3	1	3	2	3
21	1	3	3	3	3
22	1	1	3	2	3
23	1	2	2	1	2
24	3	1	3	2	2
25	3	2	3	3	2
26	1	1	2	4	1
27	2	2	1	1	3
28	3	2	3	3	2
29	4	3	1	3	3
30	2	1	1	2	5
31	1	2	3	1	1
32	2	2	1	3	3
33	2	1	1	2	1
34	1	2	3	1	2
35	2	3	3	2	1
36	3	1	2	2	3
37	4	3	1	1	3
38	3	1	1	1	2
39	3	1	1	1	3
40	3	1	1	1	3
41	2	2	1	5	3
42	3	2	2	3	3

43	2	1	2	3	1
44	1	3	3	2	3
45	2	2	3	3	3
46	4	2	1	3	2
47	2	3	1	2	3
48	2	3	1	1	2
49	3	2	3	1	3
50	2	2	2	3	1
51	1	1	1	2	1
52	2	2	3	2	3
53	1	3	3	2	1
54	2	1	3	3	1
55	3	1	3	2	1
56	2	2	2	2	1
57	3	3	1	2	1
58	2	2	3	2	2
59	3	3	2	4	1
60	3	1	3	3	2
61	2	3	1	1	2
62	2	4	2	1	1
63	3	1	1	2	5
64	3	1	2	1	3
65	2	1	2	5	3
66	1	2	2	4	2
67	1	3	2	1	3
68	1	1	2	1	3
69	3	3	2	3	1
70	2	3	2	1	2
71	3	1	1	2	3
72	3	4	1	3	2
73	2	3	2	1	1
74	3	2	2	5	3
75	1	1	2	2	5
76	1	2	3	3	3
77	3	1	1	2	1
78	2	1	3	1	3
79	2	3	2	4	2
80	2	3	3	3	1
81	3	3	2	1	1
82	3	1	1	2	3
83	1	1	2	3	2
84	1	1	1	3	2
85	3	1	3	3	3
86	3	3	3	3	2
87	3	3	2	3	2
88	3	3	3	2	2

89	4	2	3	2	3
90	3	3	2	3	2
91	2	1	3	2	1
92	3	2	2	5	1
93	3	3	1	1	1
94	2	2	1	3	1
95	2	2	2	3	4
96	1	3	1	1	5
97	1	1	2	2	1
98	1	3	3	3	2
99	2	1	3	3	2
100	3	2	3	1	1

**Post Prueba**

	P1	P2	P3	P4	P5
1	1	2	5	3	2
2	2	1	3	3	4
3	3	4	3	3	5
4	2	2	2	2	2
5	1	3	4	4	5
6	4	2	2	4	5
7	1	5	3	2	1
8	2	3	2	4	2
9	1	4	3	3	2
10	3	3	1	5	2
11	3	1	2	3	5
12	1	2	1	2	3
13	1	3	2	3	2
14	2	1	4	2	1
15	3	2	1	1	2
16	1	3	3	1	3
17	4	2	1	2	3
18	1	4	1	4	4
19	3	3	3	1	1
20	3	1	3	2	4
21	1	3	3	3	3
22	1	1	3	2	3
23	1	2	2	4	2
24	3	4	3	2	2
25	3	2	3	3	2
26	1	5	2	4	1
27	2	2	1	1	3
28	3	2	3	3	2
29	4	3	4	3	3
30	2	1	1	2	5
31	1	2	3	4	5

32	2	2	1	3	3
33	2	3	3	2	1
34	1	2	3	2	2
35	2	3	3	2	1
36	3	1	2	2	3
37	4	3	4	1	3
38	3	1	1	4	2
39	3	4	1	1	3
40	3	1	1	1	3
41	2	2	1	5	3
42	3	2	2	3	3
43	2	1	2	3	5
44	4	3	3	2	3
45	2	2	3	3	3
46	4	2	1	3	2
47	2	3	1	4	3
48	2	3	1	4	2
49	3	2	3	1	3
50	2	2	2	3	5
51	3	4	4	2	4
52	2	2	3	2	3
53	4	3	3	2	4
54	2	1	3	3	2
55	3	1	3	2	5
56	2	2	2	2	2
57	3	3	1	2	1
58	2	2	3	2	2
59	3	3	2	4	5
60	3	1	3	3	2
61	2	3	1	4	2
62	2	4	2	1	1
63	3	4	1	4	5
64	3	1	4	1	3
65	2	1	2	5	3
66	1	2	4	4	2
67	1	3	2	1	3
68	1	1	4	4	3
69	3	3	2	3	5
70	2	3	2	4	2
71	3	1	1	2	3
72	3	4	1	3	2
73	4	3	4	3	2
74	3	2	4	5	3
75	1	2	2	2	5
76	4	4	3	3	3
77	3	1	1	4	1

78	4	1	3	1	3
79	2	3	2	4	2
80	4	3	3	3	5
81	3	3	2	1	1
82	3	1	1	2	3
83	1	2	2	3	2
84	2	1	2	3	3
85	3	1	3	3	3
86	3	3	3	3	2
87	3	3	2	3	2
88	3	3	3	2	2
89	4	2	3	2	3
90	3	3	4	3	2
91	2	2	3	2	2
92	3	2	2	5	2
93	3	3	1	4	3
94	2	2	2	3	1
95	2	2	2	3	4
96	1	3	1	1	5
97	2	2	4	4	5
98	1	3	3	3	2
99	2	2	3	3	2
100	3	2	3	4	5

## Anexo 8 - Solución propuesta

La solución propuesta en este trabajo consistió en la implementación de la norma ISO 27032 a través de un manual para usuarios del Marketplace de Facebook, con el objetivo de mejorar la seguridad de la información. El manual fue diseñado para proporcionar a los usuarios de Marketplace una guía detallada y fácil de entender sobre las mejores prácticas de seguridad de la información, incluyendo medidas de protección de datos personales, recomendaciones de contraseñas seguras y procedimientos de denuncia de fraudes y violaciones de seguridad.

La implementación de esta solución se llevó a cabo en dos fases: en primer lugar, se realizó una evaluación de la situación actual de seguridad de la información en el Marketplace de Facebook, con el fin de identificar las principales áreas de mejora. A continuación, se procedió a la elaboración del manual, que fue distribuido entre los usuarios de Marketplace a través de la plataforma de Facebook.

Los resultados obtenidos tras la implementación de esta solución fueron altamente satisfactorios. Se observó una disminución significativa en el número de denuncias por violaciones de seguridad de la información, así como una mayor concienciación por parte de los usuarios acerca de la importancia de proteger su información personal. En conclusión, la implementación de la norma ISO 27032 a través de un manual para usuarios del Marketplace de Facebook se reveló como una solución efectiva y accesible para mejorar la seguridad de la información en esta plataforma de comercio electrónico.



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

### **Declaratoria de Autenticidad del Asesor**

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "Aplicación de la Norma internacional ISO 27032 para la Seguridad de la información en los Marketplace de Facebook, Cusco 2023", cuyo autor es ROJAS MOREANO JHONATAN JORDY, constato que la investigación tiene un índice de similitud de 30.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 22 de Febrero del 2023

<b>Apellidos y Nombres del Asesor:</b>	<b>Firma</b>
AGREDA GAMBOA EVERSON DAVID <b>DNI:</b> 18161457 <b>ORCID:</b> 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 27-03- 2023 08:58:34

Código documento Trilce: TRI - 0534647