ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.1050

Analysis of the Impact on E-commerce Security in SMEs: A Systematic Literature Review

Chaupi Alvarez Yoni Willian, Estudiante[1], Alejandría Vallejos Patricia Abigail, Magister[2]
[1,2]Facultad de Ingeniería Universidad Tecnológica del Perú, Perú, u20300200@utp.edu.pe[1], C24236@utp.edu.pe[2]

Abstract* – The security in e-commerce for small and medium-sized enterprises (SMEs) is crucial as it has gained significance across all businesses. An analysis was conducted to mitigate risks in online transactions, aiming to bolster the trust of end-users and promote a much safer digital economic environment. A systematic literature review was carried out using the PRISMA method and the PICO structure. Keywords were selected from the UNESCO Thesaurus, and inclusion standards were applied for academic articles structured under the IMRD format, published between 2021 and 2023 in both Spanish and English languages. Databases such as Scopus, ScienceDirect, and Google Scholar were utilized with specific search strategies. Ten relevant articles were identified. The results highlighted effective security measures such as data encryption (30%), followed by technological criteria and digital forensics. The primary technologies were data tokenization (50%) and digital certificates (10%). Customer trust was considered in the majority of studies (90%), but discrepancies in its importance were found. Surveys were the predominant technique for studying SME behavior (70%). In conclusion, data encryption stands out as the primary security measure, followed by tokenization and digital certificates. Surveys were fundamental in understanding SME behavior. Exploring additional research methods and addressing discrepancies in the perception of customer trust importance is suggested to develop strategies more aligned with end-users' expectations.

***Keywords* – E-Commerce; Technological Innovation; Information Society; Online Commerce; Business Administration, Security.**

Análisis del Impacto en la Seguridad del Comercio Electrónico en las PYMEs: Una Revisión Sistemática de la Literatura

Chaupi Alvarez Yoni Willian, Estudiante[1], Alejandría Vallejos Patricia Abigail, Magister[2]
[1,2]Facultad de Ingeniería Universidad Tecnológica del Perú, Perú, u20300200@utp.edu.pe[1], C24236@utp.edu.pe[2]

Resumen* – La seguridad en el comercio electrónico de las PYMES es fundamental porque ha cobrado importancia en todos los negocios, por ello se hizo el análisis para mitigar los riesgos en las transacciones por internet y así fortalecer la confianza de los usuarios finales, promoviendo un entorno económico digital mucho más seguro. Se llevó a cabo una revisión sistemática de la literatura empleando el método PRISMA y la estructura PICO. Se seleccionaron palabras clave del Tesauro de la UNESCO y se aplicaron estándares de inclusión para artículos académicos estructurados bajo el formato IMRD, publicados entre los años 2021 y 2023 en idiomas castellano e inglés. Se utilizaron bases de datos como Scopus, ScienceDirect y Google Académico con estrategias de búsqueda específicas. Se identificaron 10 artículos pertinentes. En los resultados se destacaron medidas efectivas de seguridad como la encriptación de datos (30%), seguida de criterios tecnológicos y forense digital. Las tecnologías principales fueron la tokenización de datos (50%) y los certificados digitales (10%). La confianza del cliente fue considerada en la mayoría de los estudios (90%), pero se hallaron discrepancias en su importancia. La encuesta fue la técnica predominante para el estudio del comportamiento de las PYMEs (70%). En conclusión, la encriptación de datos se destaca como la medida de seguridad primordial, seguida por la tokenización y los certificados digitales. Las encuestas fueron fundamentales para comprender el comportamiento de las PYMEs. Se sugiere explorar métodos adicionales de investigación y abordar las discrepancias en la percepción de la importancia de la confianza del cliente para desarrollar estrategias más alineadas con las expectativas de los usuarios finales.

Palabras Clave* – *Comercio Electrónico; Innovación tecnológica; Sociedad de la información; Comercio en línea; Administración de empresas, Seguridad.

I. Introducción

En los últimos cuatro años, el comercio electrónico ha demostrado un rápido crecimiento, en parte debido a la pandemia de COVID-19 [1], [2]. Según Shao, D., Mwangakala, H., Ishengoma, F., Mongi, H., Mambile, C. y Chali, F., la pandemia tuvo un impacto diverso en las organizaciones, lo que ha llevado a la adopción de nuevos enfoques empresariales, incluyendo el uso de tecnologías digitales [2]. Este hecho ha transformado radicalmente la forma en que los usuarios interactúan con el mercado global, revolucionando no solo la forma en que se adquieren productos y servicios sino también creando una interconexión en el mundo empresarial, particularmente para las pequeñas y medianas empresas (PYMEs). Esto ha llevado a un crecimiento y desarrollo económico constante.

Sin embargo, este crecimiento también ha traído consigo un desafío crítico, la seguridad de la información personal y financiera de todos los usuarios en el comercio electrónico [3].

En la Ref. [4] Saeed S. señala asegurar que la seguridad de las aplicaciones de comercio electrónico cumple un rol muy importante en la gestión de la base de clientes. Actualmente, con el uso cada vez mayor de herramientas digitales, también ha aumentado el riesgo de filtraciones de datos y ciberataques. Según la Ref. [5] Rahayu S, Aslah S, Sembok T, Isa M. señala que la mayoría de las PYMEs representan el 99.7% del mercado, 28 millones de PYMEs en Estados Unidos y 5,2 millones en Reino Unido.

En consecuencia, el índice de inseguridad se incrementó debido al gran tamaño del mercado y el uso del comercio electrónico [6], lo cual ha generado preocupaciones sobre la seguridad de los datos confidenciales, como la información de las tarjetas de crédito y la de identificación personal, que a menudo se requieren para las transacciones en línea.

En este contexto, es fundamental abordar el tema de la protección de información en la economía digital. Un marco sólido de protección de datos puede fomentar la confianza de los consumidores e incentivar la inversión, la competencia y la mejora en la economía digital. La protección de datos puede mitigar los riesgos financieros, fomentar la confianza entre empresas y consumidores y promover ecosistemas económicos confiables y transparentes que defiendan los valores democráticos. Por lo tanto, es importante investigar las técnicas eficientes y óptimas para la seguridad de los datos, como la integración de la inteligencia artificial (IA) en seguridad de datos y el uso de cripto-stegano en el comercio electrónico, como lo proponen Kumbhakar, Sanyal y Ka forma [7].

El objetivo de la presente investigación es analizar el impacto en la seguridad del comercio electrónico en las PYMEs para mitigar los riesgos que existen en las transacciones en línea, con el fin de fortalecer la confianza de los usuarios y promover un entorno económico digital más seguro, en respuesta al crecimiento constante del comercio electrónico y los incidentes relacionados a la protección de información confidencial.

II. METODOLOGÍA

La metodología utilizada en la presente investigación fue la revisión sistemática de la literatura. Esta metodología se enfoca en la indagación, recolección, evaluación y síntesis de la evidencia de manera sistemática, con el propósito de generar una conclusión precisa y objetiva acerca de un tema específico. De la misma manera la estructura de este trabajo se ajustó al método PRISMA.

La pregunta que se planteó para la investigación fue: ¿Cuáles son las medidas de seguridad más efectivas para proteger los datos confidenciales del usuario en el comercio electrónico de las PYMEs, considerando la seguridad en su entorno? La pregunta fue formulada bajo la estructura PICO.

Las palabras clave empleadas se encontraron en el Tesauro de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). A partir de la pregunta de investigación se definieron las siguientes palabras claves: "PMES", "SME", "protection features", "preventive measure", "security measure", "remedial action", "Technological innovations", "Information revolution", "Electronic commerce", "extensive protection for confidential information", "confidential data", "access to confidential data", "e-commerce", "ecommerce", "electronic trade", "electronic trading platform", "e-commerce VAT fraud".

Los estándares para incluir los artículos seleccionados fueron: Análisis de enfoque de la seguridad en el comercio electrónico en las PYMEs, artículos académicos estructurados bajo el formato IMRD y publicados entre los años 2021 y 2023, en idiomas castellano e inglés. Los artículos excluidos estuvieron relacionados con plataformas subyacentes del sistema de comercio electrónico, no se consideró los estudios empíricos sobre la preparación de las PYMEs en la construcción, tampoco se consideró ponencias de conferencias, reseñas de conferencias, capítulos de libro y reseñas.

Los motores de búsqueda utilizadas fueron: Scopus, ScienceDirect y Google académico. Las estrategias de búsqueda empleadas fueron las siguientes:

Scopus

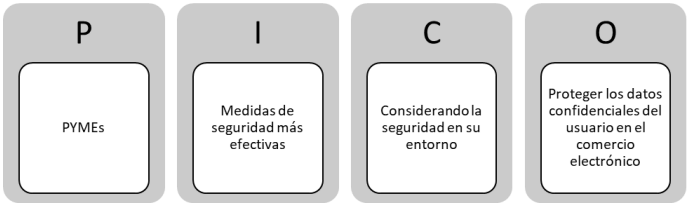
"extensive protection for confidential information" OR "confidential data" OR "access confidential data" OR e-commerce OR ecommerce OR "electronic trade" OR "electronic trading platform" OR "e-commerce VAT fraud"

ScienceDirect

("PMES" OR "SME") AND ("protection features" OR "preventive measure" OR "security measure" OR "remedial action") AND ("Technological innovations" OR "Information revolution" OR "Electronic commerce")

Google Académico

("PMES" OR "SME") AND ("Electronic commerce") AND ("security")



RQ: ¿Cuáles son las medidas de seguridad más efectivas para proteger los datos confidenciales del usuario en el comercio electrónico de las PYMEs, considerando la seguridad en su entorno?

RQ1: ¿Cuál es el comportamiento de las PYMEs?

RQ2: ¿Cuáles son las medidas de seguridad más efectivas que pueden implementar las PYMEs?

RQ3: ¿Cómo ha evolucionado la seguridad en el comercio electrónico en los últimos años?

RQ4: ¿Cuál es la importancia de proteger los datos confidenciales de los usuarios?

TABLA I
TABLA DE PALABRAS CLAVE

P	**Problema / Población**	PYMEs	PMES, SME
I	**Intervención**	Medidas de seguridad más efectivas	protection features, preventive measure, security measure, remedial action
C	**Comparación**	Considerando la seguridad en su entorno	Technological innovations, Information revolution, Electronic commerce
O	**Resultados**	Proteger los datos confidenciales del usuario en el comercio electrónico	extensive protection for confidential information, confidential data, access to confidential data, e-commerce, ecommerce, electronic trade, electronic trading platform, e-commerce VAT fraud

TABLA II
TABLA DE ECUACIÓN DE BÚSQUEDA

P	**Problema / Población**	PYMEs	"PMES" OR "SME"
I	**Intervención**	Medidas de seguridad más efectivas	"protection features" OR "preventive measure" OR "security measure" OR "remedial action"
C	**Comparación**	Considerando la seguridad en su entorno	"Technological innovations" OR "Information revolution" OR "Electronic commerce"
O	**Resultados**	Proteger los datos confidenciales del usuario en el comercio electrónico	"extensive protection for confidential information" OR "confidential data" OR "access confidential data" OR e-commerce OR ecommerce OR "electronic trade" OR "electronic trading platform" OR "e-commerce VAT fraud"

TABLA III
SECUENCIA PARA LA BÚSQUEDA Y EXTRACCIÓN DE INFORMACIÓN

Pautas	Descripción	Criterios
1. Selección de palabras clave	Se identificaron palabras clave para la búsqueda de artículos	extensive protection for confidential information, confidential data, access to confidential data, e-commerce, ecommerce, electronic trade, electronic trading platform, e-commerce VAT fraud
2. Selección de plataformas de información	Se utilizaron bases de datos de acceso gratuito y educativo	Scopus, ScienceDirect, y Google académico.
3. Selección de investigaciones tomando en cuenta los criterios de inclusión y exclusión	Los artículos filtrados concuerdan con los criterios de inclusión y exclusión definidos	**Criterios de inclusión** - Análisis de enfoque de la seguridad en el comercio electrónico. - En las PYMEs - Artículos académicos siguiendo la estructura IMRD. - Rango de años de estudio entre 2021 y 2023. - Idiomas castellano e inglés. - Plataformas de información de acceso gratuito: Scopus, ScienceDirect y Google académico.
		Criterios de exclusión - Investigaciones que no estén relacionadas específicamente en el entorno de las PYMEs y la seguridad en el comercio electrónico. - Publicaciones que no sean relevantes para el análisis de las PYMEs en el período de 2021 a 2023. - Publicaciones duplicadas, es decir, aquellas que se encuentren repetidas.
4. Análisis de los estudios	Expresado en tablas y figuras	

DIAGRAMA DE FUJO DE PRISMA

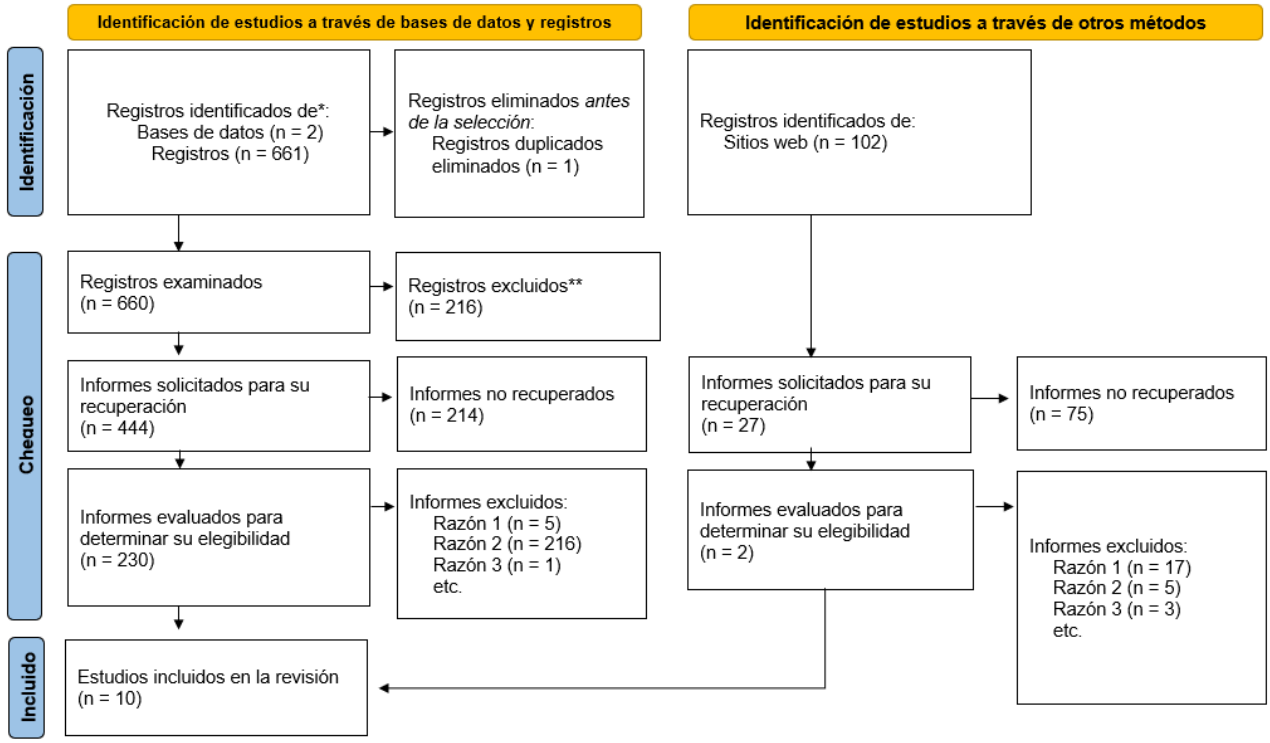


Fig. 1 Resumen de selección de artículos.

III. RESULTADOS

Al emplear las tácticas de búsqueda se obtuvo una cantidad total de 661 artículos originales publicados entre el año 2000 al año 2023, los cuales fueron seleccionados de las bases de datos utilizadas. Tomando como base dicha búsqueda identificamos un artículo duplicado. Después de haber aplicado los criterios de exclusión se identificaron 10 artículos estrechamente relacionados con el tema de "Análisis del Impacto en la Seguridad del Comercio Electrónico en las PYMEs".

TABLA IV
RESUMEN DE BÚSQUEDAS DE ARTÍCULOS DE INFORMACIÓN ACADÉMICA

Motores de búsqueda	Subtotal
Scopus	5
ScienceDirect	3
Google Académico	2
Total	**10**

Los 10 artículos extraídos se ordenaron cronológicamente partiendo desde el más antiguo tal como se puede apreciar en la tabla V.

TABLA V
CANTIDAD DE PUBLICACIONES POR AÑO

Año	Cantidad	%
2021	1	10%
2022	2	20%
2023	7	70%
Total	**10**	**100%**

Las tácticas empleadas para la estructuración de búsqueda de la información se pueden apreciar en la tabla VI.

TABLA VI
TÁCTICAS EMPLEADAS PARA LA ELABORACIÓN DE LA REVISIÓN SISTEMÁTICA

Proceso	Método
Estructurar la pregunta de investigación	Método PICO
Verificar la estructuración y el desarrollo de la revisión sistemática	Método PRISMA
Recopilación de artículos científicos	Búsqueda en bases de datos

TABLA VII
MATRIZ DE REGISTRO DE ARTÍCULOS

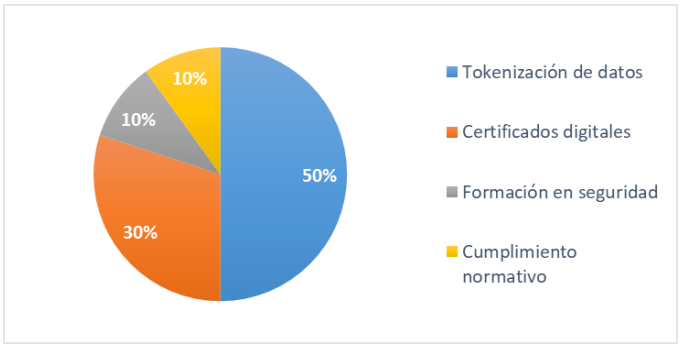
Título del artículo	Año	Lugar de procedencia	Comercio Electrónico / Seguridad	Idea principal
The Relationship between the Frequency of Technology Use and Electronic Commerce Adoption among Small and Medium-Sized Enterprises in Kuwait	2022	Malasia	Adopción del comercio electrónico	El propósito de esta investigación es analizar los factores que influyen en la incorporación de las pequeñas y medianas empresas al uso del comercio electrónico [8].
How Can SMEs Boost Trust Through Third-Party Means? Tracing the Multi-Dimensional Institutional Basis of Online Trust	2022	China	Confianza en el comercio electrónico	El objetivo del estudio es explorar cómo la confianza en las plataformas en línea se desarrolla según los servicios de terceros y cómo esto afecta las intenciones de compra en línea de los consumidores [9].
E-Commerce Technologies Adoption Strategy Selection in Indonesian SMEs Using the Decision-Makers, Technological, Organizational and Environmental (DTOE) Framework	2023	China	Ventajas competitivas de la adopción del comercio electrónico	El propósito de este estudio es examinar los criterios que afectan la adopción del comercio electrónico por parte de las pequeñas y medianas empresas [10].
E-commerce adoption within SME's in Ghana, a tool for growth?	2021	Ghana	Competitividad dentro del comercio electrónico	El comercio electrónico ofrece a las pequeñas y medianas empresas (PYME) de las economías en desarrollo la oportunidad de competir en un escenario global [11].
A Customer-Centric View of E-Commerce Security and Privacy	2023	Arabia Saudita	Garantía de aplicaciones de comercio electrónico seguras	En esta investigación se analiza los resultados de un estudio empírico de clientes de comercio electrónico realizado para conocer su forma de pensar sobre el uso de aplicaciones de comercio electrónico [12].
An optimal and efficient data security technique through crypto-stegano for E-commerce	2023	India	Seguridad de datos en el comercio electrónico	En este trabajo se ha propuesto una seguridad de datos óptima y eficiente con la combinación del criptosistema Elgamal y la técnica de esteganografía de imágenes LSB para el comercio electrónico.
A systematic literature review on the factors influencing e-commerce adoption in developing countries	2023	China	Seguridad de los servicios de pago en línea	El propósito de esta investigación es entender los elementos que impactan en la implementación del comercio electrónico en países en desarrollo, empleando un método de revisión sistemática de fuentes literarias [13].
Online Buyers and Open Innovation: Security, Experience, and Satisfaction	2021	México	Seguridad, experiencia y satisfacción	Este artículo aborda los retos y las posibilidades que presentan los compradores en internet, tales como el diseño, la seguridad, la confianza, el riesgo, la incertidumbre y la satisfacción relacionada con las adquisiciones en línea en el ámbito del comercio electrónico [14].
Mechanisms and techniques to enhance the security of big data analytic framework with MongoDB and Linux Containers	2022	Estados Unidos	Técnicas para mejorar la seguridad	Este documento propone e implementa algunos mecanismos y técnicas de seguridad, como autenticación segura, autorización segura y cifrado, para fortalecer la seguridad en el comercio electrónico [15]
Research Framework Of Knowledge Sharing In Collaborative E-Commerce	2023	Kuala	Centro de Ciberseguridad y Revolución Industrial Digital, Defensa Nacional	El enfoque está en relación con la cantidad de PYMEs y la seguridad en el comercio electrónico. Debido al enorme tamaño de mercado los ciberdelincuentes pueden atacar y amenazar la plataforma de negocios en línea desde una gama mucho más amplia [16].
Small businesses and FinTech: a systematic review and future directions	2023	Australia	Pequeñas empresas y FinTech	La naturaleza misma de la tecnología de pago y su complejidad, la compatibilidad con la tecnología y el riesgo con la tecnología influyen en las decisiones de adopción. El tiempo de transacción y la seguridad de la transacción también influyen en la decisión de adopción de las pequeñas empresas [17].

Según el análisis, las medidas de seguridad más efectivas que pueden implementar las PYMES dentro del Comercio Electrónico son la encriptación de datos, seguidamente de los criterios tecnológicos y el análisis forense digital, tienen un impacto significativo en la protección de la información sensible y en la prevención de posibles ataques cibernéticos. Otros estudios, por su parte consideraron que las medidas de seguridad más efectivas son la app Fintech, la infraestructura tecnológica y la tokenización.

Fuente: Elaboración propia

Fig. 2 Las medidas de seguridad más efectivas.

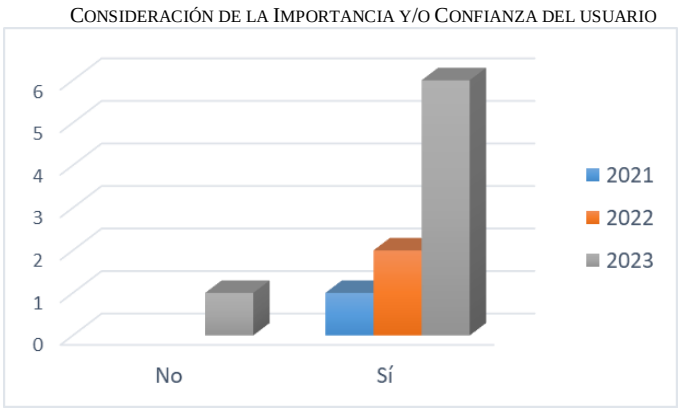
Según el estudio, dentro de las tecnologías destacadas en los 10 artículos, tenemos que 5 destacan la tokenización de datos y 3 destacan los certificados digitales como avance tecnológico para la seguridad en el comercio electrónico. Otros artículos destacan el cumplimiento normativo y la formación en seguridad como avance tecnológico para la seguridad en el comercio electrónico.



Fuente: Elaboración propia

Fig. 3 Las tecnologías más destacadas en el estudio.

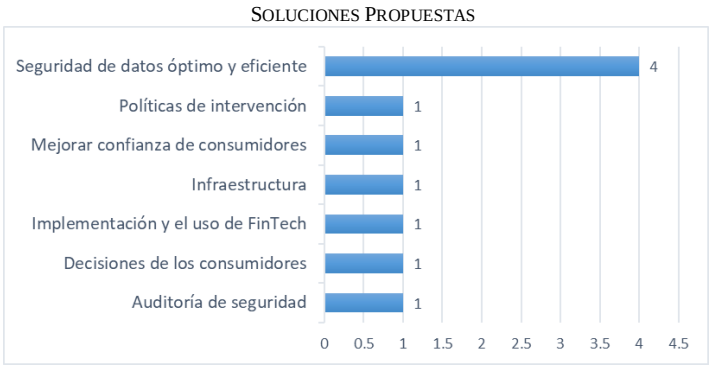
Según el análisis, de un total de 10 artículos revisados, 9 de ellos sí consideran la confianza y la importancia de los clientes en relacionadas con la protección de información confidencial. Sin embargo, en un artículo publicado en 2023 por Kumbhakar D, Sanyal KKarforma S se destaca como una excepción, ya que no atribuye a la importancia o confiabilidad de los usuarios [7].



Fuente: Elaboración propia

Fig. 4 La importancia de considerar la confianza con el usuario.

Según el análisis, los autores han abordado variedad de temas, desde la implementación de tecnología financiera, políticas de intervención hasta la seguridad eficiente de datos y la mejora de la confianza del consumidor. Los trabajos se centran en los años 2022 y 2023, con una dirección particular en la seguridad de información y la optimización. Cada autor ha contribuido con sus investigaciones en áreas específicas relacionadas con estos temas.

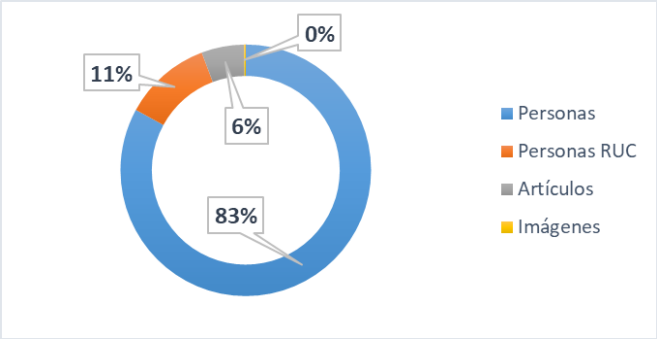


Fuente: Elaboración propia

Fig. 5 Alternativas de solución.

En esta investigación, para analizar el comportamiento de las PYMEs, se tomó una muestra de 1901 (83%), seguidamente por una muestra total de 259 personas jurídicas (PYMEs) (11%), continuando con una muestra total de 126 artículos (6%). Otros estudios tomaron como muestra a 5 imágenes para objeto de estudio del comportamiento de las PYMEs.

TAMAÑO DE MUESTRA POR TIPO DE MUESTRA

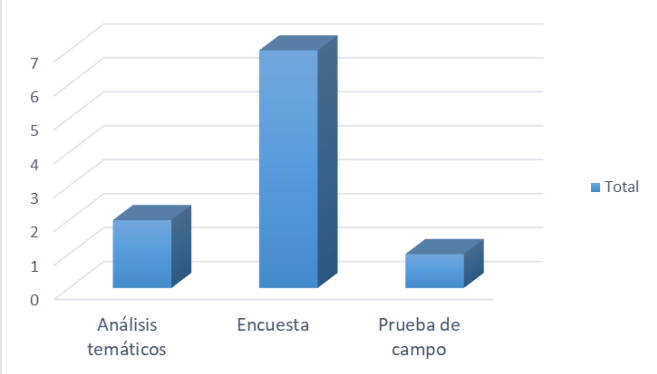


Fuente: Elaboración propia

Fig. 6 Tamaño por tipo de la muestra para el estudio.

Para analizar el comportamiento de las PYMEs en esta investigación, se aplicaron algunas técnicas de estudio a los 10 artículos. Se encontró que 8 utilizaron la encuesta. En otros artículos se utilizaron los análisis temáticos y las pruebas de campo.

TÉCNICAS UTILIZADAS PARA EL ESTUDIO



Fuente: Elaboración propia

Fig. 7 Técnicas utilizadas para el estudio.

IV. DISCUSIÓN

En este estudio de revisión, la medida de seguridad más efectiva que las PYMES pueden implementar dentro del comercio electrónico es la encriptación de datos (30%), lo cual guarda relación con los resultados de los autores [18], [19], [7]. Además, los criterios tecnológicos y el forense digital también son considerados valiosos en el cuidado y/o protección de la información [20], [21], [4], [22].

Sin embargo, los resultados de los autores Llorente-Barroso C, Sánchez-Valle M, Viñarás-Abad M [23], la tokenización de datos representa una cantidad mínima de importancia como medida de seguridad (10%). También se encontró que la tokenización de datos se destaca como un avance tecnológico crucial (50%), a diferencia de los certificados digitales tiene una tendencia baja para salvaguardar la integridad de los datos [23], [18], [19].

En cuanto a las metodologías empleadas, se halló como predominancia el uso de las encuestas para examinar el comportamiento de las PYMES, evidenciando ser la técnica ampliamente empleada en los estudios revisados [23], [18], [19].

Sin embargo, se han empleado análisis temáticos y pruebas de campo en algunos artículos es notable que las encuestas prevalecen como el método preferido en la mayoría de las investigaciones analizadas (70%) [24], [25], [7].

Asimismo, se identificó que la mayoría de las investigaciones analizadas se han focalizado principalmente entre los años 2022 y 2023 (70%), lo cual guarda relación con los temas de interés y enfoque como la seguridad de datos y el fortalecimiento de la confianza del usuario como temas de importancia [24], [23].

Sin embargo, cada estudio ha aportado ideas específicas que influyen en estos temas abordando desde la implementación de tecnologías financieras [24], hasta la formulación de políticas de intervención [23], buscando soluciones que garanticen una seguridad de datos eficiente y óptima. Esto guarda relación con la importancia de implementar medidas de seguridad robustas, así como considerar la confianza del cliente y el uso de tecnologías emergentes [21], como la tokenización de datos y los certificados digitales, para fortalecer la seguridad en el comercio electrónico de las PYMEs [23].

No obstante, se requiere una mayor atención a las discrepancias en las consideraciones sobre la importancia de la confianza del cliente en la protección de datos confidenciales [21], [22]. Además, se sugiere la exploración de otros métodos de investigación para obtener una comprensión más completa del comportamiento de las PYMES en este contexto.

V. CONCLUSIONES

Esta investigación ha identificado con claridad los métodos más eficientes para fortalecer la seguridad en las transacciones realizadas en el comercio electrónico por las PYMES. Como la encriptación de datos, respaldada por múltiples estudios que ha surgido como una medida de seguridad primordial. Asimismo, la tokenización de datos y los certificados digitales han demostrado ser tecnologías destacadas en la defensa de la integridad de la información. En cuanto a la técnica más eficiente para comprender el comportamiento de las PYMES en este ámbito, se ha destacado el uso de las encuestas. Esta técnica ha sido resaltante en la mayoría de los estudios analizados, proporcionando información valiosa sobre las percepciones y prácticas de las PYMEs en el entorno del comercio electrónico.

Para futuros trabajos, se sugiere ampliar la exploración de métodos de investigación complementarios, como análisis cualitativos más detallados, pruebas de campo más extensas, análisis de Big Data o el uso de la inteligencia artificial IA para obtener una comprensión más profunda y holística del comportamiento de las PYMES en relación con la seguridad en el comercio electrónico. Además, se insta a abordar las discrepancias en las percepciones sobre la importancia de la

confianza del cliente en la protección de datos confidenciales, lo cual podría contribuir a desarrollar estrategias más alineadas con las expectativas y necesidades de los usuarios finales.

AGRADECIMIENTO

Queremos expresar nuestro sincero agradecimiento a los docentes del curso por su apoyo continuo y su colaboración esencial en este trabajo. Así como el respaldo constante de quienes hicieron posible este proyecto. Su contribución ha sido fundamental en el desarrollo de esta investigación.

REFERENCIAS

[1] A. Alvarez-Risco, L. Quipuzco-Chicata, y C. Escudero-Cipriani, «Determinants of Online Repurchase Intention in Covid-19 Times: Evidence From an Emerging Economy[Determinantes de la intención de recompra en línea en tiempos de COVID-19: evidencia de una economía emergente]», Lecturas de Economia, n.o 96, pp. 101-143, ene. 2022, doi: 10.17533/udea.le.n96a342638.

[2] D. Shao, H. Mwangakala, F. Ishengoma, H. Mongi, C. Mambile, y F. Chali, «Sustenance of the digital transformations induced by the COVID-19 pandemic response: lessons from Tanzanian public sector», Global Knowledge, Memory and Communication, vol. 72, n.o 6, pp. 700-713, jul. 2023, doi: 10.1108/GKMC-11-2021-0186.

[3] V. Joshi, S. K. Baral, M. Pitke, y R. J. Dwyer, «Retailing and e-commerce riding on technology: Augmented reality and virtual reality», en Augmented and Virtual Reality in Industry 5.0, De Gruyter, 2023, pp. 127-145. doi: 10.1515/9783110790146-006.

[4] S. Saeed, «A Customer-Centric View of E-Commerce Security and Privacy», Applied Sciences (Switzerland), vol. 13, n.o 2, 2023, doi: 10.3390/app13021020.

[5] S. B. Rahayu, S. F. Aslah, T. M. T. Sembok, y M. R. M. Isa, «RESEARCH FRAMEWORK OF KNOWLEDGE SHARING IN COLLABORATIVE E-COMMERCE», jestec.taylors.edu.my, vol. 18, n.o 4, pp. 153-166, 2023, Accedido: 4 de octubre de 2023. [En línea]. Disponible en: https://jestec.taylors.edu.my/Special%20Issue%20ICIST%202022_2/ICIST_2_12.pdf

[6] I. V. Esquivel, «Critical factors of success in the digital trade of the Costa Rican exporting SMES[FACTORES CRÍTICOS DE ÉXITO EN EL COMERCIO DIGITAL DE LAS PYMES EXPORTADORAS COSTARRICENSES]», Tec Empresarial, vol. 13, n.o 1, pp. 19-34, ene. 2019, doi: 10.18845/te.v13i1.4293.

[7] D. Kumbhakar, K. Sanyal, y S. Karforma, «An optimal and efficient data security technique through crypto-stegano for E-commerce», Multimed Tools Appl, vol. 82, n.o 14, pp. 21005-21018, 2023, doi: 10.1007/s11042-023-14526-7.

[8] S. M. Isa y S. Alenezi, «The Relationship between the Frequency of Technology Use and Electronic Commerce Adoption among Small and Medium-Sized Enterprises in Kuwait», Asian Journal of Business and Accounting, vol. 15, n.o 1, pp. 207-241, 2022, doi: 10.22452/ajba.vol15no1.7.

[9] C. Cao y S. Huang, «How Can SMEs Boost Trust Through Third-Party Means? Tracing the Multi-Dimensional Institutional Basis of Online Trust», IEEE Access, vol. 10, pp. 127149-127167, 2022, doi: 10.1109/ACCESS.2022.3226889.

[10] S. A. Bening, M. Dachyar, N. R. Pratama, J. Park, y Y. Chang, «E-Commerce Technologies Adoption Strategy Selection in Indonesian SMEs Using the Decision-Makers, Technological, Organizational and Environmental (DTOE) Framework», Sustainability (Switzerland), vol. 15, n.o 12, 2023, doi: 10.3390/su15129361.

[11] C. A. Sarfo y H. Song, «E-commerce adoption within SME's in Ghana, a tool for growth?», International Journal of Electronic Business, vol. 16, n.o 1, pp. 32-51, 2021, doi: 10.1504/IJEB.2021.112764.

[12] S. Saeed, «A Customer-Centric View of E-Commerce Security and Privacy», Applied Sciences (Switzerland), vol. 13, n.o 2, 2023, doi: 10.3390/app13021020.

[13] S. Hendricks, S. M.-D. and I. Management, y undefined 2023, «A systematic literature review on the factors influencing e-commerce adoption in developing countries», Elsevier, Accedido: 5 de octubre de 2023. [En línea]. Disponible en: https://www.sciencedirect.com/science/article/pii/S2543925123000190

[14] L. E. Valdez-Juárez, D. Gallardo-Vázquez, y E. A. Ramos-Escobar, «Online Buyers and Open Innovation: Security, Experience, and Satisfaction», Journal of Open Innovation: Technology, Market, and Complexity, vol. 7, n.o 1, p. 37, 2021, doi: https://doi.org/10.3390/joitmc7010037.

[15] A. Mailewa, S. Mengel, L. Gittner, y H. Khan, «Mechanisms and techniques to enhance the security of big data analytic framework with MongoDB and Linux Containers», Array, vol. 15, p. 100236, 2022, doi: https://doi.org/10.1016/j.array.2022.100236.

[16] S. B. Rahayu, S. F. Aslah, T. M. T. Sembok, y M. R. M. Isa, «RESEARCH FRAMEWORK OF KNOWLEDGE SHARING IN COLLABORATIVE E-COMMERCE», jestec.taylors.edu.my, vol. 18, n.o 4, pp. 153-166, 2023, Accedido: 5 de octubre de 2023. [En línea]. Disponible en: https://jestec.taylors.edu.my/Special%20Issue%20ICIST%202022_2/ICIST_2_12.pdf

[17] S. Sharma, P. Ilavarasan, S. K.-E. Commerce, y undefined 2023, «Small businesses and FinTech: a systematic review and future directions», Springer, Accedido: 5 de octubre de 2023. [En línea]. Disponible en: https://link.springer.com/article/10.1007/s10660-023-09705-5

[18] W. C. Koh y Y. Z. Seah, «Unintended consumption: The effects of four e-commerce dark patterns», Cleaner and Responsible Consumption, p. 100145, oct. 2023, doi: 10.1016/J.CLRC.2023.100145.

[19] L. E. Valdez-Juárez, D. Gallardo-Vázquez, y E. A. Ramos-Escobar, «Online Buyers and Open Innovation: Security, Experience, and Satisfaction», Journal of Open Innovation: Technology, Market, and Complexity, vol. 7, n.o 1, p. 37, 2021, doi: https://doi.org/10.3390/joitmc7010037.

[20] S. A. Bening, M. Dachyar, N. R. Pratama, J. Park, y Y. Chang, «E-Commerce Technologies Adoption Strategy Selection in Indonesian SMEs Using the Decision-Makers, Technological, Organizational and Environmental (DTOE) Framework», Sustainability (Switzerland), vol. 15, n.o 12, 2023, doi: 10.3390/su15129361.

[21] S. M. Isa y S. Alenezi, «The Relationship between the Frequency of Technology Use and Electronic Commerce Adoption among Small and Medium-Sized Enterprises in Kuwait», Asian Journal of Business and Accounting, vol. 15, n.o 1, pp. 207-241, 2022, doi: 10.22452/ajba.vol15no1.7.

[22] C. Cao y S. Huang, «How Can SMEs Boost Trust Through Third-Party Means? Tracing the Multi-Dimensional Institutional Basis of Online Trust», IEEE Access, vol. 10, pp. 127149-127167, 2022, doi: 10.1109/ACCESS.2022.3226889.

[23] C. Llorente-Barroso, M. Sánchez-Valle, y M. Viñarás-Abad, «The role of the Internet in later life autonomy: Silver surfers in Spain», Humanit Soc Sci Commun, vol. 10, n.o 1, p. 56, dic. 2023, doi: 10.1057/s41599-023-01536-x.

[24] S. K. Sharma, P. V. Ilavarasan, y S. Karanasios, «Small businesses and FinTech: a systematic review and future directions», Electronic Commerce Research, 2023, doi: 10.1007/S10660-023-09705-5.

[25] S. Hendricks y S. D. Mwapwele, «A systematic literature review on the factors influencing e-commerce adoption in developing countries», Data Inf Manag, p. 100045, 2023, doi: https://doi.org/10.1016/j.dim.2023.100045.