

Seguridad en pagos digitales: Una revisión sistemática de amenazas y mecanismos de protección en plataformas de pagos digitales

Security in Digital Payments: A systematic review of threats and protection mechanisms in digital payment platforms

Zaleth Valentina Rivas Calderón¹ , Gian Franco Miguel Gonzalo Samana Ramírez² , Alberto Carlos Mendoza De Los Santos³ 

¹ Universidad Nacional de Trujillo, zvrivasca@unitru.edu.pe, La Libertad – Perú

² Universidad Nacional de Trujillo, gsamana@unitru.edu.pe, La Libertad – Perú

³ Universidad Nacional de Trujillo, amendozad@unitru.edu.pe, La Libertad – Perú

Autor para correspondencia: gsamana@unitru.edu.pe

RESUMEN

La rápida expansión de los pagos digitales ha transformado la economía global, pero también ha expuesto a los usuarios a amenazas cibernéticas cada vez más sofisticadas. La presente investigación sistemática, pretende analizar una selección de artículos relacionados a los temas de amenazas de seguridad y mecanismos de protección en pagos digitales. Para este propósito, se ha utilizado el método PRISMA. Las bases de datos científicas utilizadas fueron ScienceDirect, Springer y IEEE Xplore. Fueron 21 los artículos seleccionados que cumplieron con los criterios de inclusión. Los resultados indican que el phishing, el robo de credenciales y el fraude son las amenazas más latentes y probables, por otro lado, la autenticación multifactor, la biometría, la inteligencia artificial y el blockchain son los mecanismos de protección que más se mencionan en los artículos revisados. Finalmente, las variables de la confianza del usuario, la seguridad percibida, la usabilidad y la transparencia institucional, entre otros, son factores críticos y relevantes para la adopción continua de este tipo de tecnologías. La conclusión general del estudio es que el futuro de la seguridad en pagos digitales estará marcado por la innovación tecnológica y la reputación institucional de sus proveedores.

Palabras clave: Pagos digitales; Ciberseguridad; Amenazas digitales; Autenticación; Revisión sistemática.

ABSTRACT

The rapid expansion of digital payments has transformed the global economy, but it has also exposed users to increasingly sophisticated cyber threats. This systematic review aims to analyze a selection of articles related to security threats and protection mechanisms in digital payments. The PRISMA method was used for this purpose. The scientific databases used were ScienceDirect, Springer, and IEEE Xplore. Twenty-one articles were selected that met the inclusion criteria. The results indicate that phishing, credential theft, and fraud are the most latent and probable threats. On the other hand, multi-factor authentication, biometrics, artificial intelligence, and blockchain are the protection mechanisms most frequently mentioned in the reviewed articles. Finally, variables such as user trust, perceived security, usability, and institutional transparency, among others, are critical and relevant factors for the continued adoption of these technologies. The overall conclusion of the study is that the future of security in digital payments will be shaped by technological innovation and the institutional reputation of its providers.

Keywords: Digital payments; Cybersecurity; Digital threats; Authentication; Systematic review.

Derechos de Autor

Los originales publicados en las ediciones electrónicas bajo derechos de primera publicación de la revista son del Instituto Superior Tecnológico Universitario Rumiñahui, por ello, es necesario citar la procedencia en cualquier reproducción parcial o total. Todos los contenidos de la revista electrónica se distribuyen bajo una [licencia de Creative Commons Reconocimiento-No Comercial-4.0 Internacional](#).



Citar como:

Rivas Calderón, Z. V., Samana Ramírez, G. F. M. G., & Mendoza De Los Santos, A. C. (2026). Seguridad en pagos digitales: una revisión sistemática de amenazas y mecanismos de protección en plataformas de pagos digitales. *CONECTIVIDAD*, 7(2). <https://doi.org/10.37431/conectividad.v7i2.510>

1. INTRODUCCIÓN

Las aplicaciones de pagos digitales hoy por hoy ya son parte clave en los procesos de muchas empresas y, por tanto, en el crecimiento de la economía global. Esto sucede porque los tipos de pagos digitales se han ampliado, el comercio electrónico se ha potenciado y los teléfonos inteligentes se han convertido en una herramienta útil e indispensable en el día a día de las personas. No obstante, con la aparición de nuevas tecnologías emergen nuevos desafíos de seguridad y problemas en la protección de la información financiera (Khando et al., 2023). Es por eso que, en los últimos años, el interés por el impacto de estas nuevas formas de tecnología ha crecido. Autores como Shaikh (2024), identifican que las amenazas como el phishing, las filtraciones de datos y los accesos no autorizados se incrementan a medida que crece el sistema financiero digital.

El artículo de Sahi et al. (2022) señala que existe un aumento constante en la producción de estudios sobre seguridad y privacidad en pagos digitales. Los servicios financieros se están digitalizando y con ello, se generan ecosistemas complejos donde la interoperabilidad y el manejo de los datos sensibles son un desafío importante para la industria (Chauhan y Sharma, 2024). En ese sentido, estudios que analizaron las amenazas cibernéticas y los mecanismos de protección, destacan tecnologías como blockchain, inteligencia artificial y modelos Zero Trust para la mejora en la autenticación y detección de fraudes en tiempo real (Daah et al., 2024; McCabe et al., 2024). Cele & Kwenda (2025) en su revisión sistemática de 58 estudios concluyen que el phishing y el malware afectan negativamente la confianza del usuario y por tanto, que la banca digital llegue a más personas. En la misma línea, Waliullah et al. (2025), analizando 78 artículos, resaltan que la autenticación multifactor y la biometría son los mecanismos de protección más populares, mientras que la inteligencia artificial y blockchain demuestran poseer un gran potencial para evitar el fraude digital. Por último, otras investigaciones también destacan a la autenticación biométrica como una verificación de identidad digital óptima, útil y que puede reducir accesos ilegítimos (Patil et al., 2024; Rojas Solís et al., 2025).

Pero a pesar de las crecientes investigaciones, existen vacíos para presentar la integración del conocimiento entre amenazas emergentes y mecanismos de protección en pagos digitales. Khando et al. (2023) sostienen que en la mayoría de los artículos se abordan aspectos aislados, mientras que Cele & Kwenda (2025) resaltan que muchos estudios se concentran en analizar solo

las amenazas o contextos específicos, sin resultar en un análisis global de la seguridad. Por otro lado, también resaltan las observaciones para integrar la calidad de los sistemas tecnológicos, la regulación y la educación del usuario para poder enfrentar efectivamente los riesgos asociados. Por lo tanto, la presente investigación se plantea como objetivo sintetizar y analizar de manera sistemática la evidencia científica disponible sobre los temas mencionados: la seguridad en pagos digitales y los mecanismos de protección de las plataformas de pago. La relevancia de este artículo es que ofrecerá una visión actualizada e integrada de la literatura científica abordada en este campo, de esta forma se contribuye a comprender mejor los riesgos de seguridad y las estrategias implementadas en los sistemas de pago digital. Se busca aportar con información para futuras investigaciones y desarrollo de la seguridad en un contexto donde las transacciones digitales son una parte relevante en nuestras vidas.

2. MATERIALES Y MÉTODOS

El presente artículo es una revisión sistemática enfocada en el análisis de la seguridad en plataformas de pagos digitales. El estudio tiene como finalidad analizar la literatura científica, identificando las principales amenazas y los mecanismos de protección utilizados en los pagos digitales. Para ello, se empleó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), ya que proporciona un procedimiento estructurado y reproducible para la identificación, selección, evaluación y análisis de los estudios científicos (Page et al., 2021).

Con el propósito de orientar la revisión sistemática y responder al objetivo planteado, se formularon las siguientes preguntas de investigación: ¿cuáles son las principales amenazas de seguridad digital en pagos digitales?, ¿qué mecanismos de protección se utilizan para mitigar estas amenazas?, y ¿qué métodos generan mayor aceptación y confianza en los usuarios?, estas preguntas definen el alcance de la investigación y establecen los criterios para el análisis.

Todo el proceso de revisión estuvo a cargo de dos personas y se clasificaron de acuerdo a las bases de datos empleadas. Un revisor se encargó del cribado en ScienceDirect mientras que el otro revisor se encargó de las búsquedas en Springer y Xplore. Luego, para el análisis se encargaron ambas personas de realizar la síntesis y discusión de los resultados.

En cuanto hay desacuerdos entre ambas partes al momento de la selección de los registros, se resuelve por discusión verbal buscando llegar al acuerdo que beneficie el desarrollo de este

artículo de revisión. Toda información no resuelta o aclarada, que no se pudo conciliar, se busca resolver mediante la tercera opinión de un colega superior en experiencia.

La búsqueda bibliográfica se llevó a cabo en las siguientes bases de datos académicas indexadas, ScienceDirect, Springer e IEEE Xplore, mediante sus sitios web oficiales. Para todas las bases de datos se utilizó la misma llave de búsqueda: “digital payments” AND “threats” AND “security”, con el objetivo de mantener un estándar. Asimismo, se consideraron publicaciones científicas en idioma inglés y español relacionadas con amenazas digitales, ciberseguridad, autenticación, protección de datos y mecanismos de seguridad en sistemas de pago digital.

En la fase inicial de identificación, iniciada el 29 de abril del 2026, se obtuvieron 1839 registros procedentes de las bases de datos consultadas, tal como se presenta en la Tabla 1. En esta etapa no se aplicaron criterios de exclusión, con el objetivo de recopilar la mayor cantidad posible de literatura científica relacionada con el tema de estudio. Cabe señalar que no se identificaron la duplicidad en los registros, a grandes rasgos, durante el proceso posterior de cribado.

Tabla 1. Número de artículos encontrados en base de datos sin aplicar criterios de exclusión.

Fuente	Llave de Búsqueda	Artículos encontrados
Science Direct	“digital payments” and “threats” and “security”	877
Springer		704
IEEE Xplore		258
Total		1839

Fuente: Autoría propia.

Posteriormente, se inició el proceso de cribado y selección de estudios y se realizó de manera secuencial dentro de cada base de datos con el fin de asegurar la trazabilidad del análisis y optimizar la depuración de la literatura científica. Para ello, se aplicaron los criterios de exclusión definidos previamente: CE1 (rango de años de publicación 2021–2026), CE2 (tipo de documento: research article, review article, journal article y conference article), CE3 (acceso abierto u Open Access), CE4 (idioma inglés y español) y CE5 (pertinencia respecto a las preguntas de investigación).

El criterio CE5 fue aplicado como etapa final de evaluación de pertinencia, permitiendo seleccionar únicamente los estudios directamente relacionados con el objetivo de la investigación. Debido a ello, los artículos resultantes correspondieron a estudios únicos y relevantes para el análisis, por lo que no fue necesario realizar una etapa adicional de eliminación de registros

duplicados. Este filtrado progresivo permitió depurar sistemáticamente la literatura inicial y conservar únicamente los artículos con mayor relevancia científica para la revisión.

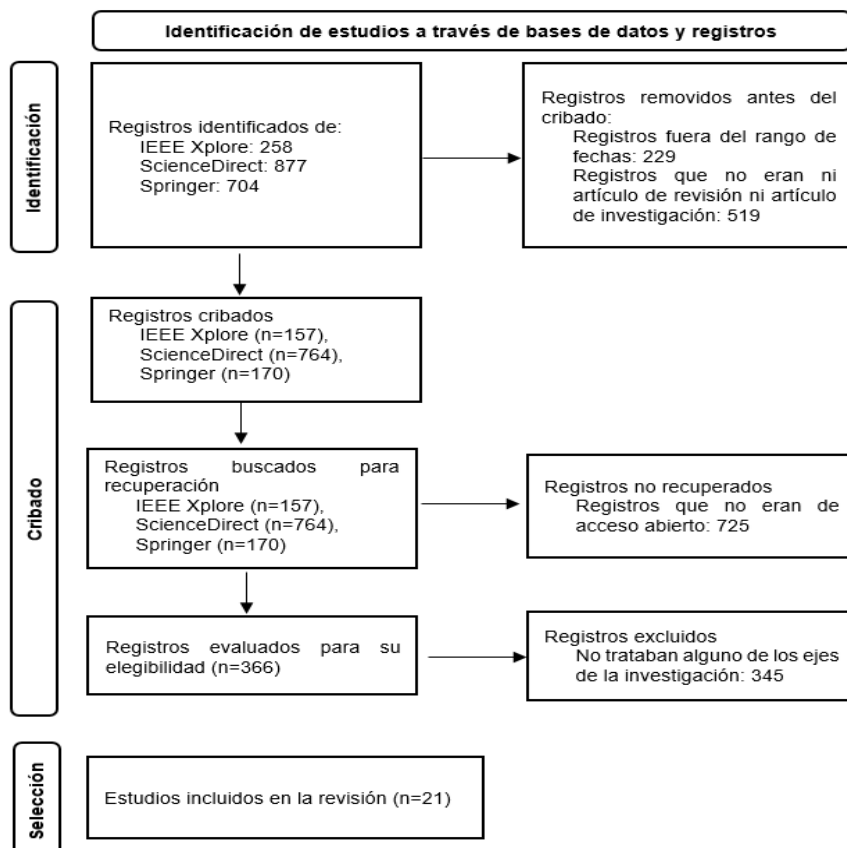
Los resultados del proceso de filtrado se presentan en la Tabla 2, donde se evidencia la reducción progresiva del número de artículos en cada base de datos a medida que se aplicaron los criterios CE1 a CE5.

Tabla 2. Número de artículos encontrados en base de datos aplicando criterios de exclusión.

Fuente	Artículos encontrados	Después de CE1 (2021–2026)	Después de CE2 (Review y Research Article)	Después de CE3 (Open Access)	Después de CE4 (Inglés y Español)	Después de CE5 (Responden a las preguntas de investigación)
Science Direct	877	768	764	292	292	12
Springer	704	657	170	61	61	8
IEEE Xplore	258	185	157	13	13	1

Fuente: Autoría propia.

Figura 1. Diagrama de flujo PRISMA para la presente revisión.



Fuente: Elaboración basada en una plantilla del diagrama en PRISMA Statement (s/f).

Se presenta también un diagrama para representar el flujo resuelto hasta la selección final de los artículos, a manera de facilitar el seguimiento, en la Figura 1.

Finalmente, el proceso termina tras 14 días calendario, finalizando el 13 de mayo del 2026, durante el cual se realizó la identificación, la elegibilidad y se seleccionaron los 21 artículos para el análisis final.

Para la extracción de los datos en las fuentes escogidas se optó por la realización de resúmenes cualitativos de los recursos, los cuáles incluían la siguiente estructura: metadatos básicos, objetivo del estudio, metodología utilizada, principales hallazgos, conclusiones del artículo y pertinencia de acuerdo a las preguntas de investigación.

Por otro lado, para el análisis de los sesgos en los artículos seleccionados se implementó mediante una comparación por lista de criterios como cantidad de las muestras utilizadas, origen geográfico y objetivo principal de los artículos. Sin embargo, se recomienda el uso de escalas apropiadas para este propósito.

Los estudios incluidos fueron organizados mediante una matriz de revisión, lo que permitió sistematizar la información y analizar las principales amenazas de seguridad en pagos digitales, los mecanismos de protección implementados y los enfoques tecnológicos predominantes en la literatura científica reciente.

3. RESULTADOS Y DISCUSIÓN

Se revisaron los 21 artículos escogidos y se identificaron tanto las amenazas planteadas como los mecanismos de protección. Estos ítems se visualizan en las Tabla 3 y Tabla 4.

Tabla 3. Cantidad de amenazas mencionadas, como tema central, en los artículos.

Amenazas identificadas	Frecuencia	Porcentaje (sobre 21)	Artículos de referencia
A1. Fraude Financiero Digital (DFF) y Robo de Fondos	11	52.38%	Ahmed et al. (2021); Aljaradat & Shukla (2026); Bojjagani et al. (2023); Fachrian et al. (2024); Li & Jiang (2025); Ly et al. (2025); Ofosu-Ampong et al. (2026); Prawira et al. (2024); Puri et al. (2025); Sasongko et al. (2022); Tran-Truong et al. (2025)
A2. Interceptación de Datos, Sniffing y Ataques MitM	5	23.81%	Ahmed et al. (2021); Bojjagani et al. (2023); Fachrian et al. (2024); Prawira et al. (2024); Tran-Truong et al. (2025)
A3. Ataques de Repetición (Replay Attacks)	2	9.52%	Bojjagani et al. (2023); Li & Jiang (2025)
A4. Phishing e Ingeniería Social	4	19.05%	Aljaradat y Shukla (2026); Alsulami et al. (2025); Ofosu-Ampong et al. (2026); Puri et al. (2025)

Amenazas identificadas	Frecuencia	Porcentaje (sobre 21)	Artículos de referencia
A5. Ransomware, Malware e Infiltración de Código	4	19.05%	Ahmed et al. (2021); Aisyah et al. (2025); Alsulami et al. (2025); Tran-Truong et al. (2025)
A6. Alteración y Pérdida de Registros de Transacción	4	19.05%	Fachrian et al. (2024); Li & Jiang (2025); Prawira et al. (2024); Sasongko et al. (2022)
A7. Suplantación de Identidad, Spoofing	4	19.05%	Bojjagani et al. (2023); Li & Jiang (2025); Ofosu-Ampong et al. (2026); Tran-Truong et al. (2025)
A8. Hackeo, Clonación o Robo de Datos Biométricos	6	28.57%	Li y Li (2023); Liébana-Cabanillas et al. (2025); Liébana-Cabanillas et al. (2026); Ofosu-Ampong et al. (2026); Puri et al. (2025); Tran-Truong et al. (2025)
A9. Brechas de Infraestructura y Exclusión Digital	5	23.81%	Adeniji et al. (2025); Padma Kiran & Vedala (2025); Mbuya et al. (2025); Mohamed Salman et al. (2026); Ungratwar et al. (2025)

Nota: Se supera la frecuencia de 21 artículos porque algunos de ellos tratan múltiples amenazas en una misma investigación.

Fuente: Autoría Propia.

En consecuencia, se crea una matriz de doble entrada para visualizar el corpus investigado a manera de sintetizar las relaciones entre las amenazas y los mecanismos de protección (Tabla 4 y Tabla 5).

Tabla 4. Cantidad de mecanismos de protección mencionados, como tema central, en los artículos.

Mecanismos identificados	Frecuencia	Porcentaje (sobre 21)	Artículos de referencia
M1. Criptografía y cifrado de datos	4	19.05%	Ahmed et al. (2021); Bojjagani et al. (2023); Li & Li (2023); Prawira et al. (2024)
M2. Autenticación Multifactor (MFA) y Biométrica	5	23.81%	Bojjagani et al. (2023); Liébana-Cabanillas et al. (2025); Liébana-Cabanillas et al. (2026); Ofosu-Ampong et al. (2026); Tran-Truong et al. (2025)
M3. Blockchain y Almacenamiento Descentralizado	3	14.29%	Fachrian et al. (2024); Li & Jiang (2025); Ungratwar et al. (2025)
M4. Inteligencia Artificial y Aprendizaje Automático	4	19.05%	Alsulami et al. (2025); Li & Jiang (2025); Ofosu-Ampong et al. (2026); Puri et al. (2025)
M5. Canales de Conexión y Protocolos de Proximidad Seguros	1	4.76%	Bojjagani et al. (2023)
M6. Controles Socio-Técnicos, Educación y Transparencia	11	52.38%	Adeniji et al. (2025); Aisyah et al. (2025); Aljaradat y Shukla (2026); Padma Kiran & Vedala (2025); Liébana-Cabanillas et al. (2026); Ly et al. (2025); Mbuya et al. (2025); Mohamed Salman et al. (2026); Prawira et al. (2024); Puri et al. (2025); Sasongko et al. (2022)

Nota: Se supera la frecuencia de 21 artículos porque algunos de ellos tratan múltiples mecanismos en una misma investigación.

Fuente: Elaboración propia.

Tabla 5. Identificación de amenazas vs mecanismos de protección en los artículos escogidos.

Amenazas \ Mecanismos de protección	M1	M2	M3	M4	M5	M6
A1	Ahmed et al. (2021); Bojjagani et al. (2023); Prawira et al. (2024)	Tran-Truong et al. (2025); Ofosu-Ampong et al. (2026); Bojjagani et al. (2023)	Fachrian et al. (2024); Li y Jiang (2025)	Li & Jiang (2025); Ofosu-Ampong et al. (2026); Puri et al. (2025)	Bojjagani et al. (2023)	Aljaradat y Shukla (2026); Sasongko et al. (2022); Ly et al. (2025); Puri et al. (2025)
A2	Ahmed et al. (2021); Bojjagani et al. (2023)	Tran-Truong et al. (2025); Bojjagani et al. (2023)	Fachrian et al. (2024)		Bojjagani et al. (2023)	Prawira et al. (2024)
A3	Bojjagani et al. (2023)	Bojjagani et al. (2023)	Li y Jiang (2025)		Bojjagani et al. (2023)	
A4		Ofosu-Ampong et al. (2026)		Alsulami et al. (2025)		Aljaradat y Shukla (2026); Puri et al. (2025)
A5	Ahmed et al. (2021)	Tran-Truong et al. (2025)		Alsulami et al. (2025)		Aisyah et al. (2025)
A6			Fachrian et al. (2024); Li y Jiang (2025)			Prawira et al. (2024); Sasongko et al. (2022)
A7	Bojjagani et al. (2023)	Tran-Truong et al. (2025); Bojjagani et al. (2023)	Li y Jiang (2025)	Ofosu-Ampong et al. (2026)		
A8	Li y Li (2023)	Liébana-Cabanillas et al. (2025); Liébana-Cabanillas et al. (2026); Tran-Truong et al. (2025)		Ofosu-Ampong et al. (2026)		Puri et al. (2025); Liébana-Cabanillas et al. (2026)
A9			Ungratwar et al. (2025)			Adeniji et al. (2025); Mohamed Salman et al. (2026); Padma Kiran & Vedala (2025); Mbuya et al. (2025)

Fuente: Elaboración propia.

Asimismo, se identificaron los tipos de investigación por artículo, mostrados en la Tabla 6.

Tabla 6. Distribución de los artículos por tipo de estudio.

Tipo de estudio	Frecuencia	Porcentaje
Primario	14	66.67%
Propuesta Técnica	4	19.05%
Revisión	3	14.29%
Total	21	100%

Fuente: Elaboración propia.

A continuación, la lista de artículos recopilados, en la cual se organizan los autores, sus países de afiliación, tipo de estudio y su aporte a la revisión, como se visualiza en la Tabla 7.

Tabla 7. Lista de artículos recopilados.

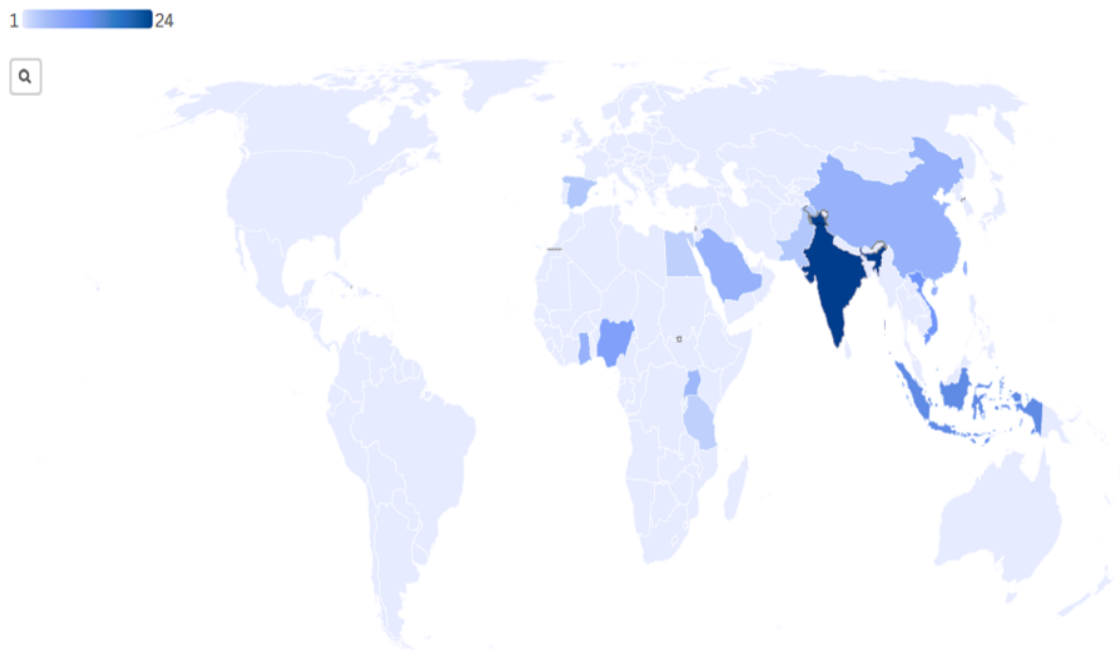
Nº	Autor(es) / País(es) de los autores	Tipo de estudio	Nivel de evidencia metodológica y aporte a la revisión
1	(Adeniji et al., 2025) Países: Nigeria, Uganda, EEUU	Primario (Mixto / Cualitativo)	Moderado. Utiliza revisión documental y entrevistas semiestructuradas. Se afirma que los pagos móviles directos a los empleados de la salud conllevan su aceptación y la eficiencia operativa de la misma.
2	(Ahmed et al., 2021) Países: Pakistán, India	Revisión	Bajo. Es una revisión teórica descriptiva y narrativa. Proporciona información valiosa sobre la tríada CIA, los tipos de sistemas de pago móviles (MPS) y las clasificaciones de sus amenazas y mecanismos de protección.
3	(Aisyah et al., 2025) País: Indonesia	Primario (Cuantitativo)	Alto. En el caso de 388 usuarios analizados, la confianza digital es la razón principal para seguir usando una aplicación de pago móvil, amortiguando el impacto negativo de los ataques cibernéticos.
4	(Aljaradat y Shukla, 2026) País: India	Primario (Cuantitativo)	Alto. Debido al estudio de 732 participantes, se aportó y validó un modelo de confianza digital indirecta, en el cual no necesariamente la confianza es un indicador del uso continuo de las apps de pago.
5	(Alsulami et al., 2025) Países: Arabia Saudita, Jordania	Propuesta Técnica	Alto. Se evalúa un modelo de IA que previene el phishing en QRs, alcanzando una precisión de hasta 99.81%, lo que demuestra viabilidad para su uso en aplicaciones del día a día.
6	(Bojjagani et al., 2023) País: India	Propuesta Técnica	Alto. Se ofrece una solución de pagos mediante dispositivos ponibles, altamente eficiente y probado rigurosamente. Una mirada a la criptografía en contexto financiero.
7	(Fachrian et al., 2024) Países: Indonesia, Polonia	Propuesta Técnica	Alto. Se propone una dApp donde la aplicación de blockchain implica que cualquier alteración en las transacciones es identificada. Esto constituye un aumento significativo en la seguridad e integridad del sistema. Sin embargo, los costos incurridos pueden desalentar la creación de soluciones.
8	(Padma Kiran & Vedala, 2025) País: India	Primario (Cuantitativo)	Alto. Usando el análisis PLS-SEM, se evidencia que, de los factores que propone UTAUT, la expectativa de rendimiento es el más influyente en la intención de adoptar la UPI (pagos unificados de la India).
9	(Li & Li, 2023) País: China	Primario (Cuantitativo)	Alto. Aplicó una serie de encuestas y analizó con PLS-SEM. Se afirma que la confianza en la tecnología y la confianza en los proveedores del servicio influyen positivamente en la intención de uso de los sistemas FRP (pago con reconocimiento facial).
10	(Li & Jiang, 2025) País: China	Propuesta Técnica	Alto. El SHCP (protocolo de consenso híbrido seguro) obtiene una precisión del 92% frente a la detección de fraude. Incluso, puede reducir el tiempo de validación en un 38%, habilitando transacciones rápidas y seguras.
11	(Liébana-Cabanillas et al., 2025) Países: España, Arabia Saudita	Primario (Mixto Cuantitativo)	Alto. Análisis que involucra 3 técnicas estadísticas para determinar que el factor más fuerte para explicar la adopción es la usabilidad y, por otro lado, la confianza digital.

Nº	Autor(es) / País(es) de los autores	Tipo de estudio	Nivel de evidencia metodológica y aporte a la revisión
12	(Liébana-Cabanillas et al., 2026) País: España	Primario (Cuantitativo)	Alto. En una muestra de 1805 usuarios, se determina que la variable que más influye en la intención de uso de las BPC (tarjetas de pago biométricas) es la expectativa de esfuerzo, y continúa, la expectativa de rendimiento.
13	(Ly et al., 2025) País: Camboya	Primario (Cuantitativo)	Alto. Utilizando PLS-SEM en 350 usuarios de una economía emergente, se concluye que la percepción de la calidad del servicio y la confianza son determinantes en la intención de uso las QR.
14	(Mbuya et al., 2025) País: Tanzania	Primario (Cuantitativo)	Alto. Utilizando el modelo PMT (Teoría de la Motivación para la Protección) se obtuvo que el factor predominante que impulsa la intención de uso en los grupos estudiados es la seguridad percibida, a diferencia de las recompensas, que no lo hacen tanto.
15	(Mohamed Salman et al., 2026) País: Egipto	Primario (Mixto)	Alto. Utilizando PLS-SEM en 406 participantes, se determina que lo que motiva el uso continuado en los pagos digitales es la facilidad de uso percibido y la pertenencia generacional (siendo los más jóvenes quienes están más abiertos a la adopción de las nuevas tecnologías).
16	(Ofosu-Ampong et al., 2026) País: Ghana	Primario (Cuantitativo)	Moderado. La muestra de 300 estudiantes universitarios reporta que tanto las protecciones técnicas realizadas con IA y las transacciones habilitadas por IA influyen positiva y fuertemente en la seguridad y confianza percibida de los usuarios.
17	(Prawira et al., 2024) País: Indonesia	Primario (Mixto)	Alto. Aplicando ECM en 522 usuarios activos de billeteras digitales se confirma que la percepción de seguridad influye positivamente en la percepción de utilidad por el usuario.
18	(Puri et al., 2025) País: India	Primario (Cuantitativo)	Alto. Analizando a 457 usuarios de pagos digitales con BRT, se estudia qué incentivos motivan al usuario a prevenir fraude financiero digital mediante sus propios medios.
19	(Sasongko et al., 2022) País: Indonesia	Primario (Cuantitativo)	Alto. Evaluando a 413 usuarios con CB-SEM, se concluye que no solo la utilidad percibida es un factor que influye a la intención de uso continuado de la tecnología de pagos, sino que lo son además la confianza y la satisfacción.
20	(Tran-Truong et al., 2025) Países: Vietnam, Finlandia	Revisión	Alto. Analizando el corpus de 70 artículos académicos y evaluando 13 herramientas de autenticación, se concluye que existe una brecha entre la teoría sobre métodos de autenticación y la práctica comercial de estas soluciones de seguridad, donde se prefiere el alcance por sobre la robustez.
21	(Ungratwar et al., 2025) País: India	Revisión	Alto. Macroestudio de escala masiva de 1959 artículos donde la investigación concluye que existe un desplazamiento hacia la banca móvil, los pagos digitales y las <i>fintech</i> , el cual el área crítica es la mitigación de riesgos cibernéticos.

Fuente: Elaboración propia.

Por otro lado, también se elabora la Figura 2, en la cual se visualiza la distribución de países afiliados a los autores de los artículos seleccionados, con el fin de visualizar la procedencia geográfica de la producción científica analizada. La amenaza que más se trata a lo largo de los 21 artículos es el fraude financiero digital (FDD).

Figura 2. Distribución de países afiliados a los autores de los artículos seleccionados.



Fuente: Elaboración propia.

Pero esta amenaza sería solo una consecuencia de otras como por ejemplo el phishing, el ransomware y/o ataques de ingeniería social. Uno de los artículos explora el ataque *ransomware* que sufrió BSI en Indonesia (Aisyah et al., 2025) donde se evidencia el impacto en la continuación de operaciones de los bancos que, si no están respaldados por una previa confianza por parte del usuario, pueden afectar la decisión de seguir usando sus servicios. Pero tomando en cuenta el contexto cultural de Indonesia, los autores afirman también que el compromiso religioso de evitar la usura actuó como el amortiguador que retuvo al 98% de los usuarios encuestados en el uso de los servicios frente a una deserción del 2%. Caso opuesto es el estudio de Aljaradat & Shukla (2026) donde se evidencia que una persona que sufrió incidentes de ciberseguridad es más propensa a estar vigilante del contexto tecnológico de las empresas financieras. Lo mismo investiga Mbuya et al. (2025) cuando demuestra que, en el contexto de economías emergentes, el riesgo de ciberseguridad percibido es un determinante en el uso de los servicios. Siendo estas amenazas sobre el servidor e infraestructura conviene explicar las amenazas que podrían ser más peligrosas: las que abordan el desconocimiento del usuario. Alsulami et al. (2025) argumenta que el phishing con QRs pueda ser de las amenazas más dinámicas y difíciles de contener al ejecutarse en tiempo real. Otro de los motivos es que son fáciles de implementar en mercados de rápida digitalización como en Nigeria o Camboya, aprovechándose de la baja

alfabetización digital de la población (Adeniji et al., 2025; Ly et al., 2025). No obstante, en países donde los pagos digitales ya están bien afianzados como en China, Li y Li (2023) exponen la contradicción conductual en la que, si el sistema es útil y de bajo esfuerzo, los usuarios pueden despreciar la vulnerabilidad percibida por posibles filtraciones de sus datos biométricos. Esta postura la apoya también Liébana-Cabanillas et al. (2026), que en un mercado británico analizó también que el riesgo percibido no tiene impacto en el uso continuo de los servicios de pago digitales. En última instancia, las amenazas en los sistemas de pago no son principalmente las de vacíos técnicos, sino que son las variables sociales como la madurez del mercado y la cultura del individuo las que pueden reducir la percepción del riesgo financiero.

Con respecto a los mecanismos de protección, existe una tendencia investigativa hacia la adopción de tecnologías avanzadas de protección como la inteligencia artificial y cadenas de bloques (Ungratwar et al., 2025). En el nivel de las blockchain, Fachrian et al. (2024) proponen un modelo basado en contratos inteligentes y almacenamiento distribuido en IPFS, una solución en la infraestructura. Mientras que Li y Jiang (2025) van más allá al proponer una solución no basada en la inmutabilidad de las *blockchain*, sino en el proceso de validación de consenso para predecir anomalías en tiempo real. Sin embargo, esta robustez técnica es altamente contrastada por la experiencia de usuario solicitada en el mercado. Si bien Bojjagani et al. (2023) diseñan complejos protocolos criptográficos ligeros para compensar las limitaciones técnicas de los dispositivos móviles y ponibles (Ahmed et al., 2021), autores como Prawira et al. (2024) aportan con una mirada de la realidad distinta: añadir capas técnicas a la autenticación no tiene un impacto sustancial en la seguridad percibida por el usuario, quienes prefieren la comunicación institucional y la transparencia en los procesos transaccionales. Esto se evidencia aún más con la investigación de Tran-Truong et al. (2025), quienes revelan la brecha de implementación en los sistemas actuales, donde se prefiere la practicidad por sobre la calidad de las técnicas de seguridad, con un 33% de los servicios de TI estudiados aun usando códigos OTP por razones de costo y familiaridad heredada. En conclusión, los mecanismos de seguridad, aunque están constantemente innovando en eficiencia y robustez técnica, no pueden quedarse solamente en la fortaleza matemática de sus implementaciones, sino que, deben considerar también la resistencia de los usuarios, quienes buscan la practicidad y usabilidad en los servicios de pagos digitales.

En cuanto a la aceptación y confianza de los usuarios, los resultados evidencian que los factores más influyentes en la adopción continua de pagos digitales son la percepción de seguridad, la facilidad de uso y la confianza institucional. Se identificó que las expectativas de rendimiento y facilidad de uso son factores determinantes para la adopción de plataformas de pago digital y tarjetas biométricas (Padma Kiran & Vedala, 2025; Aljaradat & Shukla, 2026). De igual forma, investigaciones en España y Reino Unido demuestran que la usabilidad percibida afecta más a la intención de adopción que factores sociales externos (Liébana-Cabanillas et al., 2025). Esto es así en sociedades individualistas, sin embargo, en países colectivistas como Camboya, es diferente: la influencia social y el respaldo colectivo son más determinantes para adoptar los pagos digitales (Ly et al., 2025). Estos resultados demuestran que la aceptación tecnológica no depende únicamente de la robustez técnica de la plataforma, sino también de la capacidad institucional para transmitir seguridad, transparencia y confiabilidad al usuario (Sasongko et al. 2022). Sin embargo, lo relevante es la marcada diferencia entre la seguridad técnica y la seguridad percibida por los usuarios. Se encontró que la implementación de mecanismos avanzados de protección no siempre incrementa la confianza del usuario si estos no son comprensibles, visibles o fáciles de aplicar por sí mismos (Puri et al., 2025). Por ejemplo, Ofosu-Ampong et al. (2026) comprobaron que los usuarios depositan más confianza en las medidas de seguridad visibles promovidas por la inteligencia artificial que en simples declaraciones institucionales sobre protección. Mientras que, Prawira et al. (2024) hallaron que el cifrado y una información clara acerca de la seguridad provocan una percepción de protección mayor que sistemas complejos de autenticación. Esta brecha abre un dilema ético para los proveedores de servicios TI ante el despliegue de la biometría e inteligencia artificial. Si se exponen los datos biológicos como el rostro (Li & Li, 2023) o las huellas dactilares (Liébana-Cabanillas et al., 2026) el usuario correría un alto riesgo de vulnerabilidad en sus servicios. ¿Hasta qué punto estarían los usuarios dispuestos a admitir este riesgo en los sistemas? Es una pregunta que conllevaría estudiar variables adicionales como la gobernabilidad y las regulaciones. En países donde existen marcos regulatorios que defienden la protección del usuario, se reduce la percepción de amenaza (Liébana-Cabanillas et al., 2026). Por el contrario, en entornos con vacíos de gobernanza, el despliegue involucraría un rechazo rotundo si es que no se

implementan las defensas explicables y transparentes para el cliente (Ofosu-Ampong et al., 2026). En conclusión, los métodos de seguridad que serán más eficientes para el usuario son aquellos que lo incluyen financieramente y lo forman mediante una experiencia transparente, considerando sus implicancias generacionales y de cultura (Mohamed Salman et al., 2026).

3.1. Limitaciones del estudio

El análisis de las fuentes conllevó una revisión sin uso de herramientas informáticas que ayuden con una extracción de datos más ordenada. Por otro lado, se presenta un sesgo en los recursos identificados al ser provenientes en su mayoría del continente asiático y africano. Y, además, una inclinación hacia los artículos de tipo cuantitativo. Se recomienda incorporar literatura gris que contrapesa estos vacíos, al ser, además, la búsqueda limitada a artículos de revista de acceso abierto.

4. CONCLUSIONES

Las amenazas más críticas se asocian con la identidad del usuario: el fraude digital, phishing, robo de credenciales, ataques a mecanismos de autenticación y vulneraciones relacionadas a la confianza del usuario. Los canales de estas amenazas van desde las billeteras electrónicas, los pagos móviles hasta los sistemas biométricos, códigos QR y plataformas basadas en blockchain. Esto evidencia el acelerado crecimiento de las fintech y ecosistemas de pago electrónico, pero a su vez, la rápida exposición a peligros y riesgos cibernéticos.

Sobre los mecanismos de protección identificados, se concluye que las tendencias buscan la simplicidad y rapidez en la autenticación: el método multifactor se presenta como una opción segura, aunque con pasos iniciales extensos; la biometría presenta rapidez y robustez en la mayoría de los casos; otros métodos como el cifrado avanzado, inteligencia artificial y blockchain se muestran como opciones más avanzadas, aunque costosas, para la seguridad de las transacciones y reducción del fraude. Sin embargo, los artículos revisados también coinciden en lo siguiente: ninguna solución aislada es completamente efectiva frente a las amenazas. La seguridad en los pagos digitales merece integrar todas tipo de soluciones posibles, desde tecnologías robustas y monitoreo constante hasta estrategias organizacionales y educación del usuario.

Por último, se comprende que el futuro de los pagos digitales dependerá del equilibrio entre protección, usabilidad y confianza. Aunque soluciones prometedoras como el uso de blockchain o inteligencia artificial sean las más seguras para la detección y prevención de fraude, aún siguen

lejos de las aplicaciones prácticas y estandarizadas que la industria reclama. Todavía persisten desafíos como mejorar la accesibilidad, reducir los costos de implementación, democratizar la alfabetización digital y adaptarse constantemente a nuevos ataques a la privacidad y seguridad de los usuarios. Es por esto que, resultará fundamental que las próximas investigaciones relacionadas a este campo profundicen en el análisis de soluciones de seguridad más transparentes, comprensibles y adaptables a las distintas economías y contextos geopolíticos de los usuarios de los servicios financieros.

Contribución de los Autores (CRediT): ZVRC: Conceptualización, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Validación, Visualización, Redacción - borrador original, Redacción - revisión y edición. GFMGSR: Conceptualización, Curación de datos, Investigación, Metodología, Administración del proyecto, Recursos, Validación, Visualización, Redacción - borrador original, Redacción - revisión y edición. ACMDLS: Supervisión, Validación.

Conflicto de Intereses: Los autores declaran que no existen conflictos de intereses en esta publicación.

Declaración de Uso de Inteligencia Artificial: Los autores declaran que no utilizaron herramientas de inteligencia artificial (IA) en el artículo.

REFERENCIAS

- Adeniji, F. P., Adewole, D. A., Bello, S., Ekirapa, E., Aweko, J., Kiberu, V. M., Opio, C., Waiswa, P., & Fawole, O. I. (2025). How prepared is Nigeria digital payment for health workers? A landscape analysis. *BMC Health Services Research*, 25(1), 200. <https://doi.org/10.1186/s12913-025-12338-z>
- Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in next generation mobile payment systems: A comprehensive survey. *IEEE Access: Practical Innovations, Open Solutions*, 9, 115932–115950. <https://doi.org/10.1109/access.2021.3105450>
- Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures (Amsterdam, Netherlands)*, 10(101530), 101530. <https://doi.org/10.1016/j.sftr.2025.101530>
- Aljaradat, A., & Shukla, S. (2026). Cybersecurity and trust formation in digital payment use behaviour in North India. *Discover Sustainability*, 7(1). <https://doi.org/10.1007/s43621-026-02769-x>
- Alsulami, A. A., Al-Haija, Q. A., Alturki, B., Yafoz, A., Alqahtani, A., Alsini, R., & Binyamin, S. S. (2025). Efficient malicious QR code detection system using an advanced deep learning approach. *Computer Modeling in Engineering & Sciences*, 145(1), 1117–1140.

<https://doi.org/10.32604/cmes.2025.070745>

- Bojjagani, S., Seelam, N. R., Sharma, N. K., Uyyala, R., Akuri, S. R. C. M., & Maurya, A. K. (2023). The use of IoT-based wearable devices to ensure secure lightweight payments in FinTech applications. *Journal of King Saud University - Computer and Information Sciences*, 35(9), 101785. <https://doi.org/10.1016/j.jksuci.2023.101785>
- Cele, N.N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32. <https://doi.org/10.1108/jfc-10-2023-0263>
- Chauhan, Y., & Sharma, P. (2024). A systematic literature review of digital payments. *Metamorphosis: A Journal of Management Research*, 23(2), 173-187. <https://doi.org/10.1177/09726225241257730>
- Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust models in the financial industry through blockchain integration: A proposed framework. *Electronics*, 13(5), 865. <https://doi.org/10.3390/electronics13050865>
- Fachrian, M. A., Sukarno, P., & Wardana, A. A. (2024). Decentralize transaction records of digital payment gateway using Ethereum Blockchain and Interplanetary File System. *Procedia Computer Science*, 237, 269–276. <https://doi.org/10.1016/j.procs.2024.05.105>
- Khando, K., Islam, M.S., & Gao, S. (2023). The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet*, 15(1), 21. <https://doi.org/10.3390/fi15010021>
- Li, C., & Li, H. (2023). Disentangling facial recognition payment service usage behavior: A trust perspective. *Telematics and Informatics*, 77(101939), 101939. <https://doi.org/10.1016/j.tele.2023.101939>
- Li, S., & Jiang, G. (2025). Security and efficiency improvement of internet financial payment based on blockchain technology. *Discover Computing*, 28(1). <https://doi.org/10.1007/s10791-025-09835-4>
- Liébana-Cabanillas, F., Abbasi, G. A., Higuera-Castillo, E., & Wagner, R. (2025). Press to pay: The power of biometrics in financial transactions investigated by PLS-SEM, fsQCA, and NCA. *Technological Forecasting and Social Change*, 221(124365), 124365. <https://doi.org/10.1016/j.techfore.2025.124365>

doi.org/10.1016/j.techfore.2025.124365

- Liébana-Cabanillas, F., Irimia-Diéguez, A., Albort-Morant, G., & Zarco, C. (2026). Unlocking the future of paytech: exploring biometric payment card adoption patterns. *Financial Innovation*, 12(1). <https://doi.org/10.1186/s40854-025-00883-9>
- Ly, B., Ly, R., & Ma, S. (2025). User-centric drivers of QR payment adoption in emerging economies: trust, quality, and social influence. *Future Business Journal*, 11(1). <https://doi.org/10.1186/s43093-025-00681-w>
- Mbuya, K. H., Chachage, B., & Pasape, L. (2025). The influence of security and reward on behavioral intention to adopt mobile payment: A comparative analysis of users versus non-users in Tanzania's handicraft industry. *Social Sciences & Humanities Open*, 12(102028), 102028. <https://doi.org/10.1016/j.ssaho.2025.102028>
- McCabe, C., Mohideen, A. I. C., & Singh, R. (2024). A blockchain-based authentication mechanism for enhanced security. *Sensors (Basel, Switzerland)*, 24(17), 5830. <https://doi.org/10.3390/s24175830>
- Mohamed Salman, D., Mohamed Awad, M., & Soliman, C. (2026). An integrated analysis of technology adoption, demographic moderators, and financial inclusion across generations in Egypt. *Future Business Journal*, 12(1). <https://doi.org/10.1186/s43093-026-00803-y>
- Ofosu-Ampong, K., Ansong, E., Akandekumtiim, J.-M., Asmah, A., Commey, N. O., Amankwaa, T., & Tsedzah, V. (2026). How AI-enabled security features shape payment security perceptions and trust in digital payment systems. *Telematics and Informatics Reports*, 21(100298), 100298. <https://doi.org/10.1016/j.teler.2026.100298>
- Padma Kiran, K., & Vedala, N. S. (2025). Assessing Unified Payments Interface (UPI) adoption and usage through the interplay of UTAUT factors. *Humanities & Social Sciences Communications*, 12(1). <https://doi.org/10.1057/s41599-025-05313-w>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting

- systematic reviews. *Systematic Reviews*, 10, 89. <https://doi.org/10.1136/bmj.n71>
- Patil, S., Dudhankar, V., & Shukla, P. (2024). Enhancing digital security: How identity verification mitigates E-commerce fraud. *Journal of Current Science and Research Review*, 2(02), 69–81. <https://jcsrr.org/index.php/jcsrr/article/view/73>
- Prawira, F. R., Prakoso, N. T., Handayani, P. W., & Harahap, N. C. (2024). The influence of information security factors on the continuance use of electronic wallet. *Procedia Computer Science*, 234, 1467–1475. <https://doi.org/10.1016/j.procs.2024.03.147>
- PRISMA Statement. (s/f). *PRISMA 2020 flow diagram*. Recuperado el 14 de octubre de 2026, de <https://www.prisma-statement.org/prisma-2020-flow-diagram>
- Puri, L., Kumar, A., & Singh, R. (2025). What drives or discourages fraud-safe behavior in digital transactions? a BRT perspective. *Acta Psychologica*, 260(105675), 105675. <https://doi.org/10.1016/j.actpsy.2025.105675>
- Rojas Solís, S., Aguilera Zatarain, J. J., Rendón Rendón, M. D. E. L. A., & Escobedo Rodriguez, A. M. (2025). Análisis comparativo de los mecanismos de autenticación de usuarios para el manejo seguro del dinero digital. *Revista Digital de Tecnologías Informáticas y Sistemas*, 9(1), 1–8. <https://doi.org/10.61530/redtis.vol9.n1.2025.269>
- Sahi, A.M., Khalid, H., Abbas, A.F., Zedan, K., Khatib, S.F.A., & Al Amosh, H. (2022). The research trend of security and privacy in digital payment. *Informatics*, 9(2), 32. <https://doi.org/10.3390/informatics9020032>
- Sasongko, D. T., Handayani, P. W., & Satria, R. (2022). Analysis of factors affecting continuance the electronic money application in Indonesia. *Procedia Computer Science*, 197, 42–50. <https://doi.org/10.1016/j.procs.2021.12.116>
- Shaikh, D. M. Y. Z. (2024). Security Concerns in Digital Payments: An Overview. *Educational Administration: Theory and Practice*, 30(6), 4882–4889. <https://doi.org/10.67145/kuey.v30i6.8680>
- Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., Van, L. C. P., Le, K. T., Vo, K. H., Kim, N. N. T., Nguyen, T. M., & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of Systems*

Architecture, 162(103402), 103402. <https://doi.org/10.1016/j.sysarc.2025.103402>

Ungratwar, S., Sharma, D., y Kumar, S. (2025). Mapping the digital banking landscape: a multi-dimensional exploration of fintech, digital payments, and e-wallets, with insights into current scenarios and future research. *Humanities & Social Sciences Communications*, 12(1). <https://doi.org/10.1057/s41599-025-05186-z>

Waliullah, M., George, M.Z.H., Hasan, M.T., Alam, M.K., Munira, M.S.K., & Siddiqui, N.A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, 1(01), 226–257. <https://arxiv.org/abs/2503.22710>