ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.648

Mitigation strategies for cyberattacks on electronic invoicing systems: A systematic literature review

Shelvy Carrasco-Oré[1]; Julio Andres Chauca-Lopez[2]; Gaby Mónica Felipe-Bravo[3]
[1,2,3]Universidad Tecnológica del Perú, Perú, *1100527@utp.edu.pe, U21223255@utp.edu.pe, c24905@utp.edu.pe*

***Abstract*– The growing adoption of electronic invoicing has brought operational benefits but also increased cybersecurity risks. This study conducts a systematic literature review of scientific publications from 2020 to 2025 to identify cyberattack mitigation strategies applied to electronic invoicing systems. The PRISMA approach and the PICO model were used to structure the search, resulting in the selection of 62 relevant articles from Scopus and Dimensions. The findings reveal a predominance of preventive approaches based on artificial intelligence, blockchain, and big data. Protection gaps were also identified in sectors such as SMEs and retail. The study proposes future research directions focused on integrating predictive tools with adaptive regulatory frameworks.**

***Keywords*-- Electronic invoices, electronic commerce, risk management, risk mitigation, risk control.**

Estrategias de mitigación de ciberataques en sistemas de facturación electrónica: Una revisión sistemática de la literatura

Shelvy Carrasco-Oré[1]; Julio Andres Chauca-Lopez[2]; Gaby Mónica Felipe-Bravo[3]
[1,2,3]Universidad Tecnológica del Perú, Perú, *1100527@utp.edu.pe, U21223255@utp.edu.pe, c24905@utp.edu.pe*

***Resumen*– La creciente adopción de la facturación electrónica ha traído beneficios operativos, pero también ha incrementado los riesgos cibernéticos. Este estudio realiza una revisión sistemática de la literatura científica entre 2020 y 2025 para identificar estrategias de mitigación de ciberataques aplicadas en sistemas de facturación electrónica. Se empleó el enfoque PRISMA y el modelo PICO para estructurar la búsqueda, seleccionando 62 artículos relevantes de Scopus y Dimensions. Los hallazgos evidencian un predominio de enfoques preventivos basados en inteligencia artificial, blockchain y big data. También se identificaron vacíos de protección en sectores como PYMES y retail. Se proponen líneas futuras de investigación que integren herramientas predictivas con marcos normativos adaptativos.**

Palabras clave- Facturación electrónica, comercio electrónico, gestión de riesgos, mitigación de riesgos, control de riesgos.

I. Introducción

El comercio electrónico ha experimentado una rápida expansión, impulsada en gran medida por la pandemia de COVID-19 [1]. En este contexto, la facturación electrónica se posiciona como medio estratégico para optimizar los procesos administrativos y fiscales, al facilitar una gestión más eficiente, segura y transparente [2]. Por otro lado, este avance, aunque beneficioso, ha incrementado los riesgos cibernéticos, ya que la información fiscal queda expuesta a amenazas como phishing, ransomware, inyección de código malicioso y las vulnerabilidades en APIs [3]. Estos ataques suelen dirigirse a componentes empresariales críticos, y debido a la interdependencia entre sistemas, una vulnerabilidad en una sola capa puede comprometer otras, amplificando significativamente el daño [4].

En respuesta a estos desafíos, han cobrado relevancia las soluciones basadas en blockchain. Se estima que alrededor del 60 % de las iniciativas que aplican esta tecnología en ciberseguridad se enfocan en garantizar la integridad y la inmutabilidad de los registros de facturación electrónica [5]. En paralelo, la ciberseguridad ha evolucionado frente a amenazas sofisticadas, sustituyendo enfoques tradicionales por soluciones basadas en inteligencia artificial. Técnicas como el aprendizaje automático y profundo optimizan la detección de intrusiones, mejorando la identificación de patrones anómalos y la adaptación a nuevos ataques [6]. Sin embargo, a pesar de estos avances tecnológicos, muchas organizaciones siguen enfrentando consecuencias devastadoras a raíz de los ciberataques. En particular, las pequeñas empresas presentan una alta vulnerabilidad: aproximadamente el 60 % de ellas cierra sus operaciones pocos meses después de sufrir un incidente, lo cual evidencia la fragilidad de sus sistemas y su limitada capacidad de recuperación [7]. Frente a esta realidad, el phishing destaca como una de las amenazas más costosas, con un impacto medio superior a los 4,9 millones de dólares por caso, incluyendo daños operativos, legales y reputacionales [8].

Asimismo, las proyecciones globales advierten que el costo acumulado de los ciberataques podría superar los 10,5 billones de dólares anuales en los años posteriores, lo que refuerza la necesidad urgente de adoptar medidas estructurales y sostenibles frente a esta amenaza creciente [9]. En consecuencia, resulta importante replantear las estrategias de seguridad aplicadas a sistemas críticos como los de facturación electrónica, integrando soluciones técnicas avanzadas, marcos organizacionales sólidos y programas de concienciación que fortalezcan la resiliencia digital de las instituciones.

Entre las estrategias emergentes destacan los modelos híbridos basados en XGBoost para la detección de patrones complejos [10], y enfoques de gestión dinámica de vulnerabilidades mediante virtualización, como AENNER [11].

El aumento de los ciberataques en entornos fiscales digitales y la creciente adopción de tecnologías emergentes [12], motivan la necesidad de una revisión sistemática que sintetice el conocimiento existente en torno a estrategias de mitigación aplicadas a la facturación electrónica. Aunque se han realizado avances en áreas como IoT (38 %), salud (20 %) y redes inalámbricas (12 %), este sector específico ha recibido escasa atención en estudios de revisión, pese a su criticidad operativa [13]. Esta revisión busca organizar el conocimiento disperso, identificar vacíos relevantes y orientar tanto a investigadores como a profesionales en la formulación de soluciones más robustas y sostenibles.

Por ello, este estudio buscó identificar las estrategias de mitigación de ciberataques en sistemas de facturación electrónica halladas en publicaciones científicas entre los años 2020 y 2025. A través de una revisión sistemática, se compararon enfoques, identificaron vacíos de protección y se proponen medidas para reforzar la seguridad, integridad y continuidad operativa, orientando decisiones técnicas y fomentando prácticas resilientes.

La revisión se estructura para garantizar un análisis riguroso y claro. La sección metodológica describe el enfoque sistemático, desde las preguntas de investigación hasta los criterios de selección y evaluación de estudios. En los resultados, se ofrece una visión consolidada de las estrategias identificadas, organizadas según su aplicabilidad en sistemas de facturación electrónica. La discusión analiza críticamente los

hallazgos, resalta vacíos, desafíos técnicos y tendencias emergentes. Finalmente, en las conclusiones, se sintetizan los aportes del estudio, definen sus límites y proponen nuevas rutas de investigación en seguridad digital.

II. Metodología

La presente investigación se llevó a cabo mediante una Revisión Sistemática de la Literatura, en la que se empleó un enfoque estructurado que permitió identificar, seleccionar y analizar críticamente estudios relevantes. Esta metodología ofrece una visión actualizada del estado del conocimiento, identifica vacíos existentes y orienta futuras investigaciones [14]. Para asegurar la calidad y transparencia del proceso, la estructuración del trabajo siguió los lineamientos del método PRISMA [15].

La pregunta de investigación fue: ¿Qué estrategias de mitigación de ciberataques se utilizan en sistemas de facturación electrónica reportada en la literatura científica entre el 2020 y 2025? Fue elaborada siguiendo la estructura PICO. Este modelo mejoró la precisión en la recuperación de información científica [16]. Como resultado, se formularon tres preguntas especificas cuyos elementos se visualizan en la siguiente tabla:

TABLA I
Estructura de la pregunta PICO

Componente	Pregunta	Keywords
P	¿Qué sistemas están expuestos a ciberataques?	"e-invoice", "Electronic invoices", "electronic commerce", "e-commerce", "digital commerce"
I	¿Qué estrategias de mitigación se han aplicado frente a ciberataques?	Risk management, risk assessment
C	No aplica	No aplica
O	¿Qué nivel de efectividad presentan estas estrategias en términos de protección, resiliencia y continuidad operativa?	Risk mitigation, risk control

Para garantizar la consistencia terminológica en la estrategia de búsqueda, se consultaron dos tesauros especializados. A partir de estos, se identificaron los términos controlados más relevantes vinculados con la pregunta de investigación, los cuales se detallan a continuación:

TABLA II
Tesauro y palabras clave

Tesauro	Palabras clave
IEEE Thesaurus	Electronic invoices, electronic commerce, e-commerce, digital commerce, risk management, risk assessment, risk mitigation
Library of Congress Subject Headings (LCSH)	e-invoice, risk control, enterprise, business organization, retail

Para la recolección de información, se consultaron las bases de datos Scopus y Dimensions, donde se aplicaron las siguientes ecuaciones de búsqueda:

Scopus

TITLE-ABS-KEY ("e-invoice" OR "Electronic invoices" OR "electronic commerce" OR "e-commerce" OR "digital commerce") AND TITLE-ABS-KEY ("Risk management" OR "risk assessment") AND TITLE-ABS-KEY ("Risk mitigation" OR "risk control") AND TITLE-ABS-KEY ("enterprise" OR "business organization" OR "retail")) AND PUBYEAR > 2020 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp")) AND (LIMIT-TO (LANGUAGE , "English"))

Dimensions

(e-invoice OR electronic invoices OR electronic commerce OR e-commerce OR digital commerce) AND (risk management OR risk assessment) AND (risk mitigation OR risk control) AND (enterprise OR business organization OR retail)

Tras la obtención de los resultados provenientes de las bases de datos Scopus y Dimensions, se procedió a aplicar los criterios de inclusión y exclusión, cuyos detalles se consignan en las siguientes tablas:

TABLA III
Criterios de inclusión

N. º	Criterios
CI1	Revisadas por pares
CI2	Publicados entre 2020 y 2025
CI3	En idioma ingles
CI4	Relacionado con facturación electrónica, gestión y mitigación de riesgos
CI5	Contextos empresariales: empresas, organizaciones o sector retail
CI6	Artículos indexados en Scopus o Dimensions
CI7	Disponibilidad en acceso abierto

TABLA IV
Criterios de Exclusión

N. º	Criterios
CE1	Publicaciones anteriores a 2020
CE2	Estudios de revisiones sistemáticas de la literatura y artículos de revisión.
CE3	Tipos de documento distintos a artículos científicos
CE4	Sin acceso abierto

PRISMA permitió visualizar de manera transparente y ordenada las etapas de inclusión y exclusión de los estudios [17].

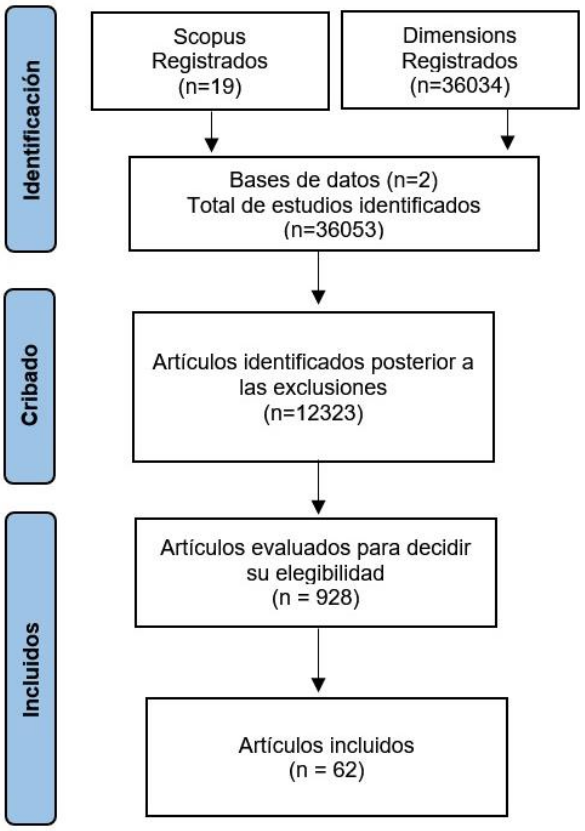
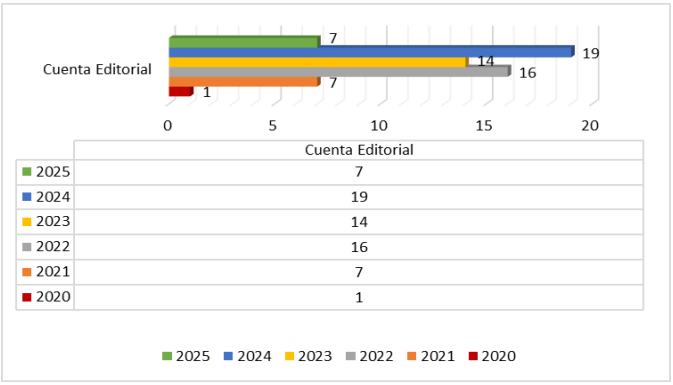


Fig. 1. Resumen de selección de artículos.

La Fig. 1 evidencia que, pese a la amplia cantidad de artículos hallados en la búsqueda inicial, únicamente 62 cumplieron con los requisitos de inclusión y exclusión.

III. Resultados

En función de los estudios recopilados, se sistematizó información bibliométrica que incluye variables como el país de publicación, año, editorial y palabras clave relevantes:



	Cuenta Editorial
2025	7
2024	19
2023	14
2022	16
2021	7
2020	1

Fig. 2. Nº Total de artículos revisados según año de publicación.

En la Fig.2 Número de artículos revisados por año. La distribución anual de publicaciones muestra un incremento hasta 2024, con un máximo de 19 registros, seguido de una disminución en 2025; el mínimo se observa en 2020.

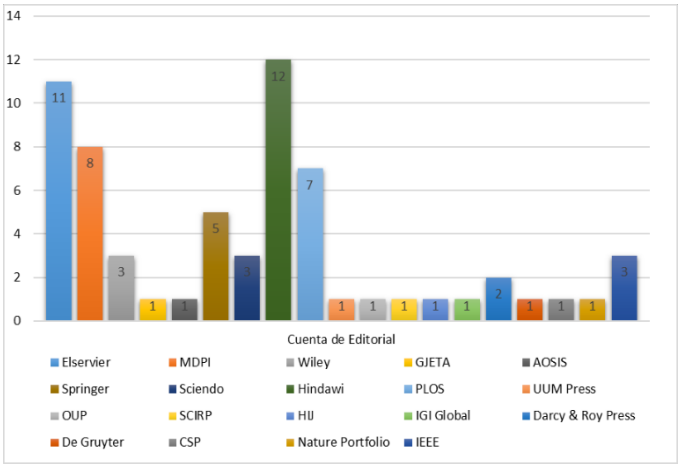


Fig. 3. Nº Total de artículos revisados según editorial de publicación.

En la Fig. 3 Número de artículos revisados por editorial. Wiley y Elsevier concentran el mayor número de publicaciones, con 12 y 11 respectivamente, seguidas por MDPI y Springer. La mayoría de las editoriales restantes presentan baja representación.

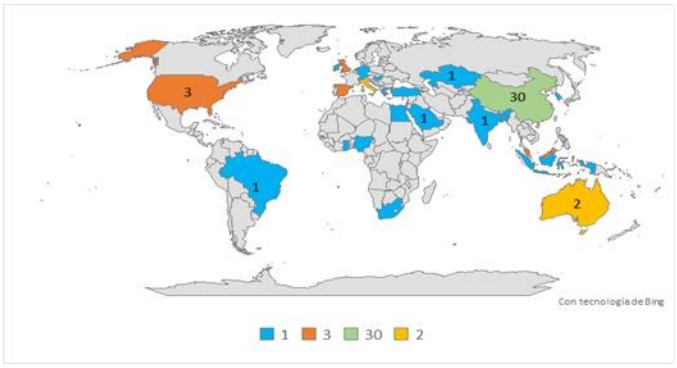


Fig. 4. Nº Total de artículos revisados según país de publicación.

En la Fig. 4 Número de artículos revisados por país. Mapa de distribución geográfica de los estudios incluidos en la revisión sistemática, destacando a China como principal país de publicación, seguido de contribuciones menores en otras regiones del mundo.

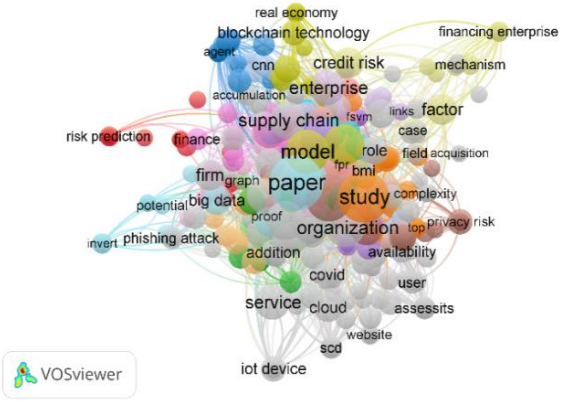


Fig. 5. Palabras clave obtenidas de la literatura científica.

La Fig. 5 presenta un mapa de coocurrencia de palabras clave cuyo objetivo es sintetizar la estructura temática de la literatura revisada. La centralidad de términos como model, study, organization, enterprise y supply chain, junto con nodos asociados a blockchain technology, phishing attack, big data, IoT device y privacy risk, permite identificar que las investigaciones se concentran en la gestión y mitigación de riesgos cibernéticos en entornos empresariales digitales.

TABLA V
EXTRACCIÓN DE DATOS DE ESTUDIOS CUALITATIVOS

Pregunta	Respuestas	Citas
¿En qué sector se identifican los ciberataques?	Sectores como finanzas, tecnología, logística, PYMES, servicios y ciberseguridad concentran los ciberataques.	[18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33],[74], [78]
¿Qué tipo de sistema es el objetivo del ciberataque?	Banca digital, SCADA, IoT, ERP, redes, facturación electrónica, DevOps, plataformas y modelos de negocio.	[34], [35], [18], [21], [36],[27],[37],[38], [30], [33], [39]
¿Qué actores son los más afectados por los ataques?	Usuarios, auditores, desarrolladores y empresarios de PYMES, resultan los principales afectados.	[40], [35], [18], [21], [27], [38],[28], [32], [24], [33], [31]
¿Qué estrategia de mitigación se propone o analiza el estudio?	Las estrategias incluyen auditoría interna, modelos predictivos, y evaluación de riesgos ,IA, análisis y gobernanza, adaptadas según el sector.	[41], [19], [34], [35], [27], [26], [38], [30], [29], [32], [24], [31], [73]
¿Qué herramienta tecnológica se aplica para mitigar el riesgo?	Se aplican tecnologías como IA, nube, Blockchain, autenticación, ERP, estadísticas, encuestas, modelado para gestionar el riesgo.	[34], [35], [21], [36], [27], [37], [22], [29], [32], [20], [74], [78]
¿Qué tipo de metodología se usa para implementar la mitigación?	Predominan enfoques como marcos conceptuales, modelo estructural, estudios de caso y modelos híbridos para aplicar mitigaciones.	[22], [36], [20], [24]
¿Qué resultado positivo se obtuvo con la estrategia aplicada?	Los estudios reportan mejor detección de amenazas, reducción de riesgos y control interno más eficiente.	[21], [20], [24]
¿Se reportan mejoras en seguridad de los sistemas de facturación electrónica?	Sí, se lograron mejoras en la seguridad operativa, disminución de incidentes y fortalecimiento de controles.	[41], [21], [24]
¿Qué indicadores o métricas se mencionan para medir los resultados?	Se emplearon métricas como reducción de errores, cumplimiento normativo e incidentes reportados para medir efectividad.	[21], [25], [24]

TABLA VI
EXTRACCIÓN DE DATOS DE ESTUDIOS CUANTITATIVOS

Pregunta	Respuestas	Citas
¿Cuál es el tipo de sistema o infraestructura tecnológica evaluada en el estudio?	Sistema IoT con microprocesador, plataformas P2P, infraestructura crítica, redes TI, auditoría financiera, Gestión de riesgos, Plataforma de comercio electrónico y sistemas de modelo contable financiero, fueron evaluados por su exposición al riesgo.	[42], [43], [44], [45], [46], [47], [48], [49], [76], [77]
¿Se reporta un tipo específico de ciberataque en el estudio?	Se identificaron ataques como fraude financiero, malware, escaneos automatizados, riesgos crediticios, fuga de datos biométricos.	[50], [51], [51], [52], [53], [75], [77]
¿El estudio se centra en un sector económico particular?	Los sectores abordados incluyen financiero, comercio electrónico, logística, banca, educación, sector público, tecnología.	[49], [48], [54], [55], [49], [56], [57], [58], [76], [79]
¿Qué tipo de estrategia de mitigación o defensa se implementó o evaluó?	Marco de cuantificación de riesgos, Evaluación de agilidad criptográfica, Modelo XGBoost-CNN-BiLSTM, Big Data + CNN, AENNER - software adaptativo con virtualización, Sistemas multiagente y Lenguaje de modelado para gestión de incidentes.	[59], [60], [61], [46], [62], [63], [44], [79]
¿Se aplicó alguna tecnología específica como IoT, Blockchain o Machine Learning?	Uso de IA y machine learning, blockchain y depp learning, aprendizaje profundo, IoT y big data, minería de datos, virtualización, Data Mining y redes neuronales	[50], [64], [61], [52], [65], [62], [65], [66]
¿La estrategia fue preventiva, reactiva o ambas?	Predomina el enfoque preventivo, Preventiva y Reactiva, previene brechas y responde a vulnerabilidades.	[67], [63], [68]
¿Se midió el nivel de reducción de riesgo o vulnerabilidad tras aplicar la estrategia?	Sí, con modelos DEMATEL-ISM que identifican causas raíz, matrices de riesgo y métricas CVSS, mejorando rendimiento del sistema IoT y benchmarking criptográfico.	[69], [62], [62], [61], [60]
¿El estudio indica una mejora en la detección o respuesta a incidentes?	Con alta precisión en fraude financiero, a través de evaluación en tiempo real y mejora dinámica por simulación MAS.	[50], [45], [63]
¿Se reportaron indicadores cuantitativos como tasas de éxito, precisión o tiempos de mitigación?	Mediante métricas de riesgo, F1-score, tasa de detección, precisión y recall del modelo, rendimiento del sistema y efectividad, eficiencia y valores de riesgo.	[66], [61], [70], [71], [47], [46], [49]

IV. DISCUSIONES

Los resultados obtenidos en esta revisión sistemática evidencian que las estrategias para mitigar ciberataques en sistemas de facturación electrónica priorizan enfoques de carácter preventivo, donde destacan tecnologías como el blockchain, la inteligencia artificial y modelos estructurados de evaluación de riesgos. Este resultado es consistente con lo

señalado en la Ref. [5], quienes destacan el uso de blockchain para garantizar la inmutabilidad de los datos, así como por la Ref. [6], quienes subrayan el impacto del aprendizaje automático en la mejora de la detección de intrusiones.

En relación con el componente de intervención del modelo PICO, se identificaron herramientas tecnológicas como redes neuronales convolucionales, plataformas de big data, análisis automatizado de vulnerabilidades y sistemas multiagente con virtualización dinámica [58]. Estas tecnologías han demostrado utilidad en la identificación temprana de patrones anómalos y la contención de amenazas en sistemas ERP y plataformas de facturación digital [61]. Sin embargo, algunos estudios advierten que su desempeño puede verse comprometido por la escasa calidad o el sesgo presente en los datos de entrenamiento, afectando la precisión de los modelos predictivos [72]. Además, la carencia de estándares comunes para cuantificar riesgos limita la interoperabilidad entre sectores y reduce la posibilidad de evaluar comparativamente la efectividad de distintas soluciones [71].

Respecto a los resultados dirigidos a los efectos obtenidos, los estudios revisados reportan mejoras en la resiliencia operativa, la reducción de incidentes y un mayor control en los procesos automatizados de facturación electrónica [21]. Estas mejoras fueron más evidentes cuando las estrategias se implementaron junto con políticas internas y marcos normativos consolidados [24]. El sector financiero ha logrado integrar herramientas de monitoreo en tiempo real y auditorías automatizadas [48]. Asimismo, el ámbito logístico y tecnológico ha incorporado prácticas de cifrado y respuesta proactiva [54]. En contraste, el sector retail evidencia una baja adopción tecnológica [31], y las pequeñas y medianas empresas presentan limitaciones en infraestructura, personal capacitado y políticas de seguridad [33].

En base al análisis realizado, se proponen tres líneas prioritarias para futuras investigaciones. Se requiere validar empíricamente la efectividad de las estrategias analizadas en entornos reales de facturación electrónica, considerando distintos niveles de madurez digital y exposición al riesgo [19]. Desarrollar marcos adaptativos que integren herramientas de predicción basadas en inteligencia artificial con normativas flexibles que respondan a contextos cambiantes [33]. Es urgente ampliar la cobertura de estudios en regiones subrepresentadas como América Latina, donde la acelerada digitalización convive con una infraestructura débil en términos de ciberseguridad fiscal [62].

La revisión también permitió identificar vacíos relevantes en la literatura. Se destaca la escasez de estudios longitudinales que evalúen la sostenibilidad de las estrategias en el tiempo, lo que impide conocer sus efectos acumulativos en el largo plazo [21]. También se evidencia una escasa inclusión de marcos legales y regulatorios en el desarrollo e implementación de las tecnologías propuestas [69]. Otro aspecto poco abordado es la dimensión organizacional: factores como la cultura institucional en seguridad, la concienciación del personal y la gestión del cambio han sido relegados frente a un enfoque predominantemente técnico [71]. Esta omisión limita la aplicabilidad real de muchas propuestas, dado que la resiliencia digital depende también de factores humanos y estructurales [7].

Estos vacíos sugieren la necesidad de estrategias más sostenibles [21], auditables [69] y acompañadas de capacitación, debido a la limitada atención a la dimensión organizacional y a los factores humanos [71], [7]. Esta demanda resulta especialmente crítica en contextos de baja madurez digital, como las PYMES y el sector retail [31], [33], y en regiones subrepresentadas [62].

Por último, deben reconocerse ciertas limitaciones metodológicas del presente estudio. La búsqueda de información se restringió a publicaciones disponibles en las bases de datos Scopus y Dimensions, lo que podría haber excluido estudios relevantes presentes en otras plataformas como Web of Science, ACM Digital Library o IEEE Xplore [15]. Además, se consideraron únicamente artículos publicados en inglés, lo cual puede haber dejado fuera literatura significativa escrita en español, portugués u otros idiomas regionales [16]. Esta restricción podría haber reducido la visibilidad de investigaciones realizadas en contextos latinoamericanos, donde se están dando avances importantes en el ámbito de la seguridad tributaria digital [17].

V. Conclusiones

La presente revisión sistemática permitió analizar el estado actual de las estrategias de mitigación de ciberataques en sistemas de facturación electrónica, con base en una muestra de 62 estudios seleccionados de las bases de datos Scopus y Dimensions. Desde un enfoque bibliométrico, se identificó una mayor concentración investigativa en países como China, Brasil, India y Estados Unidos, lo que refleja el liderazgo tanto de economías desarrolladas como emergentes en la producción científica vinculada a la ciberseguridad. Además, editoriales como Elsevier y Wiley destacaron por su alta frecuencia de publicación, reafirmando su papel clave en la divulgación académica sobre tecnologías aplicadas a sistemas de información y facturación digital.

En respuesta a la pregunta de investigación principal, se encontró que las estrategias de mitigación más frecuentes están orientadas a la prevención, con la aplicación de tecnologías como inteligencia artificial, blockchain, cifrado de extremo a extremo y modelos de aprendizaje profundo. Estas soluciones se implementan principalmente en infraestructuras como sistemas ERP, arquitecturas en la nube, plataformas web y servicios de facturación electrónica. Las amenazas más recurrentes fueron el phishing, el malware, la interceptación de datos y los fraudes por suplantación de identidad. Las tecnologías más utilizadas incluyen modelos predictivos como XGBoost y LSTM, mecanismos de detección de intrusos (IDS), herramientas de trazabilidad basadas en blockchain y sistemas de cifrado avanzado. En cuanto a los efectos observados, se reportaron mejoras en la resiliencia operativa, disminución de incidentes y mayor solidez en los mecanismos de control

interno. No obstante, la adopción tecnológica no ha sido uniforme: sectores como el financiero, logístico y tecnológico presentan mayores avances en implementación y madurez digital, mientras que el comercio minorista y las pequeñas y medianas empresas (PYMES) enfrentan limitaciones estructurales, normativas y de capacitación que incrementan su vulnerabilidad ante los ciberataques.

Asimismo, se identificaron vacíos relevantes en la literatura revisada. Existe una escasez de estudios longitudinales que evalúen el impacto sostenido de las estrategias aplicadas, lo que limita la comprensión de su efectividad a largo plazo. También se observó una limitada integración de marcos regulatorios y jurídicos en el diseño de soluciones tecnológicas, así como una débil atención a la dimensión organizacional, especialmente en lo relacionado con cultura de seguridad, concienciación del personal y gestión del cambio. Además, se detectó una clara brecha geográfica, dado que gran parte de los estudios se enfocan en contextos desarrollados, dejando de lado escenarios críticos como el latinoamericano, donde la digitalización avanza con rezagos estructurales.

Se recomienda priorizar investigaciones orientadas al diseño, validación e implementación de estrategias de mitigación de ciberataques en sistemas de facturación electrónica, especialmente en contextos con baja madurez digital como las PYMES, el sector retail y las regiones subrepresentadas. Estas estrategias deben trascender el enfoque estrictamente tecnológico e integrar de manera explícita criterios de cumplimiento normativo, auditabilidad, capacitación y fortalecimiento organizacional, dado que la resiliencia operativa depende tanto de la solidez técnica como de la preparación institucional. En esa línea, resultan necesarios estudios longitudinales y casos de aplicación en entornos reales que permitan determinar la sostenibilidad, efectividad y escalabilidad de las soluciones propuestas en diferentes escenarios empresariales.

REFERENCIAS

[1] M 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] A.K. Tiwari et. al., "Determinants of electronic invoicing technology adoption: Toward managing business information system transformation," Journal of Innovation & Knowledge, vol. 9, no. 1, 2024, doi: 10.1016/j.jik.2023.100366.

[3] D. Javaheri et al., "Cybersecurity threats in FinTech: A systematic review," Expert Systems with Applications, vol. 241, 2024, doi: 10.1016/j.eswa.2023.122697.

[4] Á. Longueira-Romero, R. Iglesias, J.L. Flores, I. Garitano, A novel model for vulnerability analysis through enhanced directed graphs and quantitative metrics, Sensors 22 (6) (2022) 2126, doi: 10.3390/s22062126.

[5] N. Moosavi y H. Taherdoost, "Blockchain technology application in security: A systematic review," Blockchains, vol. 1, no. 2, pp. 58–72, 2023, doi: 10.3390/blockchains1020005.

[6] M. A. Umar, Z. Chen, K. Shuaib, and Y. Liu, "Effects of feature selection and normalization on network intrusion detection," Data Science and Management, vol. 8, pp. 23-39, 2025, doi: 10.1016/j.dsm.2024.08.001.

[7] D. T. A. Wesley and A. V. Roth, "Developing a Culture of Cybersecurity," The International Journal of Technology, Knowledge, and Society, vol. 21, no. 1, pp. 29-48, 2025, doi: 10.18848/1832-3669/CGP/v21i01/29-48.

[8] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," Computers & Security, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.

[9] I. Makris et al., "A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions," Computer Science Review, vol. 56, p. 100717, 2025, doi: 10.1016/j.cosrev.2024.100717.

[10] Y. Dai, Q. Zhou, M. Leng, X. Yang, and Y. Wang, "Improving the Bi-LSTM model with XGBoost and attention mechanism: A combined approach for short-term power load prediction," Applied Soft Computing, vol. 130, p. 109632, Sep. 2022, doi: 10.1016/j.asoc.2022.109632.

[11] D. P. V. S, S. C. Sethuraman, and M. K. Khan, "Container security: Precaution levels, mitigation strategies, and research perspectives," *Computers & Security*, vol. 135, p. 103490, Sep. 2023, doi: 10.1016/j.cose.2023.103490.

[12] A.-T. Le, H. H. Huang, y T. K. Do, "Navigating through cyberattacks: The role of tax aggressiveness," Journal of Corporate Finance, vol. 88, art. no. 102649, Oct. 2024, doi: 10.1016/j.jcorpfin.2024.102649.

[13] N. Moosavi and H. Taherdoost, "Blockchain Technology Application in Security: A Systematic Review," Blockchains, vol. 1, no. 2, pp. 66–67, Oct. 2023, doi: 10.3390/blockchains1020005.

[14] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, y G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research", MethodsX, vol. 9, núm. 101895, p. 101895, 2022.

[15] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", Syst. Rev., vol. 10, núm. 1, p. 89, 2021.

[16] T. F. Frandsen, M. F. Bruun Nielsen, C. L. Lindhardt, y M. B. Eriksen, "Using the full PICO model as a search tool for systematic reviews resulted in lower recall for some PICO elements", J. Clin. Epidemiol., vol. 127, pp. 69–75, 2020.

[17] Page, M. J.; McKenzie, J. E.; Bossuyt, P. M.; Boutron, I., Hoffmann, T. C.; Mulrow, C. D.; Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting The BMJ, 372 doi:10.1136/bmj.n71.

[18] A. Abdurrahman, "Investigating the impact of digital business ecosystem in enhancing Islamic mobile banking adoption through the TOE framework," Digital Business, vol. 4, no. 2, Dec. 2024, doi: 10.1016/j.digbus.2024.100096.

[19] A. Barlybayev, A. Sharipbay, G. Shakhmetova, and A. Zhumadillayeva, "Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies," Applied Sciences (Switzerland), vol. 14, no. 21, Nov. 2024, doi: 10.3390/app14219858.

[20] B. Biswas, A. Mukhopadhyay, A. Kumar, and D. Delen, "A hybrid framework using explainable-AI (XAI) in cyber-risk management for defence and recovery against correlated phishing attacks A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks," 2023.

[21] Lucky Bamidele Benjamin, Ayodeji Enoch Adegbola, Prisca Amajuoyi, Mayokun Daniel Adegbola, and Kudirat Bukola Adeusi, "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies," Global Journal of Engineering and Technology Advances, vol. 19, no. 2, pp. 134–153, May 2024, doi: 10.30574/gjeta.2024.19.2.0084.

[22] J. Chen, Z. Li, W. Wang, Y. Wang, and Z. He, "Research on a Service Touchpoint Design Model Driven by Smart Technology Based on Kano–Failure Modes and Effects Analysis," Sensors, vol. 24, no. 23, Dec. 2024, doi: 10.3390/s24237854.

[23] A. Dash, S. P. Sarmah, M. K. Tiwari, S. K. Jena, and C. H. Glock, "Cybersecurity investments in supply chains with two-stage risk propagation," Comput Ind Eng, vol. 197, Nov. 2024, doi: 10.1016/j.cie.2024.110519.

[24] A. Asmah and M. Kyobe, "The impact of audit on IT governance: A study of the financial services sector in Ghana"" THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES, vol. 91, no. 1, Jan. 2025, doi: 10.1002/isd2.12349.

[25]L. Gu, "Optimized backpropagation neural network for risk prediction in corporate financial management," Sci Rep, vol. 13, no. 1, Dec. 2023, doi: 10.1038/s41598-023-46528-8.
[26]B. Huang and W. Gan, "Construction and application of computerized risk assessment model for supply chain finance under technology empowerment," PLoS One, vol. 18, no. 5 May, May 2023, doi: 10.1371/journal.pone.0285244.
[27]N. Alsafwani, Y. Fazea, and F. Alnajjar, "Strategic Approaches in Network Communication and Information Security Risk Assessment," Jun. 01, 2024, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/info15060353.
[28]J. R. Chivinge, S. Dube, and P. Ndayizigamiye, "Strategies used to address challenges encountered during website development in South Africa," SA Journal of Information Management, vol. 23, no. 1, Oct. 2021, doi: 10.4102/sajim.v23i1.1373.
[29]S. Facchinetti, S. A. Osmetti, and C. Tarantola, "A statistical approach for assessing cyber risk via ordered response models," Risk Analysis, vol. 44, no. 2, pp. 425–438, Feb. 2024, doi: 10.1111/risa.14186.
[30]M. A. Hossain, M. M. H. Chowdhury, I. O. Pappas, B. Metri, L. Hughes, and Y. K. Dwivedi, "Fake news on Facebook and their impact on supply chain disruption during COVID-19," Ann Oper Res, vol. 327, no. 2, pp. 683–711, Aug. 2023, doi: 10.1007/s10479-022-05124-1.
[31]N. Drydakis, "Artificial Intelligence and Reduced SMEs' Business Risks. A Dynamic Capabilities Analysis During the COVID-19 Pandemic", Information Systems Frontiers, vol. 24, no. 4, pp. 1223–1247, Aug. 2022, doi: 10.1007/s10796-022-10249-6.
[32]R. C. M. G. Goncalves and J. O. Imoniana, "Readiness of Low Complexity ERP for Continuous Auditing in SMEs: The Brazilian Case Study," Control and Cybernetics, vol. 51, no. 3, pp. 389–420, Sep. 2022, doi: 10.2478/candc-2022-0022.
[33]M. Wallang, M. D. K. Shariffuddin, and M. Mokhtar, "CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES (SMEs)," Journal of Governance and Development (JGD), vol. 18, no. 1, pp. 75–87, Dec. 2022, doi: 10.32890/jgd2022.18.1.5.
[34]A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations," Sensors, vol. 23, no. 9, May 2023, doi: 10.3390/s23094539.
[35]N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," Jan. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/s25010079.
[36]Y. Jingwen, A. A. Rahman, T. Tong, N. H. Kamarulzaman, and S. Bin Sidek, "A study of Chinese enterprises' business models to determine the impact of dynamic capabilities on innovation and performance," PLoS One, vol. 20, no. 1 January, Jan. 2025, doi: 10.1371/journal.pone.0310854.
[37]R. Alt, G. Fridgen, and Y. Chang, "The future of fintech — Towards ubiquitous financial services," Dec. 01, 2024, Springer Science and Business Media Deutschland GmbH. doi: 10.1007/s12525-023-00687-8.
[38]O. H. Plant, J. van Hillegersberg, and A. Aldea, "Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment," International Journal of Accounting Information Systems, vol. 45, Jun. 2022, doi: 10.1016/j.accinf.2022.100560.
[39]S. Hong, H. Wu, X. Xu, and W. Xiong, "Early Warning of Enterprise Financial Risk Based on Decision Tree Algorithm," Comput Intell Neurosci, vol. 2022, 2022, doi: 10.1155/2022/9182099.
[40]Y. Wang, R. Zhang, X. Zhang, and Y. Zhang, "Privacy Risk Assessment of Smart Home System Based on a STPA–FMEA Method," Sensors, vol. 23, no. 10, May 2023, doi: 10.3390/s23104664.
[41]M. Badawy, N. H. Sherief, and A. A. Abdel-Hamid, "Legacy ICS Cybersecurity Assessment Using Hybrid Threat Modeling—An Oil and Gas Sector Case Study," Applied Sciences (Switzerland), vol. 14, no. 18, Sep. 2024, doi: 10.3390/app14188398.
[42]D. Zhu, "A Fuzzy Comprehensive Evaluation and Random Forest Model for Financial Account Audit Early Warning," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/5425618.
[43]H. Zhao and Y. Wang, "A Big Data-Driven Financial Auditing Method Using Convolution Neural Network," *IEEE Access*, vol. 11, pp. 41492–41502, 2023, doi: 10.1109/ACCESS.2023.3269438.
[44]X. Xie, F. Zhang, L. Liu, Y. Yang, and X. Hu, "Assessment of associated credit risk in the supply chain based on trade credit risk contagion," *PLoS One*, vol. 18, no. 2 February, Feb. 2023, doi: 10.1371/journal.pone.0281616.
[45]Y. Zeng, "Neural Network Technology-Based Optimization Framework of Financial and Management Accounting Model," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/4991244.
[46]Y. Wang, "Intelligent cluster construction of internet financial security protection system in banking industry," *Open Computer Science*, vol. 13, no. 1, Jan. 2023, doi: 10.1515/comp-2022-0268.
[47] "Application of Python Automation Tool Combined with OCR Technology in 'Financial Checkup' of Universities," *Accounting and Corporate Management*, vol. 5, no. 12, 2023, doi: 10.23977/acccm.2023.051220.
[48]N. Taskin, A. Özkeleş Yıldırım, H. D. Ercan, M. Wynn, and B. Metin, "Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises," *Information (Switzerland)*, vol. 16, no. 1, Jan. 2025, doi: 10.3390/info16010066.
[49]L. Wang and H. Song, "E-Commerce Credit Risk Assessment Based on Fuzzy Neural Network," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/3088915.
[50]J. Wu, "A Security Assessment Strategy for Corporate Financial Systems Based on Data Mining Techniques," *Applied Mathematics and Nonlinear Sciences*, vol. 9, no. 1, Jan. 2024, doi: 10.2478/amns-2024-1880.
[51]Z. Ma, W. Hou, and D. Zhang, "A credit risk assessment model of borrowers in P2P lending based on BP neural network," *PLoS One*, vol. 16, no. 8 August, Aug. 2021, doi: 10.1371/journal.pone.0255216.
[52]W. Shi and Q. Huang, "The Blockchain Technology Applied in the Development of Real Economy in Jiangsu under Deep Learning," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/3088043.
[53]C. Xia, "Financial Security Risk Detection in Colleges and Universities Relying on Big Data Clustering Center Scheduling Algorithm," *Advances in Multimedia*, vol. 2022, 2022, doi: 10.1155/2022/1361041.
[54]A. G. Pérez, A. L. Martínez, and M. G. Pérez, "Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management," *Journal of Network and Computer Applications*, vol. 219, Oct. 2023, doi: 10.1016/j.jnca.2023.103728.
[55]C. Xinxian and C. Jianhui, "Digital Transformation and Financial Risk Prediction of Listed Companies," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/7211033.
[56]Z. Zuo, "Frontiers in Business, Economics and Management Development, Application, And Regulation of Web3.0."
[57]Q. Tang, "Research on the Risk Contagion Path and Prevention of Supply Chain Finance Based on DEMATEL-ISM Model," 2023.
[58]S. Muthaiyah, L. T. P. Nguyen, Y. V. Choong, and T. O. K. Zaw, "Orchestration of Federated Risk for P2P Lending Platforms: A Multi-Agent Systems (MAS) Approach," *HighTech and Innovation Journal*, vol. 5, no. 4, pp. 949–959, Dec. 2024, doi: 10.28991/HIJ-2024-05-04-06.
[59]L. Meng, "Using iot in supply chain risk management, to enable collaboration between business, community, and government," *Smart Cities*, vol. 4, no. 3, pp. 995–1003, Sep. 2021, doi: 10.3390/smartcities4030052.
[60]O. I. Odufisan, O. V. Abhulimen, and E. O. Ogunti, "Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria," *Journal of Economic Criminology*, vol. 7, p. 100127, Mar. 2025, doi: 10.1016/j.jeconc.2025.100127.
[61]X. Ma and Z. Wang, "Computer security technology in E-commerce platform business model construction," *Heliyon*, vol. 10, no. 7, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28571.
[62]T. C. Chen, Y. S. Liang, P. S. Ko, and J. C. Huang, "Optimization Model of Cross-Border E-commerce Payment Security by Blockchain Finance," *Wirel Commun Mob Comput*, vol. 2021, 2021, doi: 10.1155/2021/9192219.
[63]H. Li, "Embedded Microprocessor Wireless Communication Data Collection Aids in Early Warning of Default Risk for Internet Finance Bank Customers," *J Sens*, vol. 2021, 2021, doi: 10.1155/2021/1679907.
[64]Y. Li, J. Su, and D. Xiao, "Supply Chain Financial Risk Management under the Background of Wireless Multimedia Communication and Artificial Intelligence," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/9611699.

[65]H. S. Alwageed, I. Keshta, R. A. Khan, A. Alzahrani, M. U. Tariq, and A. Ghani, "An empirical study for mitigating sustainable cloud computing challenges using ISM-ANN," *PLoS One*, vol. 19, no. 9, Sep. 2024, doi: 10.1371/journal.pone.0308971.
[66]E. Murakami, T. Shionoya, S. Komenoi, Y. Suzuki, and F. Sakane, "Cloning and characterization of novel testis-Specific diacylglycerol kinase η splice variants 3 and 4," *PLoS One*, vol. 11, no. 9, Sep. 2016, doi: 10.1371/journal.pone.
[67]W. Zhang, H. Zhang, and Z. Deng, "Public attitude and media governance of biometric information dissemination in the era of digital intelligence," *Sci Rep*, vol. 15, no. 1, p. 2419, Dec. 2025, doi: 10.1038/s41598-025-86603-w.
[68]E. Kail, A. Riethné Nagy, R. Fleiner, A. Bánáti, and E. Rigó, "Low-impact, near real-time risk assessment for legacy IT infrastructures," *Int J Inf Secur*, vol. 24, no. 1, Feb. 2025, doi: 10.1007/s10207-024-00971-4.
[69]C. Ma, L. Colon, J. Dera, B. Rashidi, and V. Garg, "CARAF: Crypto Agility Risk Assessment Framework," *J Cybersecur*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab013.
[70]T. Li and J. Xu, "Research on Security Governance of Data Elements in the Context of Digitization," *Applied Mathematics and Nonlinear Sciences*, vol. 9, no. 1, Jan. 2024, doi: 10.2478/amns-2024-3119.
[71]A. Zadeh, B. Lavine, H. Zolbanin, and D. Hopkins, "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions," *Decision Analytics Journal*, vol. 9, Dec. 2023, doi: 10.1016/j.dajour.2023.100328.
[72]S. U. A. Rana, "Application of Data Mining Combined with K-means Clustering Algorithm in Enterprises' Risk Audit," Aug. 13, 2024. doi: 10.32388/G9G0S3.2.
[73]T. Wicaksono and C. B. Illés, "From resilience to satisfaction: Defining supply chain solutions for agri-food SMEs through quality approach," *PLoS One*, vol. 17, no. 2 February, Feb. 2022, doi: 10.1371/journal.pone.0263393.
[74]M. M. Rahman, N. Kshetri, S. A. Sayeed, and M. M. Rana, "<i>AssessITS</i>: Integrating Procedural Guidelines and Practical Evaluation Metrics for Organizational IT and Cybersecurity Risk Assessment," *Journal of Information Security*, vol. 15, no. 04, pp. 564–588, 2024, doi: 10.4236/jis.2024.154032.
[75]L. Allodi, F. Massacci, and J. Williams, "The Work-Averse Cyberattacker Model: Theory and Evidence from Two Million Attack Signatures," *Risk Analysis*, vol. 42, no. 8, pp. 1623–1642, Aug. 2022, doi: 10.1111/risa.13732.
[76]W. Bi and Y. Liang, "Risk Assessment of Operator's Big Data Internet of Things Credit Financial Management Based on Machine Learning," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/5346995.
[77]H. Zhou, G. Sun, S. Fu, L. Wang, J. Hu, and Y. Gao, "Internet Financial Fraud Detection Based on a Distributed Big Data Approach with Node2vec," *IEEE Access*, vol. 9, pp. 43378–43386, 2021, doi: 10.1109/ACCESS.2021.3062467.
[78]H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, and U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures," *Comput Secur*, vol. 128, May 2023, doi: 10.1016/j.cose.2023.103139.
[79]D. Ren and H. Wu, "Design and Implementation of Enterprise Financial Risk Control Information Management System Based on Big Data of Internet of Things," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/5677870.