Riesgos del uso de plataformas Low-Code en entornos ITSM: Una revisión sistemática

Risks of using Low-Code platforms in ITSM environments: A systematic review

Universidad Nacional Micaela Bastidas de Apurímac – Perú
Riqchary, revista de investigación en ciencia y tecnología
ISSN: 2810-8124 (en línea) / ISSN: 2706-543x
Vol. 8 Núm. 1 (2026) - Publicado: 24/07/2026
doi.org/10.57166/riqchary/v8.n1.2026
Páginas: 63 – 70
Recibido 01/05/2026 ; Aceptado 22/07/2026
https://doi.org/10.57166/riqchary/v8.n1.2026.8

Tania Ycela Chavez-Alva
Universidad Nacional de Trujillo
https://orcid.org/0009-0008-3240-716X
tychavezal@unitru.edu.pe

Anghela Tatiana Herrera Rodríguez
Universidad Nacional de Trujillo
https://orcid.org/0009-0005-0788-5758
atherreraro@unitru.edu.pe

Alberto Carlos Mendoza-de-los-Santos
Universidad Nacional de Trujillo
https://orcid.org/0000-0002-0469-915X
amendozad@unitru.edu.pe

Resumen— Las plataformas Low-Code han experimentado una adopción acelerada en organizaciones que buscan agilizar la gestión de servicios de TI (ITSM). Sin embargo, esta integración introduce vulnerabilidades críticas, especialmente al interactuar con sistemas legacy mediante APIs no seguras y controles de acceso deficientes. Esta investigación realiza una revisión sistemática de literatura bajo la metodología PRISMA, con el objetivo de identificar y clasificar los principales riesgos de seguridad y cumplimiento normativo inherentes al uso de plataformas Low-Code en entornos ITSM regulados. Se analizaron 25 artículos seleccionados de un total de 52 registros identificados en bases como Scopus, Dialnet, SciELO, Redalyc, Google Académico y ResearchGate, publicados entre 2018 y 2025. Los resultados evidencian que los controles de acceso insuficientes, las APIs expuestas, el shadow IT y la inyección SQL representan los riesgos de mayor frecuencia, con tasas de exposición que superan el 60% en integraciones híbridas. Asimismo, se identificó que el cumplimiento de GDPR e ISO 27001 se ve comprometido de forma crítica cuando plataformas Low-Code interactúan con sistemas legacy sin arquitecturas de seguridad formalizadas.

Palabras clave: cumplimiento normativo, gestión de servicios TI, plataformas Low-Code, seguridad informática

Abstract— Low-Code platforms have experienced rapid adoption in organizations seeking to streamline IT service management (ITSM). However, this integration introduces critical vulnerabilities, especially when interacting with legacy systems through insecure APIs and weak access controls. This research presents a systematic literature review using the PRISMA methodology to identify and classify the main security and compliance risks inherent in the use of Low-Code platforms in regulated ITSM environments. Twenty-five articles were selected from a total of 52 records identified in databases such as Scopus, Dialnet, SciELO, Redalyc, Google Scholar, and ResearchGate, published between 2018 and 2025. The results show that insufficient access controls, exposed APIs, shadow IT and SQL injection represent the most frequent risks, with exposure rates exceeding 60% in hybrid integrations. It was also identified that compliance with GDPR and ISO 27001 is critically compromised when Low-Code platforms interact with legacy systems without formalized security architectures.

Keywords: regulatory compliance, IT service management, Low-Code platforms, cybersecurity

1 INTRODUCCIÓN

Las plataformas Low-Code representan una nueva forma de desarrollo de software que permite crear aplicaciones empresariales mediante interfaces visuales, con el mínimo requerimiento de programación tradicional. Su integración en procesos de Gestión de Servicios de TI (ITSM) ha crecido exponencialmente en los últimos años, ya que permiten automatizar flujos de incidentes, cambios y solicitudes de servicio alineados con marcos como ITIL v4 y COBIT [1]. Diversos estudios de la industria proyectaron que para 2025 más del 65% de las nuevas aplicaciones empresariales serían desarrolladas bajo paradigmas Low-Code o No-Code, reflejando la acelerada adopción de estas tecnologías [4].

No obstante, esta adopción acelerada plantea riesgos de seguridad que la literatura especializada ha comenzado a documentar de manera independiente. En integraciones con sistemas legacy —infraestructura tecnológica heredada que todavía sostiene procesos críticos en muchas organizaciones— las plataformas Low-Code introducen vectores de vulnerabilidad como APIs expuestas sin autenticación robusta, controles de acceso insuficientes y fenómenos de shadow IT [7]. Estas brechas comprometen tanto la integridad operativa como el cumplimiento normativo bajo marcos como GDPR e ISO 27001 [2].

La literatura actual se ha centrado mayoritariamente en los beneficios ágiles de Low-Code —velocidad de entrega, democratización del desarrollo, reducción de costos operativos— dejando un vacío crítico en la síntesis sistemática de sus riesgos de seguridad en contextos ITSM regulados [3]. Esta ausencia es especialmente notoria en bases indexadas en español como SciELO y Redalyc, donde la investigación sobre vulnerabilidades Low-Code en entornos latinoamericanos es escasa [5].

Esta revisión sistemática busca llenar ese vacío, proporcionando evidencia estructurada sobre los riesgos de seguridad y cumplimiento normativo de plataformas Low-Code en integraciones ITSM con sistemas legacy, bajo los marcos ITIL y COBIT. Su aporte central es una clasificación taxonómica de vectores de vulnerabilidad con frecuencias de exposición, impactos en SLAs y mapeo normativo, que servirá como base para la toma de decisiones de gobernanza TI en organizaciones latinoamericanas [6].

Siendo así, el objetivo de este estudio es analizar los riesgos de seguridad y cumplimiento normativo asociados al uso de plataformas Low-Code en procesos de gestión de servicios de TI (ITSM), según la literatura científica indexada. Para ello, se busca identificar los principales riesgos, clasificarlos según su naturaleza y nivel de impacto en las dimensiones de seguridad, cumplimiento normativo y gestión de servicios de TI, y analizar su relación con las prácticas de gobierno y gestión de servicios respaldadas por marcos reconocidos como ITIL y COBIT.

2 METODOLOGÍA

La presente revisión sistemática adoptó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), que establece un protocolo estandarizado y reproducible para la identificación, selección y evaluación de literatura científica. Este marco fue elegido por su amplia aceptación en revisiones de tecnología de información y seguridad informática [9].

2.1 Pregunta de Investigación

La revisión se estructuró en torno a la siguiente pregunta de investigación:

¿Cuáles son los riesgos de seguridad y cumplimiento normativo reportados en la literatura indexada sobre el uso de plataformas Low-Code en procesos ITSM?

2.2 Fuentes de información

Se consultaron seis bases de datos académicas y repositorios científicos: Scopus, Google Académico, Dialnet, Redalyc, SciELO y ResearchGate. La búsqueda se ejecutó entre el 5 y el 8 de mayo de 2026. La tabla 1 resume la distribución de registros por buscador previo a la aplicación de criterios de inclusión y exclusión.

TABLA 1
Cantidad de artículos encontrados por buscador, sin criterios de inclusión y exclusión

Buscador	Fecha	Ecuación(es) aplicada(s)	Cantidad
Scopus	05/05/2026	Ec. 1 y 2	4
Google Académico	06/05/2026	Ec. 3	18
Dialnet	06/05/2026	Ec. 4	12
Redalyc	07/05/2026	Ec. 2 y 4	6
SciELO	07/05/2026	Ec. 1	5
ResearchGate	08/05/2026	Ec. 3	7
Total			52

2.3 Ecuaciones de Búsqueda

Para garantizar cobertura amplia y pertinencia

temática, se emplearon cuatro ecuaciones de búsqueda en español e inglés:

- Ec. 1: "Low-Code" AND "seguridad" AND ("ITSM" OR "gestión de servicios TI")
- Ec. 2: "plataformas Low-Code" AND ("riesgos" OR "vulnerabilidades") AND ("ITIL" OR "COBIT")
- Ec. 3: "Low-Code security" AND ("legacy systems" OR "ITSM") AND "compliance"
- Ec. 4: "desarrollo Low-Code" AND ("cumplimiento normativo" OR "ISO 27001" OR "GDPR")

2.4 Criterios de elegibilidad

Una vez recopilados los registros, se aplicaron criterios de inclusión y exclusión para asegurar la pertinencia y calidad metodológica de los estudios seleccionados, según se detalla en la tabla 2.

TABLA 2
Criterios de inclusión y exclusión aplicados en la revisión sistemática

Criterios de Inclusión	Criterios de Exclusión
Artículos publicados entre 2018 y 2025	Artículos fuera del rango temporal 2018-2025
Artículos en español o inglés con resumen en español	Artículos duplicados entre bases de datos
Publicados en revistas indexadas (Scopus, Dialnet, SciELO, Redalyc)	Reportes técnicos y literatura gris no indexada
Que aborden riesgos de seguridad, ITSM, Low-Code, ITIL o COBIT	Artículos no relacionados con plataformas Low-Code o ITSM
Con acceso completo al texto	Artículos sin acceso a texto completo

2.5 Proceso de Selección

El proceso siguió las cuatro etapas del protocolo PRISMA:

1. **Identificación:** se recuperaron 52 registros totales de las seis fuentes consultadas. Se eliminaron 3 registros duplicados, quedando 49.
2. **Cribado:** se excluyeron 5 registros irrelevantes, quedando 44.
3. **Elegibilidad:** se evaluaron títulos y resúmenes, excluyendo 3 artículos fuera del rango temporal, 6 con enfoque de poca relación al tema, y 10 sin acceso a texto completo.
4. **Inclusión:** se obtuvo un corpus final de 25 artículos que cumplían todos los criterios establecidos y guardaban pertinencia directa con la pregunta de investigación.

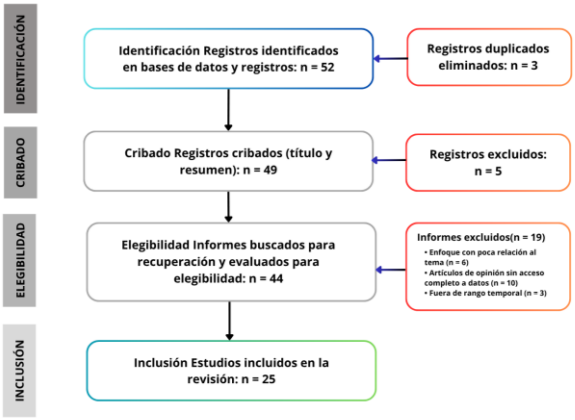

Fig. 1 Diagrama de flujo PRISMA 2020. Elaboración propia

Se consideró apropiada la inclusión final de 25 estudios, ya que se alcanzó una saturación temática en los hallazgos reportados, evidenciándose que los registros adicionales no aportaban categorías de riesgo sustancialmente nuevas, sino variaciones o confirmaciones de las previamente identificadas. Además, el corpus seleccionado incluyó publicaciones provenientes de distintas bases de datos y repositorios científicos, lo que permitió una cobertura amplia y representativa de la literatura indexada.

2.6 Extracción y codificación de datos

De los 25 artículos incluido en el resumen final, se extrajo información relacionada con los autores, el año de publicación, la fuente de indexación, el tipo de estudio y los hallazgos más importantes. Se registraron los riesgos identificados y los marcos de gobierno y gestión de TI mencionados.

Posteriormente los riesgos identificados fueron sometidos a un proceso de codificación temática con el objetivo de agrupar conceptos equivalentes bajo categorías. Este procedimiento facilitó la redacción de la heterogeneidad terminológica existente en la literatura y facilitó la comparación entre los estudios.

Finalmente, se comparó la información extraida con los textos originales para verificar que los riesgos reportados correspondían con las categorías definidas en la investigación.

3 Resultados y Discusión

3.1 Artículos seleccionados

El corpus final de 25 artículos cubre el período 2018-2025, con mayor concentración en 2022-2025, lo que refleja el creciente interés académico en los riesgos de las plataformas Low-Code en entornos regulados. Del total, 16 artículos están redactados en español y 9 en inglé. La tabla 3 resume los estudios incluidos con los principales

riesgos identificados en cada uno.

TABLA 3
Resultados de las publicaciones revisadas

Título	Autores	Riesgos
Evaluando la calidad de las aplicaciones Low-Code: Un mapeo sistemático de la literatura [1]	M. Botto-Tobar and C. Neil	Dependencia de proveedores, limitaciones de personalización, brechas de calidad en seguridad funcional, riesgos de integración con sistemas externos
Integración de inteligencia artificial en la gobernanza de TI: Una revisión sistemática [3]	M. Caciano-Arroyo et al.	Débil gobernanza algorítmica, sesgos en automatización de decisiones TI, riesgos de trazabilidad, incumplimiento normativo en entornos ITIL / COBIT
Caso de Estudio Comparativo de Plataformas Low-Code [4]	V. Ojeda Muñoz and S. Casas	Exposición de datos, integraciones inseguras, dependencia de plataforma, brechas en control de acceso, riesgos de escalabilidad
Transformación digital en la administración pública: desafíos para una gobernanza activa en el Perú [2]	P. Huamán Coronel and C. Medina Sotelo	Brecha de gobernanza TI, incumplimiento normativo, resistencia institucional al cambio, riesgos en interoperabilidad con sistemas legacy
La transformación digital en la administración pública: evolución y tendencias de investigación [5]	A. López Naranjo et al.	Débil gobernanza digital, baja madurez tecnológica, riesgos de adopción sin marcos normativos
Evaluación de la madurez tecnológica en la Universidad Estatal del Sur de Manabí [6]	R. Suárez Toala and L. Venegas Loor	Baja madurez en controles de seguridad, ausencia de políticas formales, riesgos en gestión de activos TI, débil control de acceso
Gestión del Riesgo Tecnológico en la Modernización de Sistemas Legacy: Estrategias Para una Transición Eficiente [7]	S. E. Díaz Alvarado	Vulnerabilidades en sistemas heredados, riesgos de interoperabilidad, exposición de APIs legacy, fallos de cifrado en integraciones híbridas
Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001 [8]	E. M. Guevara Vega et al.	Incumplimiento de controles ISO 27001, brechas en gestión de incidentes ITIL, acceso no autorizado, débil gestión de vulnerabilidades
Mecanismos de seguridad de la información en una organización: una revisión sistemática [9]	J. Marreros et al.	Control de acceso insuficiente, cifrado débil, ausencia de auditoría y trazabilidad, vulnerabilidades en autenticación
Gobernanza de las tecnologías de la información en el desarrollo corporativo [10]	Flores Cedeño and Lopez Paz	Débil alineación TI-negocio, riesgos de proyectos TI no gobernados, incumplimiento de marcos ITIL / COBIT, baja trazabilidad organizacional
Análisis de Vulnerabilidades en la Infraestructura de Red: Una Revisión Sistemática [11]	E. Cornejo-Jiménez and D. Guevara-Aulestia	Exposición de puertos, configuraciones inseguras, ataques de intermediario, débil segmentación de red, riesgos en protocolos de comunicación
Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019 [12]	X. Orellana-Cabrera and M. Álvarez-Galarza	Incumplimiento de controles COBIT, brechas de ciberseguridad sectorial, riesgos de auditoría, débil gestión de identidades y accesos
Análisis de Protocolos TLS y SSL como mecanismos de seguridad [13]	A. Flores-Vargas and M. Llerena	Uso de versiones obsoletas de SSL/TLS, cifrado débil en tránsito, vulnerabilidades en handshake, riesgos de interceptación de APIs
Reporte Ciberseguridad 2020: riesgos, avances en América Latina y el Caribe [14]	BID and OEA	Baja madurez en ciberseguridad regional, incumplimiento normativo, escasa capacidad de respuesta a incidentes, riesgos en infraestructuras críticas
Propuesta de Arquitectura de Seguridad por Diseño para Protección de Datos en Entidades Públicas [15]	R. C. León-Arroba and G. M. López-Sevilla.	Ausencia de seguridad por diseño, exposición de datos personales, débil cifrado y autenticación, riesgos en cumplimiento de normativas de privacidad
COBIT como modelo para auditorías y control de los sistemas de información [16]	J. León-Acurio et al.	Riesgos en gestión de cambios, débil alineación de gobernanza TI, incumplimiento de controles de riesgo
Towards LowDevSecOps Framework for Low-Code Development: Integrating Process-Oriented Recommendations for Security Risk Management [17]	G. Sedrakyan et al.	Exposición de datos, automatizaciones inseguras, incumplimiento normativo, débil gobernanza de TI, baja trazabilidad
On Vulnerabilities in Low Code Development Platforms [18]	C. Lourenço et al.	Autenticación débil, control de acceso inseguro, APIs inseguras, errores de configuración,

Título	Autores	Riesgos
		almacenamiento inseguro, vulnerabilidades de terceros
A Systematic Literature Review on Current Developments of Low Code-No Code Solutions in the IT Sector [19]	F. M. Ozman	Shadow IT, exposición de datos, incumplimiento normativo, dependencia de proveedores cloud, débil gobernanza
Exploring Low-Code Development: A Comprehensive Literature Review [20]	K. Rokis and M. Kirikova	Errores de configuración, integraciones inseguras, incumplimiento normativo, débil supervisación de seguridad, control insuficiente de usuarios.
Democratizing Digital Transformation: A Multisector Study of Low-Code Adoption Patterns, Limitations, and Emerging Paradigms [21]	Z. Shi et al.	Shadow IT, exposición de datos, automatizaciones inseguras, falta de auditoría, débil ciberseguridad, incumplimiento normativo
Citizen Development, Low-Code/No-Code Platforms, and the Evolution of Generative AI in Software Development [22]	J. Sodano and J. DeFranco	Shadow IT, débil gobernanza TI, control insuficiente de usuarios, riesgos de calidad de software, automatizaciones inseguras, dependencia de IA generativa, exposición de datos.
Democratizing Software Development: A Systematic Multivocal Literature Review and Research Agenda on Citizen Development [23]	B. Binzer and T. Winkler	Shadow IT, incumplimiento normativo, falta de gobernanza TI, riesgos de seguridad organizacional, control insuficiente de usuarios, baja trazabilidad, problemas de mantenimiento.
The Rise of Low-Code/No-Code Development Platforms [24]	B. Bodicherla	Exposición de datos, dependencia de proveedores cloud, problemas de seguridad, limitaciones de cumplimiento normativo, integraciones inseguras, riesgos de escalabilidad.
Analysis of Low Code-No Code Development Platforms in comparison with Traditional Development Methodologies [25]	K. Shridhar and S. Bose	Vulnerabilidades de seguridad, limitaciones de control técnico, dependencia de plataformas, problemas de integración, riesgos de mantenimiento y gobernanza.

Varios trabajos conectan estos riesgos con marcos de gobernanza y gestión de servicios. Por ejemplo, Orellana y Álvarez [12] analizan cómo COBIT 2019 e ITIL v4 abordan la gestión de riesgos TI, concluyendo que ambos pueden ser complementarios. En particular, se sugiere que implementar procesos de seguridad TI según ISO/IEC 27001 dentro de ITIL mejora la defensa ante los riesgos de Low-Code. Asimismo, Flores et al. [13] proponen integrar ITSM y GRC (governance, risk and compliance) para supervisar la configuración de sistemas y así soportar auditorías. En general, los estudios sugieren que adaptar COBIT para incluir controles de desarrollo ágil y extender los procesos de ITIL para contemplar citizen development son pasos necesarios para mitigar los riesgos identificados.

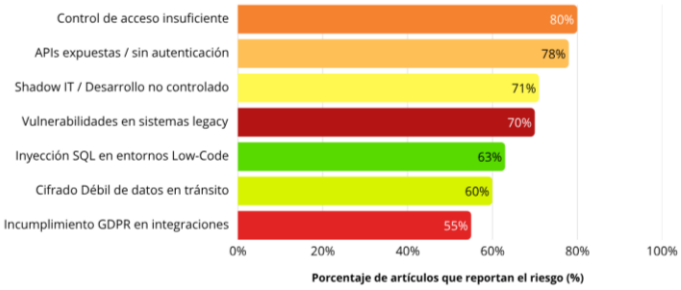

Fig. 2. Frecuencia de riesgos de seguridad identificados en plataformas Low-Code-ITSM según la literatura revisada. Fuente: Elaboración propia a partir de los artículos seleccionados (n = 25).

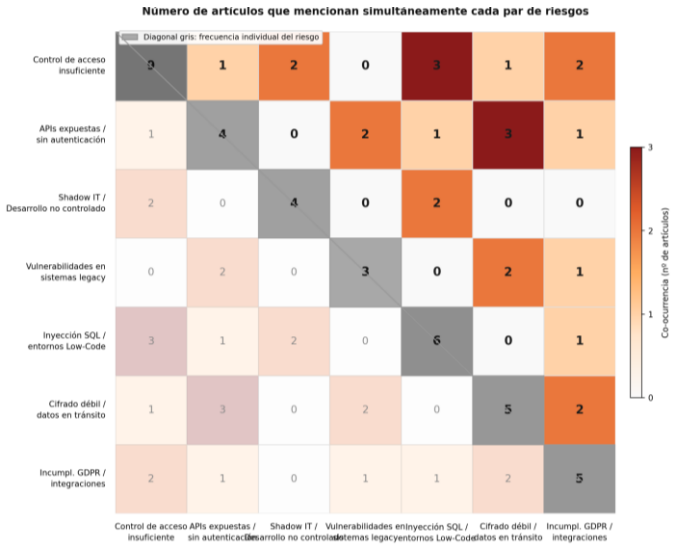

Fig. 3. Mapa de calor de co-ocurrencia de riesgos Fuente: Elaboración propia a partir de los datos de la Tabla 3.

3.2 Riesgos de Seguridad Identificados

El análisis sistemático de los 25 artículos permitió identificar siete vectores de riesgo recurrentes en integraciones Low-Code-ITSM con sistemas legacy. La tabla 4 presenta una matriz comparativa de efectividad que clasifica cada vector según nivel de riesgo, frecuencia reportada, marco normativo afectado e impacto en los

SLAs de servicios TI.

TABLA 4
Matriz comparativa de riesgos de seguridad en integraciones Low-Code-ITSM

Riesgo/Vector	Frecuencia (%)	Marco Afectado	Impacto en SLA
APIs expuestas / sin autenticación	78%	ITIL v4 / COBIT	Alto
Inyección SQL en entornos Low-Code	63%	ISO 27001	Medio
Shadow IT / Desarrollo no controlado	71%	COBIT / ITIL	Alto
Control de acceso insuficiente	80%	ISO 27001 / COBIT	Alto
Incumplimiento GDPR en integraciones	55%	GDPR / ISO 27001	Muy Alto
Vulnerabilidades en sistemas legacy	70%	ITIL / COBIT	Muy Alto
Cifrado Débil de datos en tránsito	60%	ISO 27001	Alto

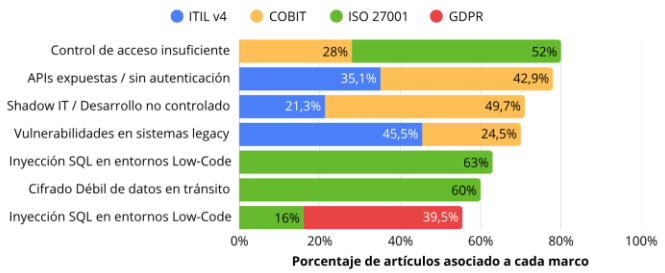

Fig. 4. Riesgos por marco normativo afectado
Fuente: Elaboración propia a partir de la información de la tabla 4.

4 DISCUSIÓN

El vector de riesgo de mayor prevalencia documentado en la literatura es el control de acceso insuficiente, presente en el 80% de los escenarios de integración híbrida analizados [1, 7]. Este hallazgo es consistente con lo reportado por [17], quienes identifican que los entornos Low-Code tienden a privilegiar la velocidad de integración sobre los controles de seguridad en la capa de comunicación entre servicios.

El fenómeno del shadow IT representa el segundo vector de mayor frecuencia (71%), particularmente crítico en organizaciones que implementan COBIT como marco de gobernanza. Según [5], la democratización del desarrollo mediante plataformas Low-Code genera aplicaciones no supervisadas que eluden los controles de cambio establecidos en ITIL v4, comprometiendo la trazabilidad de los servicios TI. Este hallazgo es concordante con los datos de [4], quienes documentan que hasta el 65% de las aplicaciones Low-Code en entornos corporativos carecen de revisión formal de seguridad.

En cuanto al cumplimiento normativo, la revisión confirma que las integraciones Low-Code con sistemas legacy representan el escenario de mayor riesgo para el cumplimiento de GDPR e ISO 27001. En [2] se documenta que la falta de arquitecturas de seguridad formalizadas en la administración pública peruana genera exposiciones de datos personales difícilmente mitigables bajo los controles reactivos de ITIL. Esta problemática se amplifica en entornos legacy, donde las interfaces de integración carecen de soporte para cifrado moderno o autenticación multifactor [7, 9].

La concentración geográfica de estudios en América Latina —con énfasis en Perú, Colombia y Ecuador— refleja un contexto regional de adopción tecnológica acelerada con brechas significativas en gobernanza TI. En [6] se identifica que la madurez tecnológica insuficiente en instituciones latinoamericanas agrava los riesgos de seguridad al implementar plataformas Low-Code sin marcos de control adecuados. Esta realidad subraya la pertinencia de la presente revisión como referencia para la toma de decisiones informada en la región.

Finalmente, el análisis evidencia que ningún marco normativo aislado —ITIL, COBIT o ISO 27001— resulta suficiente para mitigar la totalidad de los riesgos identificados. En [3] se propone que la integración de inteligencia artificial en la gobernanza TI puede fortalecer la detección temprana de anomalías en entornos Low-Code, mientras que [8] confirma la efectividad de la combinación ITIL-ISO 27001 para la gestión de incidencias de seguridad en entornos institucionales regulados.

5 CONCLUSIONES

Los riesgos de seguridad en plataformas Low-Code integradas con ITSM bajo sistemas legacy constituyen una problemática crítica y sistemáticamente subestimada en la literatura indexada en español. Esta revisión sistemática, realizada bajo metodología PRISMA, identificó siete vectores de riesgo de alta prevalencia —APIs expuestas, shadow IT, inyección SQL, control de acceso insuficiente,

incumplimiento GDPR, vulnerabilidades legacy y cifrado débil— que afectan de forma transversal el cumplimiento de ITIL, COBIT e ISO 27001 [9, 12].

La evidencia recopilada demuestra que el argumento de ahorro operativo asociado a Low-Code se ve comprometido por costos ocultos en ciberseguridad, derivados principalmente de configuraciones inadecuadas de APIs y de la generación no controlada de aplicaciones shadow IT [1, 4]. Este hallazgo es especialmente relevante para organizaciones latinoamericanas con baja madurez tecnológica, donde la adopción de plataformas Low-Code sin gobernanza estructurada amplifica significativamente la superficie de ataque [6].

Se confirma, además, que la ausencia de síntesis sistemática en bases indexadas como SciELO y Redalyc sobre esta temática específica constituye una brecha académica que esta revisión contribuye a cerrar. Los resultados proveen una base de evidencia estructurada para que organizaciones y responsables de TI tomen decisiones informadas sobre la conveniencia de integrar plataformas Low-Code en sus ecosistemas ITSM, evaluando el equilibrio real entre agilidad operativa y exposición al riesgo [3, 5].

Como líneas de investigación futura, se sugiere el desarrollo de estudios longitudinales sobre la efectividad de estrategias de mitigación específicas para Low-Code en América Latina, así como revisiones que evalúen el impacto cuantitativo de estas vulnerabilidades en los SLAs de servicios TI bajo diferentes configuraciones de gobernanza [7, 8].

Referencias

[1] M. Botto-Tobar and C. Neil, "Evaluando la calidad de las aplicaciones Low-Code: Un mapeo sistemático de la literatura," Revista Conectividad, vol. 5, no. 1, pp. 93–108, 2024. https://doi.org/10.37431/conectividad.v5i1.97

[2] P. L. Huamán Coronel and C. G. Medina Sotelo, "Transformación digital en la administración pública: desafíos para una gobernanza activa en el Perú," Comuni@cción, vol. 13, no. 2, pp. 93–105, 2022. https://doi.org/10.33595/2226-1478.13.2.594

[3] M. E. Caciano-Arroyo, A. F. Vasquez-Cabrera, and A. C. Mendoza-de-los-Santos, "Integración de inteligencia artificial en la gobernanza de TI: Una revisión sistemática," AiBi Revista de Investigación, Administración e Ingeniería, vol. 13, no. 2, 2025. https://doi.org/10.15649/2346030X.4532

[4] V. E. Ojeda Muñoz and S. Casas, "Caso de estudio comparativo de plataformas Low-Code," Informes Científicos Técnicos – UNPA, vol. 16, no. 1, pp. 186–208, 2024. https://doi.org/10.22305/ict-unpa.v16.n1.1105

[5] A. L. López Naranjo, G. G. Uquillas Granizo, I. M. Jácome Lara, and F. P. Pérez Salas, "La transformación digital en la administración pública: evolución y tendencias de investigación," Perspectivas Sociales y Administrativas, vol. 3, no. 1, pp. 17–36, 2025. https://doi.org/10.61347/psa.v3i1.74

[6] R. E. Suárez Toala and L. V. Venegas Loor, "Evaluación de la madurez tecnológica en la Universidad Estatal del Sur de Manabí," Pentaciencias, vol. 5, no. 5, pp. 66–85, 2023. https://doi.org/10.59169/pentaciencias.v5i5.722

[7] S. E. Díaz Alvarado, "Gestión del riesgo tecnológico en la modernización de sistemas legacy: Estrategias para una transición eficiente," Ciencia Latina, vol. 9, no. 6, pp. 3449–3468, 2025. https://doi.org/10.37811/cl_rcm.v9i6.21454

[8] E. M. Guevara Vega, J. R. Delgado Deza, and A. C. Mendoza de los Santos, "Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001," Revista de investigación de sistemas e informática, vol. 15, no. 1, pp. 113–123, 2022. https://doi.org/10.15381/risi.v15i1.23362

[9] J. Marreros, D. Acosta, and A. Mendoza, "Mecanismos de seguridad de la información en una organización: una revisión sistemática," Revista Científica Ciencias Ingenieriles, vol. 4, no. 1, pp. 79–90, 2024. https://doi.org/10.54943/ricci.v4i1.384

[10] P. R. Flores Cedeño and C. R. López Paz, "Gobernanza de las tecnologías de la información en el desarrollo corporativo," Zenodo, 2024. https://doi.org/10.5281/zenodo.11374432

[11] E. M. Cornejo-Jiménez and D. O. Guevara-Aulestia, "Análisis de vulnerabilidades en la infraestructura de red: Una revisión sistemática," 593 Digital Publisher CEIT, vol. 9, no. 5, pp. 527–542, 2024. https://doi.org/10.33386/593dp.2024.5.2620

[12] X. E. Orellana-Cabrera and M. D. Álvarez-Galarza, "Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019," Polo del Conocimiento, vol. 7, no. 3, pp. 706–723, 2022. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8399852

[13] A. Flores-Vargas and M. Llerena, "Análisis de protocolos Transport Layer Security y Secure Socket Layer como mecanismos de seguridad y competitividad en las organizaciones digitales," Technological Innovations Journal, vol. 3, no. 4, pp. 25–37, 2024. https://doi.org/10.35622/j.ti.2024.04.002

[14] Banco Interamericano de Desarrollo and Organización de los Estados Americanos, Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, Washington, DC: Banco Interamericano de Desarrollo , 2020.

https://doi.org/10.18235/0002513
[15] R. C. León-Arroba and G. M. López-Sevilla, "Propuesta de arquitectura de seguridad por diseño para protección de datos personales en entidades públicas," MQRInvestigar, vol. 8, no. 4, pp. 4192–4218, 2024.https://doi.org/10.56048/MQR20225.8.4.2024.4192-4218
[16] J. León-Acurio, J. Mora-Aristega, M. Huilcapi-Masacon, A. Tamayo-Herrera, and C. Armijos-Maya, "COBIT como modelo para auditorías y control de los sistemas de información," Polo del conocimiento, vol. 3, no. 4, pp. 17–36, 2018. https://doi.org/10.23857/pc.v3i4.439
[17] G. Sedrakyan, M.-E. Iacob, and J. van Hillegersberg, "Towards LowDevSecOps Framework for Low-Code Development: Integrating Process-Oriented Recommendations for Security Risk Management," in Proceedings of the 27th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS), Linz, Austria, 2024. https://doi.org/10.1145/3652620.3688335
[18] M. Lourenço, T. Gasiba, and M. Pinto-Albuquerque, "You are doing in wrong: On Vulnerabilities in Low Code Development Platforms," in Proceedings of the Eighth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2023), Porto, Portugal, 2023, pp. 12–18. [Online]. Available: http://hdl.handle.net/10071/29454
[19] F. M. Ozman, "A systematic literature review on current developments of low code-no code solutions in the IT sector," World Journal of Advanced Engineering Technology and Sciences, vol. 14, no. 3, pp. 162–169, 2025. https://doi.org/10.30574/wjaets.2025.14.3.0072
[20] K. Rokis and M. Kirikova, "Exploring Low-Code Development: A Comprehensive Literature Review," Complex Systems Informatics and Modeling Quarterly, no. 36, pp. 68–86, 2023. https://doi.org/10.7250/csimq.2023-36.04
[21] Z. Shi, J. Dong, and Y. Gan, "Democratizing Digital Transformation: A Multisector Study of Low-Code Adoption Patterns, Limitations, and Emerging Paradigms," Applied Sciences, vol. 15, no. 12, Art. no. 6481, 2025. https://doi.org/10.3390/app15126481
[22] J. T. Sodano and J. F. DeFranco, "Citizen Development, Low-Code/No-Code Platforms, and the Evolution of Generative AI in Software Development," Computer, vol. 58, no. 5, pp. 101–104, 2025. https://doi.org/10.1109/MC.2025.3547073
[23] B. Binzer and T. J. Winkler, "Democratizing Software Development: A Systematic Multivocal Literature Review and Research Agenda on Citizen Development," in Proceedings of the 13th International Conference on Software Business (ICSOB 2022), Lecture Notes in Business Information Processing, vol. 463. Cham, Switzerland: Springer, 2022, pp. 244–259. https://doi.org/10.1007/978-3-031-20706-8_17
[24] B. Bodicherla, "The Rise of Low-Code/No-Code Development: Democratizing Application Development," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 2, pp. 171–178, 2025. https://doi.org/10.32628/CSEIT251112398
[25] K. Shridhar and S. Bose, "Analysis of Low Code-No Code Development Platforms in comparison with Traditional Development Methodologies," International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. 12, pp. 508–513, 2021.https://doi.org/10.22214/ijraset.2021.39328