# Enhancing Cybersecurity Resilience in SMEs: A Governance Model for Third-Party Risk and AI-Enabled Services

Diego Bolatti [1*], Javier Diaz [2], and Veronica A. Bollati [3]

[1] Universidad Tecnológica Nacional, Facultad Regional Resistencia, Argentina
dbolatti@gfe.frre.utn.edu.ar
[2] Universidad Nacional de La Plata, Argentina
jdiaz@unlp.edu.ar
[3] Universidad Tecnológica Nacional, Facultad Regional Resistencia, CONICET, Argentina
vbollati@ca.frre.utn.edu.ar

**Abstract.** This paper addresses the growing cybersecurity risks faced by small and medium-sized enterprises (SMEs) due to their increasing dependence on third-party and outsourced services. While international frameworks such as ISO/IEC 27036, NIST SP 800-161, CIS Controls, and the Cloud Security Alliance Cloud Controls Matrix provide structured approaches to supply chain risk management, their direct adoption remains challenging for SMEs due to resource constraints and limited cybersecurity maturity.

The study analyzes the applicability of these frameworks in SME environments and identifies key barriers that hinder their implementation, including lack of expertise, informal supplier management practices, and limited governance capabilities. In addition, the paper examines the impact of Artificial Intelligence (AI) as an emerging risk factor within third-party ecosystems, highlighting issues such as lack of transparency, data dependency, and model vulnerabilities.

Based on this analysis, a simplified and scalable governance model is proposed, structured around six core pillars and aligned with international standards, including the NIST Artificial Intelligence Risk Management Framework (AI RMF). The model integrates traditional cybersecurity practices with AI-related risk considerations and is designed to support progressive implementation according to SME capabilities.

The proposed model is conceptual and has not yet been validated through empirical implementation. Future work will focus on pilot applications in SME environments to evaluate its effectiveness, scalability, and adaptability in real-world contexts.

**Keywords:** cybersecurity, SMEs, third-party risk, supply chain security, AI governance, risk management.

* Corresponding author: dbolatti@gfe.frre.utn.edu.ar

# Mejorando la Resiliencia en Ciberseguridad de las PyMEs: Un Modelo de Gobernanza para el Riesgo de Terceros y Servicios Habilitados por IA

**Abstract.** Este artículo aborda los crecientes riesgos de ciberseguridad que enfrentan las pequeñas y medianas empresas (PyMEs) debido a su creciente dependencia de servicios de terceros y externalizados. Si bien marcos internacionales como ISO/IEC 27036, NIST SP 800-161, los CIS Controls y la Cloud Controls Matrix de la Cloud Security Alliance proporcionan enfoques estructurados para la gestión de riesgos de la cadena de suministro, su adopción directa sigue siendo un desafío para las PyMEs debido a las limitaciones de recursos y a la madurez limitada en ciberseguridad.

El estudio analiza la aplicabilidad de estos marcos en entornos de PyMEs e identifica las principales barreras que dificultan su implementación, incluyendo la falta de experiencia, las prácticas informales de gestión de proveedores y las capacidades limitadas de gobernanza. Además, el trabajo examina el impacto de la Inteligencia Artificial (IA) como un factor de riesgo emergente dentro de los ecosistemas de terceros, destacando problemas como la falta de transparencia, la dependencia de datos y las vulnerabilidades de los modelos.

A partir de este análisis, se propone un modelo de gobernanza simplificado y escalable, estructurado en torno a seis pilares centrales y alineado con estándares internacionales, incluyendo el Marco de Gestión de Riesgos de Inteligencia Artificial del NIST (AI RMF). El modelo integra prácticas tradicionales de ciberseguridad con consideraciones de riesgo relacionadas con la IA y está diseñado para apoyar una implementación progresiva según las capacidades de cada PyME.

El modelo propuesto es de carácter conceptual y aún no ha sido validado mediante implementación empírica. El trabajo futuro se enfocará en aplicaciones piloto en entornos de PyMEs para evaluar su efectividad, escalabilidad y adaptabilidad en contextos reales.

**Keywords:** ciberseguridad, PyMEs, riesgo de terceros, seguridad de la cadena de suministro, gobernanza de IA, gestión de riesgos.

## 1 Introduction

The digital transformation of small and medium-sized enterprises (SMEs) has significantly increased their reliance on third-party providers for critical business functions. Cloud computing, Software-as-a-Service (SaaS), and managed service providers (MSPs) enable SMEs to access advanced technological capabilities

without substantial upfront investments. However, this operational dependency introduces a complex and often underestimated cybersecurity challenge: the expansion of the attack surface through external service relationships.

High-profile incidents such as the SolarWinds supply chain compromise and the Kaseya ransomware attack have demonstrated how vulnerabilities in third-party providers can propagate across entire ecosystems, affecting thousands of downstream organizations, including SMEs. These events highlight a structural weakness: even organizations with adequate internal controls remain exposed when their providers are compromised.

Empirical evidence confirms that third-party risk has become a dominant vector in the global threat landscape. A significant proportion of cyber incidents are linked to supply chain vulnerabilities, while SMEs remain particularly exposed due to limited governance capabilities and lack of structured risk management practices (ENISA, 2023; IBM Security & Ponemon Institute, 2022; Verizon, 2023). This challenge is further intensified by the increasing adoption of outsourced digital services, which often operate under shared responsibility models that SMEs do not fully understand.

In Argentina, this situation is reinforced by a sustained increase in cyber incidents and evolving regulatory requirements. National reports indicate a growing number of attacks, particularly phishing and fraud-related incidents, while regulatory frameworks such as those issued by the Central Bank impose strict incident reporting obligations, including those involving third-party providers. At the same time, institutions such as the National Institute of Industrial Technology (INTI) support SMEs through training and technological assistance, although the adoption of structured cybersecurity governance remains uneven.

Despite the availability of internationally recognized frameworks—such as ISO/IEC 27036, NIST SP 800-161 Rev.1, the Cloud Security Alliance Cloud Controls Matrix (CCM), and CIS Controls v8.1—their implementation within SMEs remains limited. These frameworks often assume levels of organizational maturity, technical expertise, and resource availability that do not align with SME realities.

In parallel, the rapid adoption of Artificial Intelligence (AI) through third-party services is introducing new dimensions of risk. As AI-enabled capabilities become increasingly embedded in outsourced platforms, SMEs face new challenges related to transparency, data dependency, and control over external systems.

The contributions of this paper are threefold: (i) a structured analysis of leading cybersecurity frameworks from the perspective of third-party risk management; (ii) the identification of key barriers that limit their adoption in SMEs; and (iii) the proposal of a scalable AI-ready cybersecurity governance framework tailored to SME environments, integrating traditional supply chain security practices with emerging risks associated with AI-enabled third-party services.

The proposed approach is formalized as an AI-ready cybersecurity governance framework tailored to SME environments.

## 2 Background and Related Work

Cybersecurity frameworks have evolved from isolated technical control sets toward comprehensive governance models that address organizational, operational, and supply chain risks. This evolution is particularly relevant in environments where organizations depend heavily on external providers, as is the case with SMEs.

ISO/IEC 27036 provides structured guidance for managing information security in supplier relationships, covering the full lifecycle from supplier selection to contract termination. Its integration with ISO/IEC 27001 enables organizations to incorporate third-party risk management into broader information security management systems. However, its formal structure and reliance on governance maturity can limit its applicability in resource-constrained environments (International Organization for Standardization, 2021).

NIST Special Publication 800-161 Revision 1 extends this perspective by introducing a comprehensive approach to Cybersecurity Supply Chain Risk Management (C-SCRM). It emphasizes supplier trust, system provenance, and integration with enterprise risk management. While highly detailed, it is primarily designed for large organizations and critical infrastructure, making direct adoption challenging for SMEs (Boyens et al., 2022).

In cloud-based environments, the Cloud Security Alliance Cloud Controls Matrix (CCM) offers a control framework specifically tailored to cloud providers. Its alignment with multiple standards and the availability of assessment tools such as the Consensus Assessment Initiative Questionnaire (CAIQ) make it particularly useful for evaluating third-party services (Cloud Security Alliance, 2022).

The CIS Controls framework provides a more pragmatic approach, focusing on prioritized and actionable security measures. Control 15, which addresses service provider management, offers practical guidance for evaluating and monitoring third-party relationships. This makes it particularly suitable for SMEs seeking incremental improvements without significant resource investment (Center for Internet Security, 2023).

Prior research has highlighted persistent barriers to framework adoption in SMEs, including limited financial resources, lack of specialized expertise, and low levels of cybersecurity awareness (AlGhamdi et al., 2020; ENISA, 2023). SMEs often rely on informal trust relationships with providers rather than structured risk management processes, increasing their exposure to supply chain threats.

More broadly, the transition from traditional information security to cybersecurity reflects a shift from perimeter-based protection toward ecosystem-based risk management, where dependencies on external services play a central role (Von Solms & Von Solms, 2018).

Personal data protection represents an additional dimension that is closely intertwined with third-party risk management, particularly when outsourced and AI-enabled services involve the processing of personal data on behalf of the SME. ISO/IEC 27701 extends ISO/IEC 27001 and ISO/IEC 27002 with a Privacy Information Management System (PIMS), providing requirements and

guidance for organizations acting as either personal data controllers or processors (International Organization for Standardization, 2019). Incorporating this standard as a reference point allows the proposed governance model to explicitly address privacy obligations arising from data-sharing relationships with third-party providers, complementing the broader cybersecurity and AI governance considerations discussed throughout this study.

In addition to these frameworks, the emergence of Artificial Intelligence has led to the development of specialized governance models. The Artificial Intelligence Risk Management Framework (AI RMF 1.0), developed by the National Institute of Standards and Technology (National Institute of Standards and Technology, 2023), provides a structured approach for managing risks associated with AI systems. Organized around the functions Govern, Map, Measure, and Manage, it emphasizes trustworthiness, transparency, and accountability.

Although not specifically designed for SMEs, the AI RMF introduces principles that are highly relevant in third-party contexts, where AI capabilities are often consumed indirectly through external providers. This creates a new layer of dependency that extends beyond traditional supply chain risk.

Additional studies have explored the organizational and behavioral dimensions of cybersecurity in SMEs, highlighting the importance of culture, awareness, and policy effectiveness (Alshaikh, 2020; Bada et al., 2019; Doherty & Fulford, 2005). Other research has examined barriers to adoption and risk perception in SMEs, particularly in developing economies (Alahmari & Duncan, 2020; Santos et al., 2021).

From an operational perspective, industry reports emphasize the growing importance of structured third-party risk management practices and supply chain resilience (Cybersecurity and Infrastructure Security Agency, 2021; Deloitte, 2022; KPMG, 2022). These findings are complemented by broader analyses of cyber risk economics and systemic vulnerabilities (Ghadge et al., 2020; Sen & Borle, 2020).

Recent research has also explored adaptive governance models specifically designed for SMEs, emphasizing progressive implementation and alignment with organizational capabilities (Bolatti et al., 2025). These approaches reinforce the need for flexible and context-aware frameworks that bridge the gap between theoretical models and practical adoption.

## 3 Problem Analysis: Third-Party Risk in SMEs

Despite the availability of established cybersecurity frameworks, SMEs face persistent challenges in managing risks associated with third-party services. These challenges are multidimensional, involving technical limitations, organizational constraints, and economic factors.

A primary limitation is the lack of internal cybersecurity expertise. Many SMEs operate without dedicated security personnel, which restricts their ability to evaluate provider security postures, interpret compliance requirements, and implement continuous monitoring mechanisms. As a result, supplier selection

is often based on cost or operational convenience rather than structured risk assessment.

Resource constraints further complicate adoption. Frameworks such as ISO/IEC 27036 and NIST SP 800-161 require investments in governance processes, supplier evaluation, and ongoing monitoring that frequently exceed SME capabilities. Consequently, organizations either implement these frameworks partially or not at all.

Another critical gap lies in procurement and contractual practices. SMEs often fail to include cybersecurity requirements in service agreements, such as incident notification timelines, data protection obligations, or audit rights. This omission increases exposure to operational disruptions and regulatory risks.

The widespread adoption of cloud services introduces additional complexity. While providers typically offer robust security controls, SMEs frequently misunderstand shared responsibility models, assuming that providers are fully responsible for protecting systems and data. This misconception reduces oversight and weakens governance.

In Latin America, and particularly in Argentina, these challenges are further amplified. Empirical studies indicate that a significant proportion of SMEs lack formal cybersecurity controls and rarely assess risks associated with third-party providers. At the same time, regulatory frameworks impose increasing obligations that many organizations are not prepared to meet, creating a gap between compliance requirements and operational capabilities.

The growing integration of AI into outsourced services introduces an additional layer of complexity. SMEs are increasingly dependent on AI-enabled platforms without having visibility into how these systems operate or how risks are managed. This reinforces the need for governance models that not only address traditional third-party risks but also incorporate AI-related considerations.

These limitations reveal a fundamental gap between the design of existing cybersecurity frameworks and their practical implementation in SME environments. This gap is consistent with findings from regional and international organizations, which highlight the limited maturity of cybersecurity practices in SMEs and the need for targeted capacity-building initiatives (International Telecommunication Union, 2021; OECD, 2021; Organization of American States & Inter-American Development Bank, 2020).

## 4 Proposed Governance Model for SMEs

Based on the analysis of existing frameworks and the structural limitations identified in SMEs, this paper proposes a simplified and scalable governance model for managing cybersecurity risks associated with third-party services. The model is designed to align with international standards while remaining operationally feasible for resource-constrained environments. Figure 1 presents the proposed governance model for SMEs.

This work introduces an AI-Ready Cybersecurity Governance Framework for SMEs, defined as a simplified, structured, and scalable model that integrates

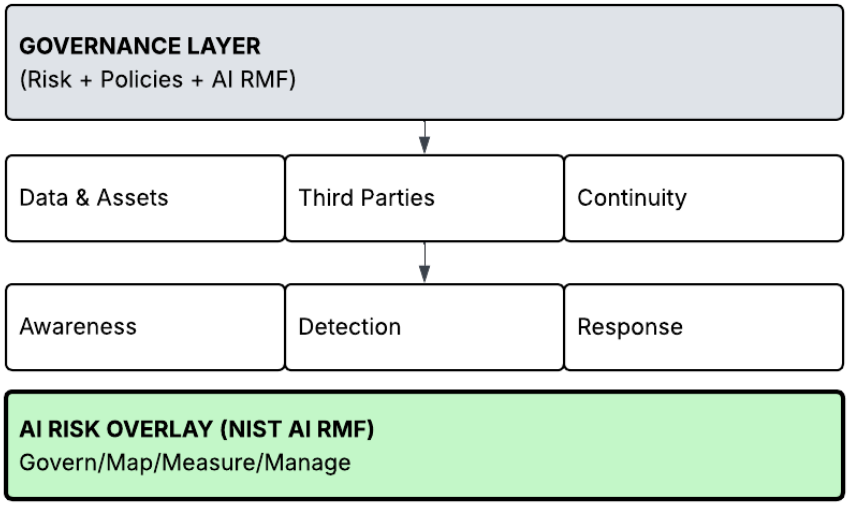


**Fig. 1.** AI-Integrated Cybersecurity Governance Model for SMEs (adapted from the proposed model).

traditional cybersecurity governance with third-party risk management and AI-specific risk considerations.

The framework is designed to address the limitations of existing approaches by providing a minimum viable governance structure that aligns with international standards while remaining feasible for resource-constrained environments. Unlike traditional frameworks, which assume high levels of organizational maturity, the proposed framework emphasizes progressive implementation, adaptability, and operational simplicity.

A key distinguishing feature of this framework is the integration of AI-related risk as a transversal dimension, aligned with the NIST AI Risk Management Framework. This enables SMEs to extend their governance capabilities beyond conventional cybersecurity practices to include emerging risks associated with AI-enabled services.

Overall, the framework provides a cohesive approach that unifies governance, operational controls, third-party management, and AI risk considerations into a single, SME-oriented model.

Table 1 summarizes the key characteristics of the proposed AI-ready cybersecurity governance framework for SMEs, highlighting its scope, structure, and differentiating features.

The framework is operationalized through six core governance pillars, each addressing a specific dimension of cybersecurity risk. These pillars are derived from established frameworks such as NIST CSF 2.0, CIS Controls v8.1, and the

**Table 1.** Characterization of the AI-Ready Cybersecurity Governance Framework for SMEs

| **Dimension** | **Description** |
|---|---|
| Purpose | Provide a simplified and scalable governance model for managing cybersecurity risks in SMEs, with a focus on third-party services. |
| Scope | Covers governance, operational controls, third-party risk management, and AI-related risks. |
| Target Organizations | Small and medium-sized enterprises (SMEs) with limited resources and cybersecurity maturity. |
| Framework Basis | Aligned with ISO/IEC 27036, NIST SP 800-161, CIS Controls v8.1, and CSA Cloud Controls Matrix (CCM). |
| AI Integration | Incorporates AI risk as a transversal dimension aligned with the NIST AI Risk Management Framework (AI RMF). |
| Core Structure | Six governance pillars: governance, data & assets, continuity, third parties, awareness, and detection/response. |
| Implementation Approach | Progressive maturity model enabling incremental adoption. |
| Key Differentiator | Integration of AI-related risks into third-party governance within a simplified SME-oriented framework. |
| Expected Benefits | Improved risk visibility, better supplier control, and enhanced cybersecurity resilience in SMEs. |

Cloud Security Alliance CCM, but are adapted to provide a minimum viable implementation path for SMEs.

The first pillar focuses on governance and risk management, establishing the foundation for aligning cybersecurity with business objectives. This includes defining basic policies, identifying critical assets, and maintaining a simplified risk assessment process that can be periodically reviewed by management. In practice, this translates into a short security policy document, a register of critical information assets, and a lightweight risk matrix that classifies likelihood and impact on a simple scale, allowing an SME owner or manager to revisit priorities at low cost.

The second pillar addresses the protection of data and assets, ensuring that confidentiality, integrity, and availability are preserved through practical controls such as asset inventory, patch management, and backup strategies. At the implementation level, this pillar also incorporates basic data classification (e.g., distinguishing personal, financial, and operational data) and privacy-oriented controls, drawing on guidance such as ISO/IEC 27701 when personal data is processed on behalf of customers or shared with external providers.

The third pillar emphasizes availability and business continuity, recognizing that service disruptions—whether caused by cyber incidents or provider failures—can have disproportionate impacts on SMEs. Concretely, this pillar covers minimum viable continuity practices such as defining recovery time objectives for critical services, maintaining tested backups, and identifying alternative providers for services considered essential to operations.

The fourth pillar focuses on the management of third-party services, which represents the central theme of this study. Given its centrality, this pillar is decomposed into a set of concrete sub-processes intended to guide implementation in an SME context: (i) *provider inventory and classification*, consisting of a structured registry of third-party services with a criticality rating (e.g., high, medium, low) based on data sensitivity, business dependency, and access level; (ii) *due diligence at onboarding*, involving a lightweight security questionnaire—inspired by tools such as the CAIQ—applied before contracting a new provider, particularly for those rated as high or medium criticality; (iii) *contractual security requirements*, ensuring that agreements explicitly address incident notification timelines, data protection obligations, audit rights, and minimum security expectations; (iv) *ongoing monitoring*, through periodic reassessment of providers (e.g., annually for high-criticality providers) and monitoring of public security advisories or breach disclosures associated with them; and (v) *offboarding and contract termination*, covering data return or deletion, access revocation, and verification that contractual security obligations remain enforceable after the relationship ends. This decomposition is intended to make the pillar actionable for SMEs with limited procurement or legal capacity, while remaining compatible with more mature practices such as those described in ISO/IEC 27036 (International Organization for Standardization, 2021) and CIS Control 15 (Center for Internet Security, 2023).

The fifth pillar addresses awareness and training, recognizing that human factors remain one of the primary vectors of cybersecurity risk. This includes periodic, role-based awareness activities (e.g., phishing simulations and short briefings) and specific guidance for personnel involved in selecting or managing third-party providers, so that procurement decisions incorporate basic security criteria.

The sixth pillar integrates detection, response, and resilience capabilities, promoting simplified incident response procedures and monitoring mechanisms. For SMEs, this typically translates into a short incident response checklist, clearly defined escalation contacts, and basic logging or alerting capabilities, which can later evolve toward more advanced detection mechanisms as organizational maturity increases.

A key contribution of this model is the incorporation of AI-related risk considerations across all pillars. For example, third-party evaluation processes are extended to include AI transparency, data handling practices, and model governance aspects.

To complement this transversal perspective, the framework also considers AI-related risks at the component level. To further operationalize AI-related risks, the proposed framework aligns these risks with the main components of AI systems, following the principles of the NIST AI Risk Management Framework (AI RMF).

AI-related risks can be categorized according to key components of AI systems:

- **Data layer**: Risks associated with data quality, integrity, privacy, and exposure during data processing.
- **Model layer**: Risks related to model behavior, including lack of transparency and vulnerability to adversarial attacks.
- **Infrastructure layer**: Risks arising from the platforms hosting AI capabilities, including cloud dependencies and availability issues.
- **Application layer**: Risks associated with AI integration into business processes, including incorrect outputs and lack of human oversight.

This component-based view provides a more granular perspective aligned with the "Map" and "Measure" functions of the NIST AI RMF.

The model is designed to be implemented progressively through maturity levels, allowing SMEs to start with basic controls and evolve toward more advanced capabilities over time. This approach aligns with the implementation tiers defined in NIST CSF 2.0, ranging from informal and reactive practices to adaptive and risk-informed cybersecurity governance.

## 5 Discussion and Implications

The proposed governance model contributes to bridging the gap between comprehensive cybersecurity frameworks and the practical realities of SMEs. While frameworks such as ISO/IEC 27036 and NIST SP 800-161 provide detailed guidance, their direct implementation often exceeds the capabilities of smaller organizations. By contrast, the model presented in this study translates these frameworks into a structured yet simplified approach that can be realistically adopted.

One of the key implications of this work is the recognition that third-party risk management cannot be treated as a standalone activity. Instead, it must be integrated into a broader governance structure that includes risk management, operational controls, and organizational awareness. This integrated perspective is particularly important in SME environments, where responsibilities are often distributed across a small number of individuals.

Another important contribution is the explicit incorporation of Artificial Intelligence as a risk amplifier within third-party ecosystems. Unlike traditional cybersecurity models, which primarily focus on technical and organizational controls, the proposed model integrates AI-specific risk dimensions, including transparency, data governance, and model reliability. By aligning with the NIST AI Risk Management Framework, this study extends third-party governance beyond conventional supply chain security toward AI-aware risk management.

Market analyses also indicate a growing investment in cybersecurity capabilities in emerging economies, although adoption remains uneven among SMEs (Mordor Intelligence, 2024).

From a practical perspective, the model provides a pathway for SMEs to transition from informal and reactive approaches toward structured governance. Its emphasis on minimum viable controls, progressive maturity, and alignment with existing frameworks allows organizations to improve their cybersecurity posture without requiring significant upfront investment.

In the context of Argentina and Latin America, the model also supports alignment with emerging regulatory requirements and institutional initiatives. By incorporating elements such as incident reporting, provider accountability, and capacity building, it provides a foundation for improving resilience in environments characterized by resource constraints and evolving threat landscapes.

However, this study has important limitations. The proposed governance model is conceptual in nature and has not yet been validated through empirical implementation in real-world SME environments. As such, its effectiveness, scalability, and operational feasibility remain to be tested. Additionally, while the model integrates AI-related risk considerations, the rapid evolution of AI technologies may introduce new challenges that require continuous adaptation of governance practices.

Future work will focus on validating the model through pilot implementations and case studies in SMEs, particularly within Latin America. This will enable the assessment of its practical applicability, identification of implementation barriers, and refinement of its structure based on empirical evidence.

## 6 Conclusion

The increasing dependence of SMEs on third-party services has fundamentally transformed the cybersecurity landscape, introducing new forms of risk that extend beyond traditional organizational boundaries. While international frameworks provide valuable guidance, their complexity and resource requirements often limit their adoption in SME environments.

This paper has analyzed the applicability of leading cybersecurity frameworks in the context of third-party risk management and identified key barriers that hinder their implementation. In response, it proposes a simplified and scalable governance model that aligns with international standards while remaining accessible to SMEs.

A central contribution of this work is the integration of Artificial Intelligence as a critical dimension of third-party risk. As AI-enabled services become more prevalent, SMEs must expand their governance practices to address issues related to transparency, data management, and model reliability. The alignment with the NIST AI Risk Management Framework provides a foundation for incorporating these considerations into existing cybersecurity strategies.

The proposed model offers a practical pathway for SMEs to improve their cybersecurity posture through incremental implementation, focusing on essential controls and progressive maturity. By doing so, it enables organizations to move from reactive security practices toward proactive and structured governance.

Future work should focus on validating the model through real-world implementations, particularly in SME environments within Latin America. Additional research is also needed to explore the evolving intersection between cybersecurity and AI governance, ensuring that SMEs remain resilient in an increasingly complex digital ecosystem.

This work contributes to advancing cybersecurity governance in SMEs by providing a practical and adaptable model that addresses both current and emerging risks, positioning SMEs to better navigate increasingly complex digital ecosystems.

**Acknowledgment on AI-assisted writing** During the preparation of this work, the authors used an artificial intelligence tool (ChatGPT, OpenAI) to improve the language, clarity, and readability of the manuscript. After using this tool, the authors reviewed and edited the content as necessary and assume full responsibility for the content of this publication.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.

## References

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: A systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Alshaikh, M. (2020). Developing a cybersecurity culture to influence employee behavior: A practical perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Bada, M., Sasse, M. A., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? *Human Aspects of Information Security & Assurance*, *13*(1), 118–127. https://arxiv.org/abs/1901.02672

Bolatti, D., Díaz, J., & Bollati, V. (2025). Ciberseguridad estratégica para PyMEs: Un modelo de gobernanza adaptado y progresivo. *Actas del XXXI Congreso Argentino de Ciencias de la Computación (CACIC 2025)*, 893–902. http://sedici.unlp.edu.ar/handle/10915/189846

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (tech. rep. No. NIST SP 800-161 Rev.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Center for Internet Security. (2023). Cis critical security controls v8.1. https://www.cisecurity.org/controls

Cloud Security Alliance. (2022). Cloud controls matrix (ccm v4.0). https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Cybersecurity and Infrastructure Security Agency. (2021). Defending against software supply chain attacks. https://www.cisa.gov

Deloitte. (2022). *Global third-party risk management survey* (tech. rep.). Deloitte Insights. https://www.deloitte.com

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, *18*(4), 21–39. https://doi.org/10.4018/irmj.2005100102

ENISA. (2023). *ENISA threat landscape 2023* (tech. rep.). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

IBM Security & Ponemon Institute. (2022). *Cost of a data breach report 2022* (tech. rep.). IBM Security. https://www.ibm.com/reports/data-breach

International Organization for Standardization. (2019). *Iso/iec 27701:2019 – security techniques – extension to iso/iec 27001 and iso/iec 27002 for privacy information management – requirements and guidelines*. ISO. https://www.iso.org/standard/71670.html

International Organization for Standardization. (2021). *Iso/iec 27036: Information security for supplier relationships*. ISO. https://www.iso.org/standard/59689.html

International Telecommunication Union. (2021). *Global cybersecurity index 2020* (tech. rep.). ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

KPMG. (2022). *Third-party risk management outlook* (tech. rep.). https://kpmg.com

Mordor Intelligence. (2024). Argentina cybersecurity market: Industry overview and forecast 2024–2029. https://www.mordorintelligence.com

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (ai rmf 1.0)* (tech. rep.). NIST. https://doi.org/10.6028/NIST.AI.100-1

OECD. (2021). *The digital transformation of SMEs* (tech. rep.). OECD Publishing. https://doi.org/10.1787/bdb9256a-en

Organization of American States & Inter-American Development Bank. (2020). *Cybersecurity: Risks, progress and the way forward in latin america and the caribbean* (tech. rep.). OAS / IDB. https://publications.iadb.org/en/2020-cybersecurity-report

Santos, O. C., González, G. V., & Anido, L. (2021). Evaluation of the effectiveness of critical cis security controls. *Computers & Security*, *108*, 102355. https://doi.org/10.1016/j.cose.2021.102355

Sen, R., & Borle, S. (2020). The economics of data breaches: A literature review. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa007

Verizon. (2023). *Data breach investigations report (DBIR) 2023* (tech. rep.). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R., & Von Solms, S. (2018). Cybersecurity and information security: What goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025