Journal of Engineering Research

ISSN 2764-1317 vol. 5, n. 9, 2025

ARTICLE

Acceptance date: 24/12/2025

COMPARATIVE ANALYSIS OF GLOBAL AND REGIONAL CYBERSECURITY: A FOCUS ON MEXICO AND LATIN AMERICA

Nicolás Alonzo Gutiérrez
National Technological Institute of Mexico/Apizaco Technological Institute

Lucía Muñoz Dávila
National Technological Institute of Mexico/Apizaco Technological Institute

ABSTRACT: This article analyzes the current state of cybersecurity globally, with an emphasis on Mexico and Latin America, by comparing five recent reports: ISC2 (2024), KPMG (2024), PwC (2025), ESET (2024), and a local survey by TecNM. The findings reveal significant similarities in talent gaps, AI adoption, persistent threats such as ransomware and phishing, and regulatory challenges. Common patterns are identified that call for comprehensive cyber resilience strategies, increased investment in training, and clear policies for AI use. Collaboration across sectors and the adoption of robust security frameworks are key to mitigating risks.

KEYWORDS: Cybersecurity, cyber resilience, ransomware, artificial intelligence, talent gap, regulation, Latin America, MSMEs, phishing, awareness.

Introduction

Cybersecurity has become a fundamental pillar for the economic and operational stability of organizations globally. In a context marked by rapid digital transformation, the adoption of artificial intelligence (AI), and increasingly sophisticated threats, it is imperative to understand the current state of digital security from a comprehensive perspective. This article seeks to offer a comparative view of the global cybersecurity situation, with a special focus on Mexico and Latin America, based on the analysis of five recent reports: the ISC2 Cybersecurity Workforce Study (2024), the KPMG Cybersecurity Survey (2024), the PwC Digital Trust Insights (2025) – Mexico Edition, the ESET Security Report (2024) – Latin America, and a local survey conducted by the National Technological Institute of Mexico / Technological Institute of Apizaco (TecNM-ITA) (2024), supplemented by the findings of the 3rd Cybersecurity Study in Mexico 2023 by AIMX and CDETECH.

The convergence of findings between these reports allows us to identify patterns and trends that transcend borders and sectors. In the Mexican context, there is a marked dichotomy between large companies and MSMEs, with the latter operating on limited or no budgets, lacking formalized policies, and showing insufficient preparedness against threats such as phishing, ransomware, and identity theft. These data reflect a complex scenario, where lack of preparedness, insufficient investment, and the rapid evolution of threats represent common challenges.

Methods

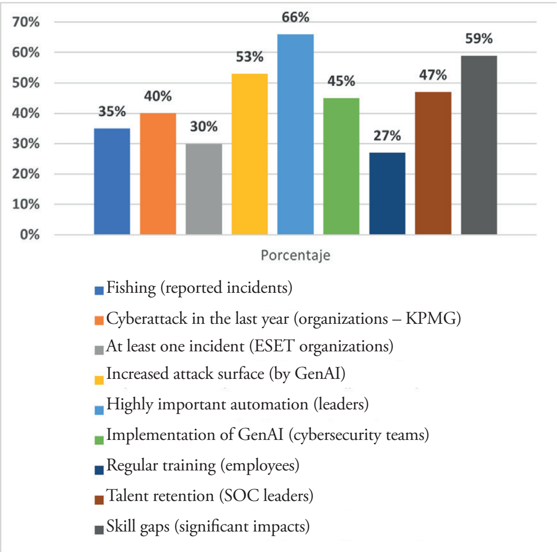
Five main data sources were used to conduct this comparative analysis:

1. ISC2 Cybersecurity Workforce Study (2024): Global survey of 15,852 professionals.
2. KPMG Cybersecurity Survey (2024): Focus on Security Operation Center (SOC) leaders in the US.
3. PwC Digital Trust Insights (2025) – Mexico: Data from 4,042 global executives, with segmentation for Mexico.
4. ESET Security Report (2024) – Latin America: Surveys and telemetry from 2,141 professionals in the region.
5. TecNM-ITA Survey (2024): Local data from 27 Mexican companies, supplemented by the 3rd Cybersecurity Study in Mexico 2023 by AIMX and CDETECH, which included 1,293 users, 324 families, and 257 companies.

The analysis was conducted by identifying six cross-cutting thematic categories and comparing the findings of each report in each of them. Figure 1 shows a bar chart displaying cybersecurity indicators and illustrating the thematic interconnections identified. The qualitative analysis was complemented by a quantitative synthesis of the data reported in the reports.

Table 1 presents a detailed analysis of the key similarities identified in the reports analyzed, organized by thematic categories, and summarizes the most relevant findings in each of these categories in a comparative manner.

In relation to the talent and skills gap, 59% of professionals surveyed by ISC2 report significant impacts due to skills gaps, while KPMG identifies that 47% of SOC leaders have talent retention issues. In the Mexican context, the situation is exacerbated by the fact that only 27% of employees receive regular training, according to the ESET study.



Source: own elaboration

Figure 1 Cybersecurity indicators.

Regarding the adoption of AI and automation, ISC2 indicates that 45% of cybersecurity teams have implemented GenAI in their security tools, corroborated by KPMG, which notes that 66% of leaders consider AI-based automation to be “very important.” However, PwC warns that 53% of organizations have seen their attack surface increase due to GenAI.

In terms of persistent threats, ESET reports that 30% of organizations in Latin America suffered at least one security incident in 2023, while KPMG indicates that 40% experienced a cyberattack in the last year. In Mexico, studies agree that phishing is the most prevalent threat, accounting for between 30% and 40% of reported incidents.

Results

The results of the comparative analysis confirm the existence of common cybersecurity challenges at the global and regional levels. Table 2 presents a comparative summary of the most relevant quantitative findings organized by thematic category.

The results reveal that the talent gap significantly affects organizations’ ability to protect themselves against cyber threats. The ISC2 study shows that 59% of professionals believe that skills gaps impact their ability to protect organizations, while KPMG identifies that 47% of SOC leaders face talent retention issues. In Latin America, ESET reports that only 27% of employees receive regular training on security issues.

In terms of the adoption of emerging technologies, ISC2 indicates that 45% of cybersecurity teams have implemented GenAI in their security tools. KPMG corrobo-

Category	ISC2 (2024)	KPMG (2024)	PwC (2025)	ESET (2024)	TecNM-ITA/ AIMX
Talent gap	59% report impact from skills gaps	47% have talent retention problems	Only 25% allocate budget to key risks	62% consider the budget insufficient	Only 27% receive regular training
AI adoption	45% use GenAI in security tools	66% consider AI "very important"	53% report an increase in attack surface due to GenAI	-	-
Persistent threats	-	40% experienced a cyberattack in the last year	-	30% suffered incidents; ransomware common	Phishing main threat (30-40%)
Regulation	65% believe more regulations are needed for GenAI	-	98% increased investment due to regulations	-	-
Investment	37% report budget cuts	-	83% expect to increase their budget in 2025	62% consider the budget insufficient	22% of MSMEs without a specific budget line
Training	-	-	-	Only 27% receive regular training	18% never carry out awareness campaigns

Table 1 Key similarities identified in cybersecurity reports

Category	Metric	ISC2 (Global)	KPMG (SOC)	PwC (Mexico)	ESET (Latin America)	TecNM-ITA
Talent	Professionals affected by breaches	59	47	-	-	-
Talent	Periodic training received	-	-	-	27%	26%
AI	GenAI adoption	45	66	-	-	-
AI	Increased attack surface	-	-	53%	-	-
Threats	Organizations with incidents	-	40%	-	30%	48
Threats	Phishing attacks	-	-	-	40%	30
Investment	Budget cuts	37	-	-	-	-

Table 2. Comparative cybersecurity results by thematic category

DOI https://doi.org/10.22533/at.ed.317592504123

rates this trend, noting that 66% of leaders consider AI-based automation to be "very important." However, PwC warns that 53% of organizations have experienced an increase in their attack surface due to the implementation of GenAI.

Regarding security threats, ESET documents that 30% of organizations in Latin America suffered at least one security incident in 2023, while KPMG reports that 40% experienced a cyberattack in the last year. In Mexico, TecNM-ITA identifies phishing as the most prevalent threat, accounting for 30% of reported incidents, followed by identity theft (15%) and information loss (11%).

In terms of investment, there is a paradox where PwC reports that 83% of organizations in Mexico in the region surveyed expect to increase their cybersecurity budget in 2025, while ISC2 indicates that 37% globally report budget cuts. ESET finds that 62% of organizations consider the allocated budget to be insufficient, and in Mexico, in the region, TecNM-ITA reveals that 22% of MSMEs do not have a specific budget line for cybersecurity.

Finally, in the regulatory sphere, PwC highlights that 98% of Mexican companies increased their investment in cybersecurity due to regulations, while ISC2 notes that 65% of professionals believe that more regulations are needed for the safe use of GenAI.

Discussion

The findings of this study reveal a fundamental paradox: although there is widespread recognition of the importance of cybersecurity and an increase in investment, critical gaps remain in talent, implementation of advanced measures, and adoption of resilience frameworks. The similarity in the challenges and solutions reported globally and regionally suggests that solutions must be coordinated and based on international best practices.

AI emerges as a dual factor in the cybersecurity landscape. While it offers powerful tools for defense and automation of security processes, it also expands the attack surface and introduces new risk vectors. The lack of clear strategies for its safe use, reported by ISC2 (2024) and PwC (2025), represents a significant vulnerability that requires immediate attention.

The discrepancy between the perception of preparedness and the reality of incidents suggests possible overconfidence or lack of visibility in the face of sophisticated threats. While KPMG reports that 85% of SOC leaders feel prepared, ESET documents that 30% of organizations suffered security incidents. In Mexico, in the region surveyed, this gap is accentuated by the disparity between MSMEs and large companies, where the former operate in highly vulnerable conditions due to budgetary and technical limitations.

The exploitation of old vulnerabilities, as reported by ESET (2024), where 81% of attacks with exploits targeted old vulnerabilities in Office, underscores the critical importance of patch management and continuous updates as basic security measures.

Conclusions

Cybersecurity faces common challenges at the global and regional levels, including the talent gap, AI adoption, persistent threats, and regulatory requirements. To move toward greater resilience, the following is recommended:

1. Strengthen talent training and retention through specialized programs, certifications, and academia-industry collaboration, with a particular focus on the needs of MSMEs.

2. Develop comprehensive strategies for AI adoption that include policies for safe use, governance, and risk management specific to generative technologies.

3. Increase investment in advanced technologies such as EDR, Threat Intelligence, and DLP, with specific support mechanisms for MSMEs through subsidy schemes and specialized technical advice.

4. Promote collaboration between sectors to share threat intelligence, best practices, and coordinate responses to significant incidents, particularly in critical sectors.

5. Harmonize regulatory frameworks that facilitate compliance without hindering innovation, and establish minimum security standards by sector, considering operational particularities and risk levels.

6. Foster a culture of cybersecurity through national awareness campaigns and digital education programs from an early age, with special attention to the human factor as a critical link in security.

These actions, implemented in a coordinated manner between the public, private, and academic sectors, will contribute to building a more secure and resilient digital ecosystem in Mexico and Latin America.

References

[1] Anderson, R., & Moore, T. (2006). The Economics of Information Security. Science, 314(5799), 610-613.

[2] Asociación de Internet MX & CDETECH. (2023). 3er Estudio de Ciberseguridad en México 2023.

[3] ESET. (2024). ESET Security Report Latinoamérica 2024.

[4] Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5(4), 438-457.

[5] Hadlington, L. (2017). Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours. Heliyon, 3(7).

[6] INEGI. (2019). Censo Económico 2019.

[7] Verizon. (2023). 2023 Data Breach Investigations Report.

[8] TecNM-ITA. (2024). Encuesta de Ciberseguridad 2024 (Dataset no publicado).

[9] CIS (Center for Internet Security). (2024). *CIS Benchmarks for Linux Systems*. Recuperado de https://www.cisecurity.org/cis-benchmarks

[10] MITRE Corporation. (2024). *Common Vulnerabilities and Exposures (CVE) System*. Recuperado de https://cve.mitre.org

[11] NIST National Institute of Standards and Technology. (2023). *Security Content Automation Protocol (SCAP) Specifications*. NIST Special Publication

[12]NSA. (2023). *Security Technical Implementation Guides (STIGs) for Linux Environments*. Recuperado de https://public.cyber.mil/stigs/

[13]Thompson, John & Davis, Emily & Carter, Michael & Brooks, Samantha & William, Elijah. (2024). Continuous Verification in Zero Trust Adoption.

GLOSARIO DE SIGLAS TÉCNICAS

APT - Advanced Persistent Threat (Amenaza Persistente Avanzada)

CIS - Center for Internet Security (Centro para la Seguridad en Internet)

CPE - Estándar de nomenclatura mantenido por NIST (National Institute of Standards and Technology) que proporciona un método estructurado para identificar y describir de manera única plataformas tecnológicas.

CVE - Common Vulnerabilities and Exposures (Vulnerabilidades y Exposiciones Comunes).

CVSS - Common Vulnerability Scoring System (Sistema de Puntuación de Vulnerabilidades Comunes).

DISA STIGs (Security Technical Implementation Guides del Defense Information Systems Agency - Guías de Implementación Técnica de Seguridad de la Agencia de Sistemas de Información de Defensa).

DLP - Data Loss Prevention (Prevención de Pérdida de Datos).

EDR - Endpoint Detection and Response (Detección y Respuesta en Endpoints).

GDPR - General Data Protection Regulation (Reglamento General de Protección de Datos).

GPO - Group Policy Object (Objeto de Directiva de Grupo).

IDS - Intrusion Detection System (Sistema de Detección de Intrusiones).

IPS - Intrusion Prevention System (Sistema de Prevención de Intrusiones).

LAPS - Local Administrator Password Solution (Solución de Contraseñas de Administrador Local).

NIST - National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

OVAL - Open Vulnerability and Assessment Language (Lenguaje Abierto de Vulnerabilidades y Evaluación).

PCI-DSS - Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago).

SCAP - Security Content Automation Protocol (Protocolo de Automatización de Contenido de Seguridad).

SCCM - System Center Configuration Manager (Administrador de Configuración de System Center).

SIEM - Security Information and Event Management (Gestión de Eventos e Información de Seguridad).

SOC - (Security Operation Center) Equipo centralizado de profesionales de ciberseguridad que monitorean, analizan y responden a amenazas de seguridad en una organización las 24 horas del día, los 7 días de la semana.

STIG - Security Technical Implementation Guide (Guía de Implementación Técnica de Seguridad).

UEBA - User and Entity Behavior Analytics (Análisis de Comportamiento de Usuarios y Entidades).