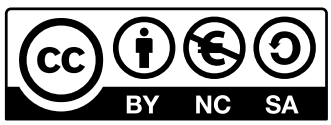
Securing Critical Infrastructure in Latin America: Policy, Risk, and Resilience

DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI whalemate



Credits

Digi Americas Alliance

Alain Karioty
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Federico Nan
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
Marcos Pupo
Mario de la Cruz Sarabia
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

Editors

Belisario Contreras
Andy Kotz

Contents

Introduction

Critical infrastructure (CI) refers to various sectors and actors that underpin national stability and public welfare. In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) identifies 16 critical infrastructure sectors, including Energy, Communications, Financial Services, Healthcare and Public Health, Transportation, Water and Wastewater, and Information Technology, among others.[1] While classifications vary across countries, Latin American governments also recognize energy grids, telecommunications networks, financial systems, transportation corridors, water systems, and public services as foundational to economic growth, democratic governance, and social stability.[2]

In recent years, these systems have increasingly become targets of malicious cyber operations carried out by criminal groups, hacktivists, insider threats, and state-sponsored actors. State-sponsored actors, particularly from China and Russia, treat critical infrastructure not only as economic assets but as strategic leverage in geopolitical competition.[3] Russian operations in Ukraine show that cyberattacks on government networks, telecommunications systems, and energy infrastructure can precede or accompany military action, which blurs the line between cyber and kinetic warfare.[4] Similarly, China-linked campaigns such as Volt Typhoon and Salt Typhoon have targeted telecommunications and other critical infrastructure sectors to gain persistent, stealthy access to networks—often pre-positioning within systems to enable potential disruption during future geopolitical crises.[5]

For Latin America, the stakes remain particularly high. The region is undergoing rapid digital transformation, expanding connectivity, modernizing energy infrastructure, and integrating more deeply into global supply chains. At the same time, many countries face uneven regulatory frameworks, limited cybersecurity resources, legacy infrastructure, and growing exposure to transnational cyber threats. These risks are compounded by increasing activity from advanced persistent threat (APT) groups linked to major powers, which have demonstrated the capability to infiltrate and persist within infrastructure networks for extended periods, often undetected.[6] As a result, critical infrastructure security goes beyond a technical issue; it stands at the center of national resilience, regional stability, and long-term development.[7]

Because CI spans diverse sectors, no single approach can secure it. Protecting a healthcare system requires different measures from those for securing a

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[2] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[3] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[4] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/
[5] https://www.congress.gov/crs-product/IF12798
[6] https://www.congress.gov/crs-product/IF12798
[7] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

hydropower facility or major port. A key factor that distinguishes CI security from traditional cybersecurity lies in the use of operational technology (OT), the hardware and software that monitor and control physical processes. Industrial control systems (ICS), which connect information technology (IT) systems with OT environments, create risks that differ significantly from conventional IT networks. In most countries, these systems still rely on legacy technologies originally designed for reliability and operational continuity rather than cybersecurity.[8] At the same time, AI now reshapes both defense and attack: defenders use AI-driven anomaly detection to identify subtle disruptions in industrial processes, while adversaries can use AI to map complex networks, discover vulnerabilities in legacy systems, and craft more precise, automated intrusion strategies against OT environments.[9]

Historically, such systems operated in relative isolation and faced limited exposure to cyber threats.[10] However, as infrastructure operators across the region adopt digital monitoring tools, remote access capabilities, and cloud-based management platforms, physical systems have become more interconnected and vulnerable. The convergence of IT and OT environments has expanded the attack surface for critical infrastructure across energy, water, mining, transportation, and telecommunications sectors. This expanded attack surface mirrors vulnerabilities exploited in Ukraine, where Russian actors have repeatedly targeted power grids, communications networks, and digital services with increasingly sophisticated cyber campaigns since 2014.[11] AI accelerates this situation because it enables more scalable, adaptive attacks while empowering defenders to deploy predictive analytics, automated incident response, and digital twins to simulate and mitigate cascading failures in interconnected systems.

Across all sectors, supply chains represent an especially attractive target for malicious actors. By compromising vendors, managed service providers, or software dependencies, adversaries can gain indirect access to high-value infrastructure assets. These risks are not theoretical. In the case of China-linked Volt Typhoon, intelligence agencies have warned that attackers infiltrated sectors including energy, transportation, and water systems and maintained access for years, suggesting a strategy focused on pre-positioning for potential disruption during future crises rather than traditional espionage.[12]

Governments, regulators, CI owners and operators, and private-sector partners throughout Latin America must therefore adapt to an evolving threat landscape. In doing so, it is important to distinguish the roles of actors within that ecosystem: critical infrastructure operators bear direct responsibility for securing the systems they operate, while technology providers,

[8] https://www.cisa.gov/topics/industrial-control-systems
[9] https://red.anthropic.com/2026/mythos-preview/
[10] https://www.cisa.gov/topics/industrial-control-systems
[11] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/
[12] https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure

including cloud service providers, software developers, and equipment manufacturers, support that mission with secure, certifiable platforms and transparency about the security of their products. In this context, AI should be understood not as a standalone solution but as a force multiplier: its effective use will depend on governance frameworks, data quality, and human expertise, while its misuse could lower the barrier to entry for sophisticated cyber operations against critical infrastructure. Addressing IT/OT convergence risks, strengthening supply chain security with role-appropriate obligations, direct investment in workforce development, and adopting secure-by-design and secure-by-default principles are all critical steps toward building more resilient infrastructure across the region.

Identifying and Prioritizing Critical Infrastructure

Identifying and correctly prioritizing critical infrastructure is a foundational step in developing effective cybersecurity strategies, particularly in resource-constrained environments. Governments must first determine which assets and systems are most essential to national security, economic stability, and public safety, since not all infrastructure can be protected equally. This process typically involves risk-based assessments that evaluate both the likelihood of disruption and the potential consequences of failure, including spillover effects across interconnected sectors. In this context, governments should also consider less visible but highly consequential assets. These may include subsea telecommunications cables, which carry most international data traffic and are critical to economic continuity and national connectivity. Despite their importance, these assets are often overlooked in traditional critical infrastructure frameworks and may lack adequate physical and cyber protection measures.

In Latin America, where dependencies between energy, telecommunications, financial systems, and transportation networks are increasing, prioritization must also account for systemic risk and cross-sector interdependencies. Scenarios that introduce hybrid risk environments where physical and cyber threats converge, such as unmanned aerial systems (drones) being used to target physical infrastructure, require expanded definitions of what constitutes critical infrastructure.

By defining critical assets and ranking them according to their strategic importance and vulnerability, policymakers and operators can more effectively allocate limited resources, focus mitigation efforts, and improve overall resilience against both cyber and physical threats. Additionally, sectors such as space-based services (including satellite communications and GPS), data centers supporting cloud infrastructure, and undersea energy pipelines should be better incorporated into national critical infrastructure inventories, as their disruption could have disproportionate and cross-border impacts.

Supply Chain Security

Critical infrastructure supply chains are complex ecosystems that can span hundreds of suppliers, integrators, owners, operators, and service providers.[13] They include hardware manufacturers, software developers, cloud providers, maintenance contractors, logistics companies, certification bodies, and regulatory authorities. These supply chains interact through physical processes such as production and transportation, as well as digital services such as remote monitoring, software updates, and data exchange.[14]

[13] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles
[14] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf

One of the most significant developments affecting critical infrastructure and its supply chains is rapid digitalization.[15] Infrastructure systems are increasingly dependent on software-driven components, cloud-based services, and remote connectivity. AI further transforms supply chains because it enables predictive maintenance, automated decision-making, and real-time analytics, while also introducing new risks related to data integrity, model security, and adversarial manipulation. Looking ahead, advances in quantum computing may challenge current cryptographic standards that underpin secure communications across supply chains, which creates the need for long-term planning around quantum-resistant encryption. As a result, the security of a single operator now depends on the resilience of every link in its supply chain. A vulnerability introduced by an external software vendor, managed service provider, or equipment supplier can spread across multiple sectors and even across national borders.

To manage the increasing complexity, organizations can start meaningful risk reduction with the establishment and enforcement of minimum cybersecurity standards for suppliers. What distinguishes supply chain cybersecurity in the CI context is its collective nature and the fact that different actors bear different, clearly defined obligations. Critical infrastructure operators retain primary accountability for the security of their operational environments, including how they configure, integrate, and govern third-party technologies within those environments. Technology providers such as cloud service providers, managed security service providers, and software vendors are accountable for the security of their platforms and services, typically evidenced through industry certifications (ISO 27001, SOC 2, FedRAMP-equivalent), contractual commitments, and published shared responsibility policies. Clear baseline security requirements, contractual enforcement mechanisms, and appropriate oversight should reflect this role differentiation — ensuring accountability at every stage of procurement, integration, and maintenance without displacing operator responsibility onto providers who do not control how their services are ultimately deployed.

The distribution of these visibility obligations must follow operational control: infrastructure operators are responsible for inventorying their own deployments, configurations, and dependencies, including any cloud-based components. Technology providers, in turn, are responsible for providing the documentation — software bills of materials, security advisories, clear architecture details, and audit evidence — that enables operators to fulfill their own visibility obligations. As supply chains expand to include AI-driven services and, in the future, quantum-enabled capabilities, transparency around algorithms, data sources, and cryptographic dependencies will become more critical. Regulatory frameworks that require providers to conduct visibility exercises within customer environments invert this logic and undermine effective accountability.

[15] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf

Continuous monitoring, third-party risk assessments, and cybersecurity clauses embedded in procurement contracts translate high-level policy commitments into operational practice. Secure-by-design and secure-by-default must become procurement requirements, not only aspirations. Organizations should embed cybersecurity requirements in vendor contracts with measurable compliance criteria and establish clear accountability. This includes a requirement for vendors to show secure development practices for AI systems and early planning for post-quantum cryptographic readiness. To make these baselines effective at scale, governments and industry consortia must align on standardized frameworks and procurement policies. Initiatives such as the NIST Cybersecurity Framework 2.0[16] and CISA's secure-by-design principles[17] can serve as foundational models for harmonizing supplier expectations and enforcing accountability. As digital transformation accelerates, the attack surface of critical infrastructure will only expand. Therefore, strengthening supply chain security is not just a technical necessity but a strategic imperative for national resilience and economic stability.

OT/IT Convergence and Its Implications for Security

As the integration between IT and OT increases, their security measures should not function as isolated systems. Traditional IT security emphasizes the confidentiality, integrity, and availability (CIA) triad, while OT security prioritizes the continuous and reliable operation of physical processes and control systems. To safeguard against a growing range of cyber threats, OT environments rely on supervisory control and data acquisition (SCADA) systems and industrial control systems to maintain operational resilience.[18] The ongoing convergence of IT and OT presents a challenge: to align the differing priorities of these domains to ensure both cyber resilience and uninterrupted operational performance across the critical infrastructure supply chain.

Emergent and emerging technologies accelerate this convergence. AI enhances threat detection, automates anomaly identification, and optimizes operational efficiency across both IT and OT environments. However, these capabilities also introduce new risks, including the potential for adversarial attacks on AI models, data poisoning, and overreliance on automated decision-making in safety-critical systems. At the same time, the future impact of quantum computing and other emerging technologies on

[16] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[17] https://www.cisa.gov/securebydesign
[18] https://www.paloaltonetworks.com/cyberpedia/iot-security-vs-ot-security

encryption and secure communications poses a strategic challenge for IT and OT systems, particularly where long-lived infrastructure assets rely on cryptographic protections that may become vulnerable over time. Preparation for these shifts will require practical, forward-looking security strategies that incorporate AI governance and quantum-resilient cryptography.

Beyond technical outcomes, the threat response procedures and compliance obligations for IT and OT often differ in practice. Governments and regulators must account for these distinctions as they craft future requirements and must further distinguish between critical infrastructure operators and integrators — who bear direct operational accountability — and technology solution providers such as cloud platforms or connectivity services, whose regulatory obligations should align with their actual sphere of control. Applying critical infrastructure operator obligations to technology providers that do not directly operate essential systems would distort accountability and risk slowing the adoption of advanced security capabilities that resource-constrained operators urgently need.

Survey of Regional Experts

Background

To better understand the critical infrastructure cybersecurity ecosystem in Latin America, Digi Americas Alliance conducted a survey of 141 stakeholders across the region. Approximately 46% of respondents work at critical infrastructure operators, while the remaining participants represent related organizations involved in cybersecurity, technology, and policy. Respondents represent a diverse set of countries, including Colombia (19%), Mexico (14%), Argentina (9%), Panama (7%), and Ecuador (7%), as well as Brazil, Costa Rica, Spain, Uruguay, the Dominican Republic, Chile, the United States, Venezuela, Guatemala, Honduras, Paraguay, and Peru.

Participants also represent various roles within their organizations. Nearly half of respondents (47%) work in security-related roles, while 21% are members of the C-suite. Another 19% work in broader technology functions, with the remaining respondents working in areas such as cybersecurity, general management, analysis, and sales. This diversity of roles shows how different groups interpret cybersecurity challenges as perceived across organizational leadership, technical teams, and operational stakeholders.

Organizations

Respondents represent organizations with varying ownership structures that operate across multiple sectors. Approximately 60% work in privately owned organizations, 30% in publicly owned or government organizations, and 10% in organizations with mixed ownership structures.

The surveyed organizations also span a broad range of industries that play key roles in national economies and public services. The largest share of respondents works in the information technology sector (24%), followed by financial services (19%) and government services (11%). Other sectors represented include energy

(8%), communications, education, healthcare and public health, agriculture, and several additional industries. This diversity shows that critical infrastructure spans multiple sectors and that risks can move from one sector to another.

Survey Results

Fig. 1 — Do you have a documented cybersecurity strategy?

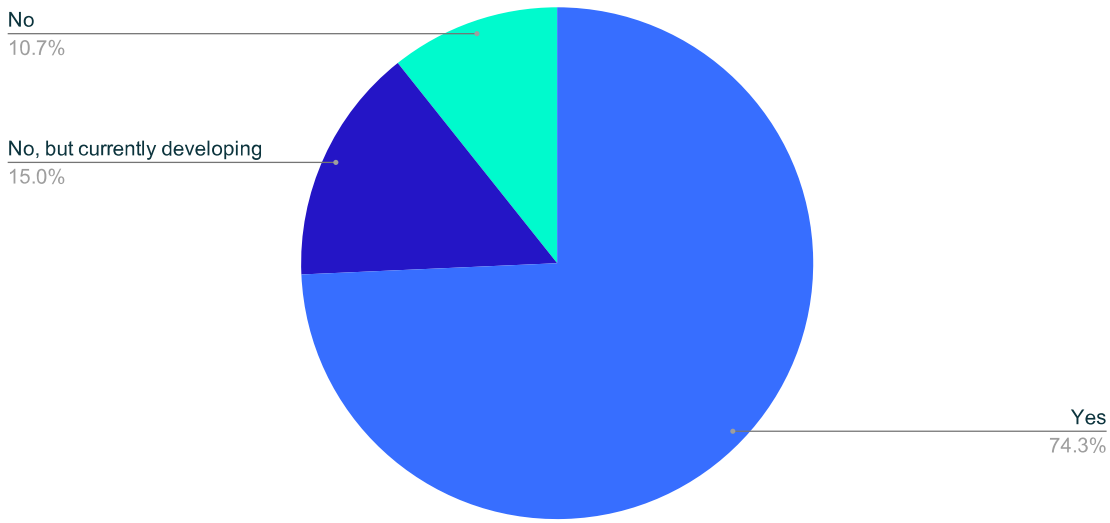


Fig. 2 — Does your strategy include OT?

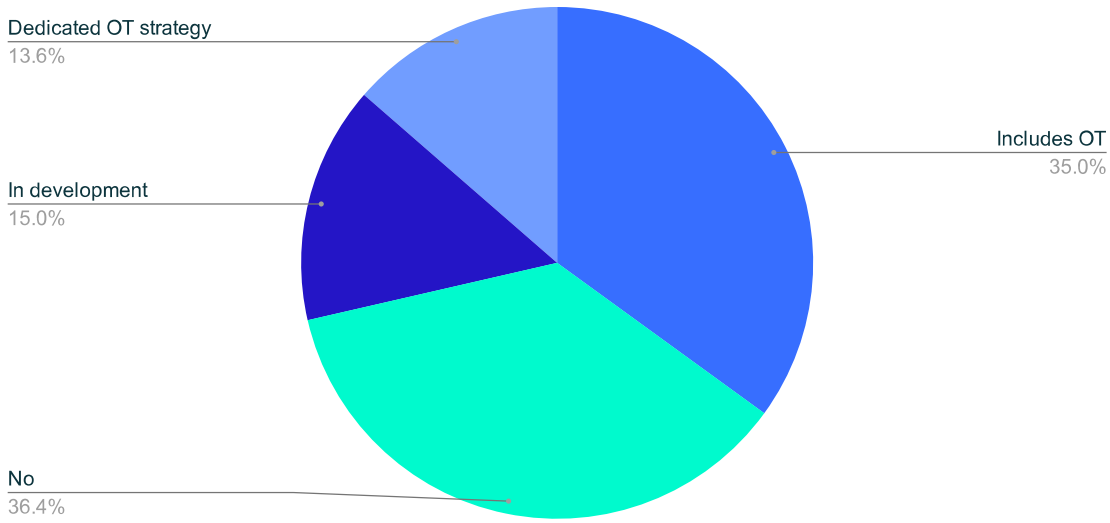


Fig. 3 — Do you rely on IT security practices to protect OT environments?

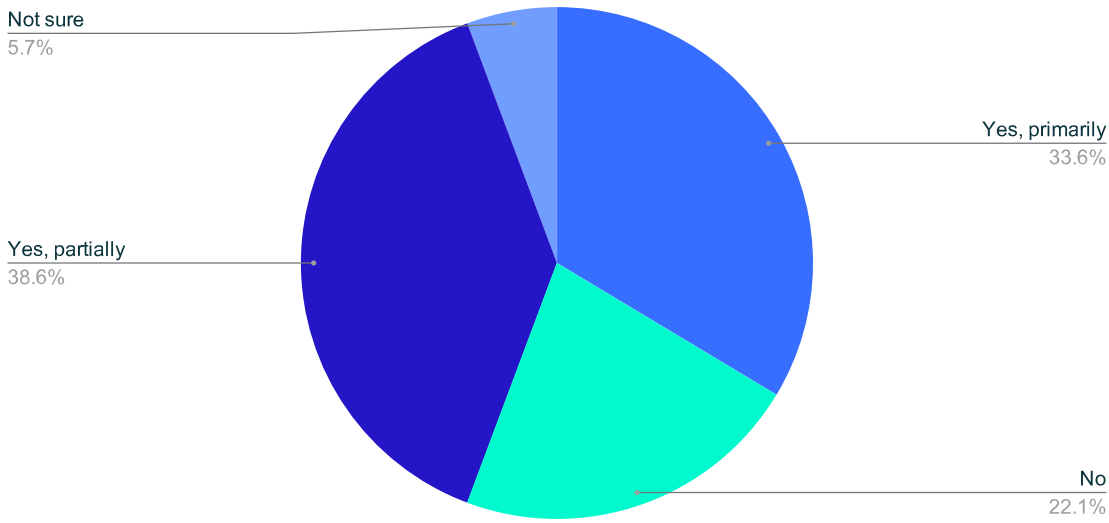
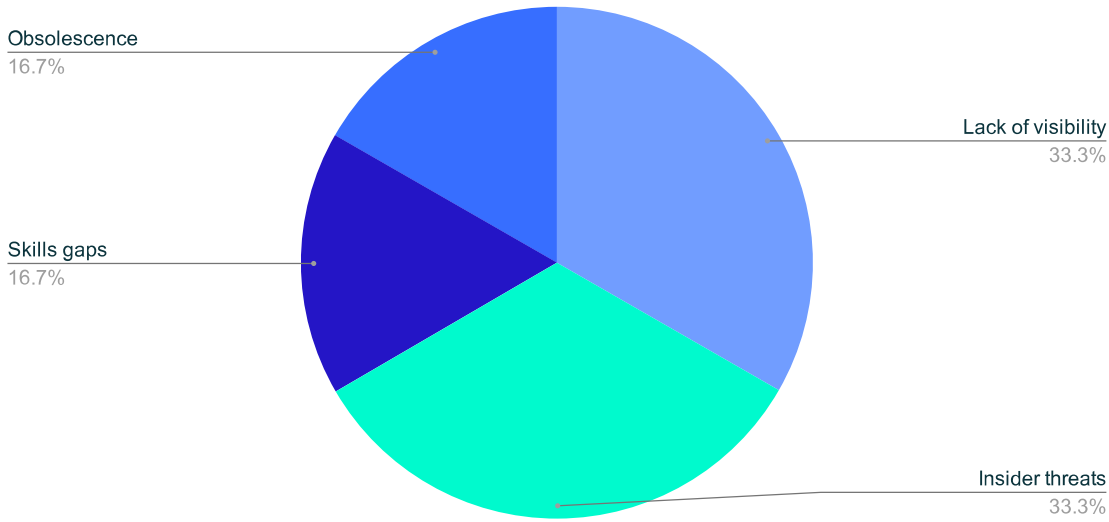


Fig. 4 — Main challenges for protecting IT/OT data?



One of the most important steps for organizations, particularly those designated as critical infrastructure, is to establish a clear plan to protect both their operational technology (OT) and information technology (IT) assets. Figure 1 shows that most organizations (90%) either have a documented cybersecurity strategy or are actively developing one. However, Figure 2 indicates that a majority (51%) of these same organizations do not currently have a plan that explicitly references OT, which points to a critical gap that must be addressed. Protecting physical systems requires deliberate plans that address the distinct risks associated with OT environments. Figure 3 further highlights that most organizations (72%) at least partially rely on IT security practices to protect OT systems. While IT and OT share some similarities, they involve fundamentally different operational requirements and risk profiles and therefore require distinct security strategies and practices.

AI in Security

Fig. 5 — Do you use AI/ML for cybersecurity?

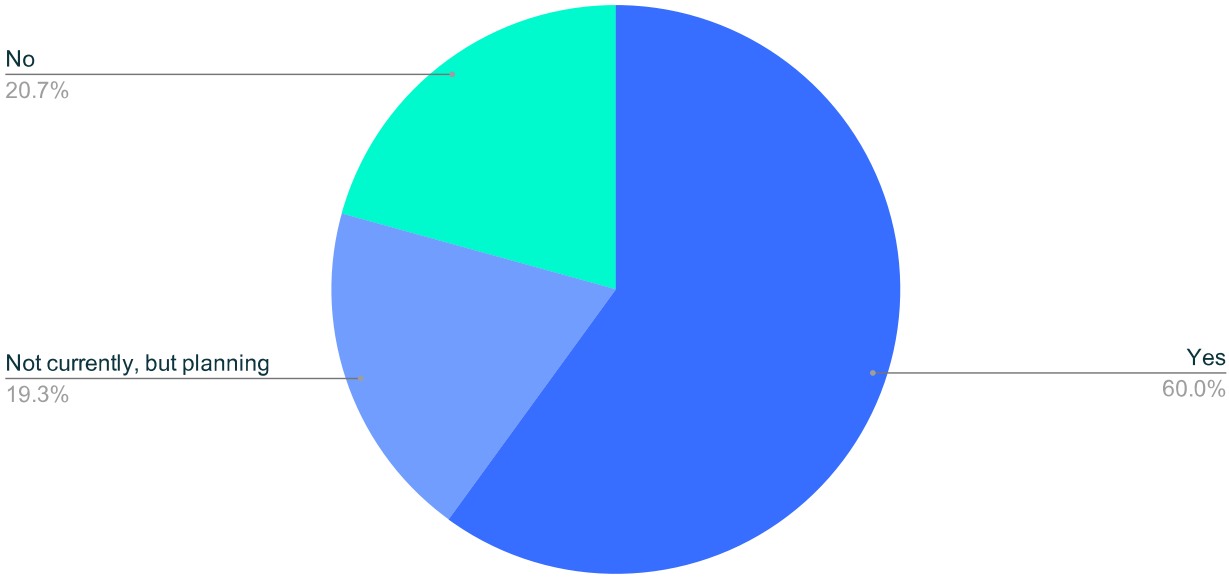


Fig. 6 — Have you developed AI usage policies?

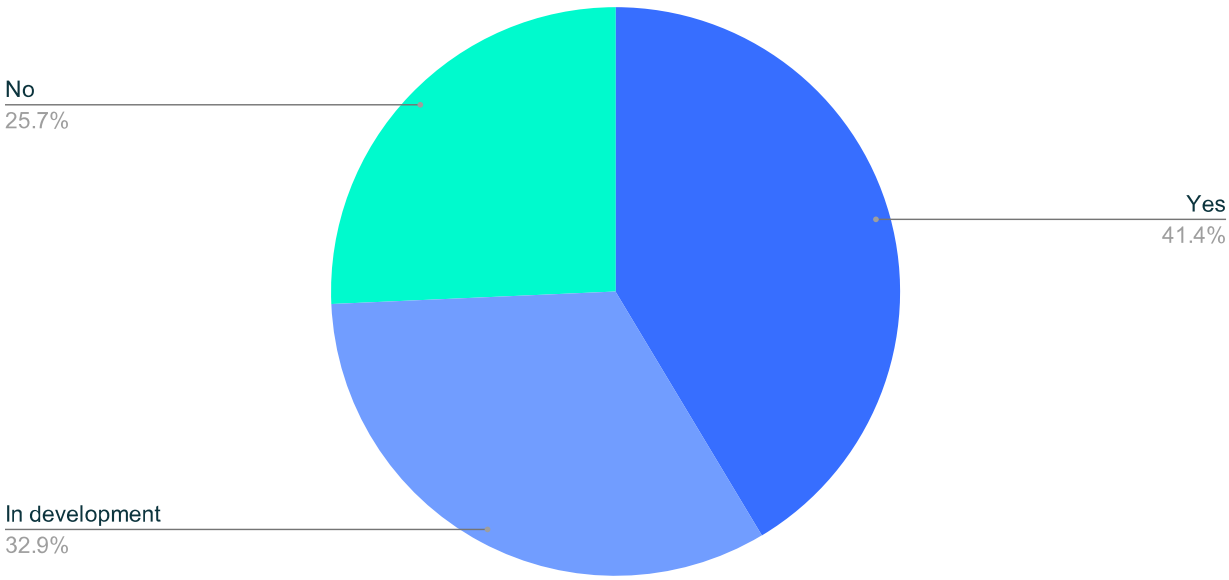


Fig. 7 — How prepared do you consider your organization to be to face AI-driven cyber threats?

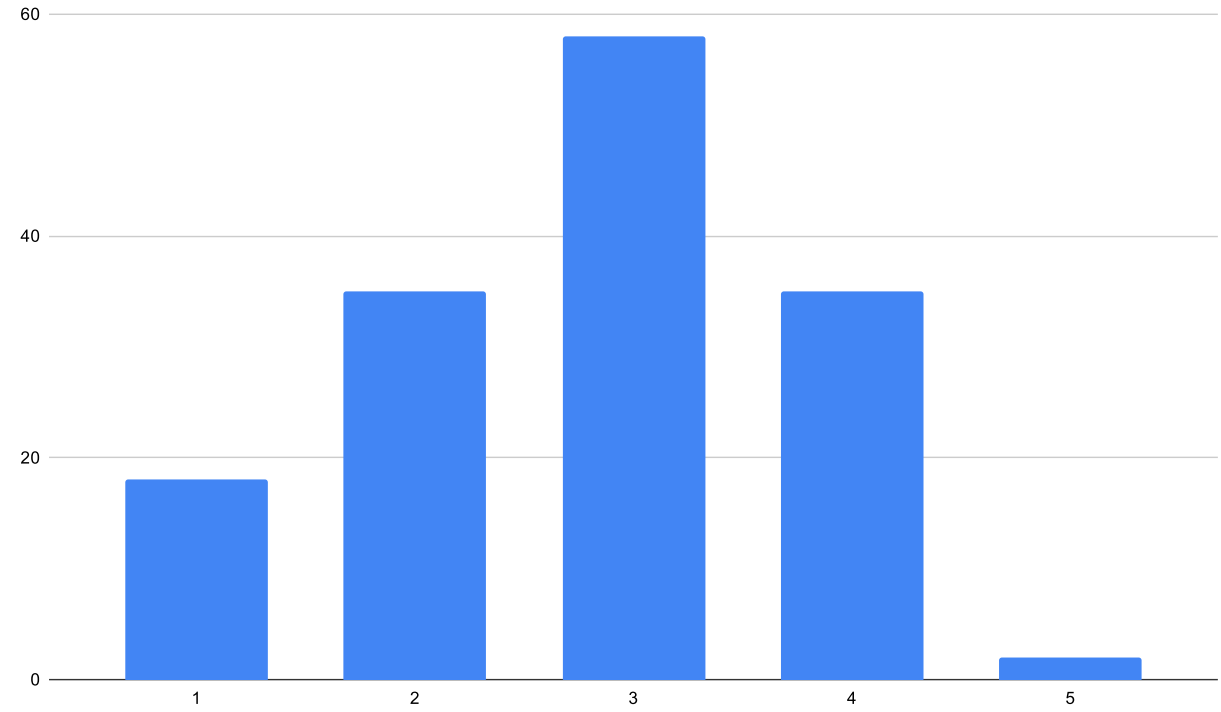
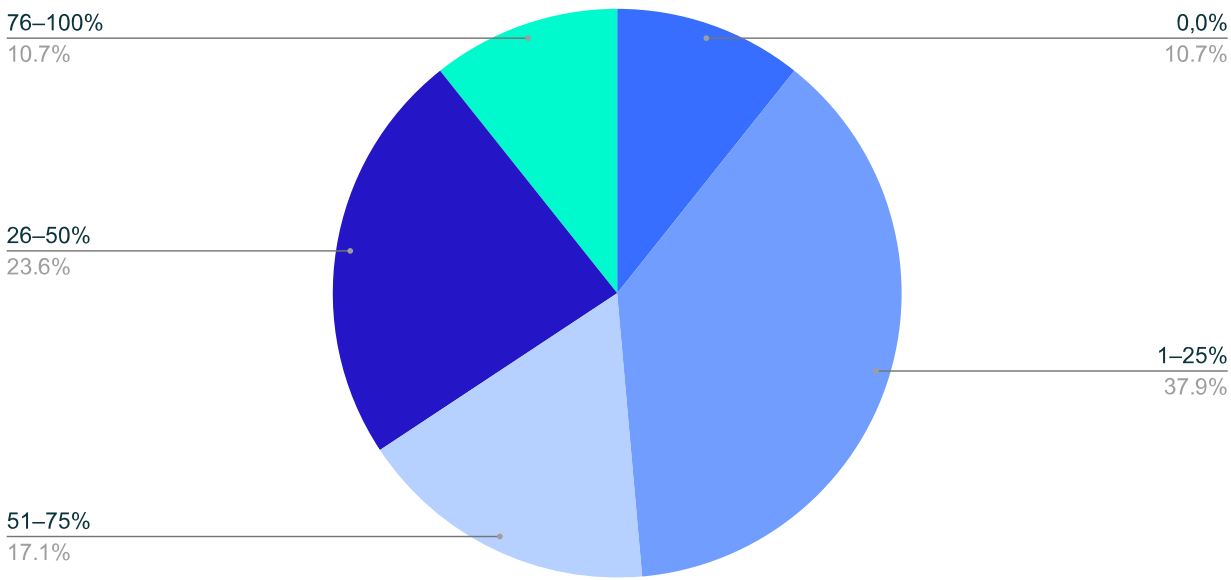


Fig. 8 — What % of critical systems (IT/OT) run in the cloud?



Figures 5 and 6 highlight the growing role of artificial intelligence in cybersecurity operations within critical infrastructure organizations. Approximately 80% of respondents reported that their organizations either actively use AI in cybersecurity systems (60%) or are planning its implementation (19%). This suggests that AI is already having a significant impact on cybersecurity operations, particularly in areas such as threat detection, monitoring, and automation. However, despite this widespread adoption, about 25% of organizations report that they do not have a formal AI policy governing either internal use or third-party providers. As AI continues to evolve and become more integrated into cybersecurity environments, establishing clear policies will be essential to manage both the benefits and potential risks associated with its use.

Figure 7 highlights the other side of AI's growing role in cybersecurity: the emergence of new and more sophisticated threats. AI introduces both defensive capabilities and new attack vectors. Hence, organizations must address AI security across three dimensions: AI for security (using AI to detect anomalies and automate threat response), security for AI (to protect AI systems from adversarial attacks) and AI governance (to establish policies for responsible AI use). When asked how prepared their organization is to handle AI-driven cyber threats, such as deepfakes or AI-generated malware, almost no respondents indicated that they felt "very prepared." Most respondents selected a moderate preparedness level (3), and many others chose lower (2) or somewhat higher (4) levels of preparedness. These responses show that while organizations are increasingly adopting AI as a defensive tool, many still feel uncertain about their ability to counter AI-enabled attacks. Since AI capabilities continue to advance, it is crucial to improve organizational readiness to address these threats, which will become increasingly important.

Cloud Security

Cloud infrastructure offers critical advantages that better protect operational technology and critical infrastructure systems than on-premises environments can match. For resource-constrained Latin American organizations that face sophisticated state-sponsored threats, cloud adoption transforms cybersecurity from a costly burden that requires constant investment into a shared capability that improves with scale. This makes it safer as a strategic imperative for protecting critical infrastructure while it also enables digital transformation.

Figure 8 highlights the extent to which critical infrastructure systems currently operate in cloud environments. The results show that most organizations have begun to integrate cloud technologies into their operations, though typically in a limited capacity. The largest share of respondents (37.9%) reported that between 1–25% of their critical systems (IT/OT) currently operate in the cloud. Another 23.6% indicated that between 26–50% of their systems run in cloud environments, while smaller portions reported higher levels of adoption, including 17.1% with 51–75% of systems in the cloud and 10.7% with 76–100%. Only a small share of respondents reported either no cloud usage or very minimal adoption.

These results suggest that while cloud technologies move into critical infrastructure environments, many organizations are still taking a cautious approach, particularly for operational technology systems that have traditionally remained on-premises. As cloud adoption expands, organizations should ensure that appropriate security controls, visibility, and governance frameworks protect IT and OT assets in hybrid and cloud-based environments.

Best Practices

The survey results indicate that governments, industry, and other stakeholders must take action. While many countries in the region are still developing policies and regulatory frameworks to address critical infrastructure security, several governments and institutions worldwide have already begun implementing strategies, standards, and guidance designed to strengthen the resilience of critical infrastructure and industrial systems. These efforts demonstrate a range of approaches, including integrating OT security into national cybersecurity strategies, developing dedicated OT frameworks, strengthening supply chain security, and establishing regional regulatory requirements for critical sectors.

The following section highlights a selection of these best practices from both within and outside the region. By showcasing existing initiatives, the section aims to provide policymakers, regulators, and private sector operators with practical examples of how governments and organizations are addressing critical cybersecurity risks. These models offer lessons that can help countries develop or refine their own frameworks, promote stronger public-private collaboration, and establish consistent standards to protect the systems that underpin essential services and critical infrastructure.

Brazil

National Cybersecurity Strategy

Brazil's National Cybersecurity Strategy (E-Ciber) emphasizes protection of critical infrastructure and essential services, such as energy, telecommunications, healthcare, and other strategic sectors, which rely heavily on OT systems.[19] The strategy prioritizes improving the security and resilience of critical infrastructure, promoting risk management, incident prevention, and stronger coordination between government and the private sector to prevent and respond to cyber incidents affecting these systems.

By explicitly linking cybersecurity policy to the protection of essential services and infrastructure, Brazil's strategy also addresses the security of OT environments that underpin these sectors. This approach offers a useful lesson for other countries in the region and demonstrates that national cybersecurity strategies should not focus solely on IT systems but also incorporate the protection of industrial and operational systems that support critical

[19] https://www.in.gov.br/en/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784

infrastructure. Embedding OT security into broader national cyber governance frameworks can help governments strengthen resilience, encourage public-private collaboration, and promote consistent security standards across critical sectors.

Colombia

National Digital Security Strategy 2025-2027

Colombia's National Digital Security Strategy 2025–2027 builds on the foundation established by CONPES 3995 (2020) and adopts a more operational and implementation-focused approach to cybersecurity, with a strong emphasis on protecting critical infrastructure and essential services.[20] [21] The strategy prioritizes the security and resilience of critical cyber infrastructure, acknowledging its central role in supporting sectors such as energy, finance, healthcare, and government services.

A key element of the strategy is its emphasis on cyber resilience and risk management. It promotes proactive identification of vulnerabilities, continuous monitoring, and stronger incident detection and response capabilities across both public and private sector operators. The framework also emphasizes preparedness for large-scale cyber incidents, including coordinated national response mechanisms and better recovery capabilities for essential services. Additionally, the strategy strengthens institutional governance and capacity building, addressing gaps identified under earlier frameworks. It includes efforts to enhance national cyber defense capabilities, expand workforce development, and align cybersecurity initiatives with broader national development and digital transformation goals.

Colombia's approach offers a key lesson for the region: strengthening critical infrastructure resilience requires not only technical controls but also well-defined governance structures and coordinated national capabilities. The integration of cybersecurity into broader digital trust and risk management frameworks can improve countries' ability to better manage threats to IT and operational environments that support essential services.

European Union

Directive 2022/2555 - NIS2

The European Union's Network and Information Security Directive 2 (NIS2) sets out one of the most comprehensive regulatory approaches to cybersecurity for critical infrastructure.[22] Adopted in 2022 and replacing the original NIS Directive, NIS2 establishes a common legal framework for cybersecurity across EU member states, covering organizations that operate in 18 critical sectors such as energy, transport, healthcare, finance, and digital infrastructure. The directive

[20] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[21] https://depp.oecd.org/policies/COL2168
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

obliges public and private entities deemed "essential" or "important" to implement risk-management measures, improve governance and incident response capabilities, and report significant cyber incidents to national authorities within defined timelines.[23]

The directive has clear implications for operational technology (OT) and cyber-physical infrastructure, as many covered sectors rely heavily on industrial control systems and other OT environments. By mandating baseline security controls, supply-chain risk management, and executive-level accountability for cybersecurity, NIS2 improves the overall resilience of critical infrastructure across the EU.[24]

This model provides a useful lesson for other regions: establishing harmonized cybersecurity requirements for critical sectors at a regional level can help standardize protections, improve cross-border cooperation, and ensure that both IT and OT systems that support essential services are secured against evolving cyber threats.

Mexico

National Cybersecurity Plan 2025-2030

Mexico's National Cybersecurity Plan 2025–2030[25] marks a significant shift toward a more centralized, preventive, and infrastructure-focused cybersecurity model. Developed by the Agency for Digital Transformation and Telecommunications (ATDT), the plan represents the country's first comprehensive, cross-sector cybersecurity policy and prioritizes the protection of critical infrastructure and essential services as a core national objective.[26]

A central component of the plan is the creation of a unified governance and operational architecture to replace historically fragmented efforts. This includes the establishment of a National Cybersecurity Operations Center (CNSOC) for real-time monitoring, a federal incident response center (CSIRT), and a national inventory of critical infrastructure to identify and prioritize the protection of strategic assets across sectors such as energy, finance, telecommunications, and government systems.[27] These measures are complemented by a vulnerability assessment and alert system designed to proactively identify and remediate weaknesses in public-sector systems.[28]

[23] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[24] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[25] https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
[26] https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030
[27] https://nearshoreamericas.com/mexico-moves-to-strengthen-cybersecurity-with-new-national-plan-and-law/
[28] https://blog.knowbe4.com/mexico-unveils-its-first-national-cybersecurity-plan-a-new-era-of-digital-resilience

The plan also introduces mandatory cybersecurity standards, incident reporting requirements, and risk management frameworks for federal entities, which signals a move toward more enforceable and standardized protections for critical infrastructure. In parallel, Mexico aims to strengthen coordination across government, industry, and academia through a National Cybersecurity Council and expanded information-sharing mechanisms, recognizing that infrastructure resilience depends on multi-stakeholder collaboration.[29]

Mexico's approach offers an important lesson for the region: transitioning from fragmented cybersecurity efforts to a centralized, policy-driven framework—with dedicated institutions, mandatory standards, and a national inventory of critical infrastructure—can significantly enhance visibility, coordination, and resilience. At the same time, the Mexican case underscores the need to complement high-level governance reforms with sector-specific and technical guidance, particularly for OT environments that underpin critical infrastructure.

Singapore

Operational Technology Cybersecurity Masterplan 2024

Singapore has taken a targeted approach to operational technology (OT) security through its Operational Technology Cybersecurity Masterplan 2024, released by the Cyber Security Agency of Singapore (CSA).[30] The plan acts as a national blueprint to strengthen the cybersecurity posture of organizations that operate OT systems across both critical information infrastructure (CII) sectors and other OT-dependent industries. It focuses on strengthening capabilities across three pillars (people, processes, and technology) including the expansion of the OT cybersecurity talent pipeline, better information sharing and incident reporting, resilience beyond traditional critical infrastructure sectors, and the use of secure-by-deployment and secure-by-design principles throughout the lifecycle of OT systems.[31]

Singapore's approach offers an important lesson for other regions: rather than treating OT security solely as a subset of general cybersecurity policy, governments can develop dedicated national frameworks for OT systems that address workforce development, sector coordination, and lifecycle security of industrial technologies. By integrating government agencies,

[29] https://www.eleconomista.com.mx/tecnologia/gobierno-sheinbaum-presenta-plan-nacional-ciberseguridad-2025-20251204-789652.html
[30] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/
[31] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/

industry stakeholders, and educational institutions into a coordinated strategy, Singapore demonstrates how countries can proactively strengthen the resilience of critical infrastructure and emerging physical systems.[32]

United States of America

Department of Energy (DOE) Supply Chain Cybersecurity Principles

In 2024, the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) released a set of supply chain cybersecurity principles to support suppliers and end users in order to protect the supply chain, with a specific focus on the energy sector.[33] The principles covered the following cybersecurity concepts and objectives:

- Impact-driven risk management
- Framework-informed defenses
- Cybersecurity fundamentals
- Secure development and implementation
- Transparency and trust building
- Implementation guidance
- Lifecycle support and maintenance
- Proactive vulnerability management
- Proactive incident response
- Business and operational resilience

The document also emphasizes that security is a shared responsibility and that collaboration is absolutely necessary across a complex supply chain. For example, the document highlights that "Energy technology vendors may source subcomponents from hundreds of different manufacturers for a single piece of equipment; that technology may in turn be purchased by another vendor and integrated into an additional system before it reaches the end user." For end users to be confident in their systems, they must trust that the entire supply chain follows the same security principles.[34]

NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security

In 2023, NIST published SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security.[35] The document provides comprehensive guidance on securing OT, "while addressing their unique performance, reliability, and safety requirements."[36] In addition to an explanation of OT, OT security, and how OT fits into different system environments, the document also gives an overview of "OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and lists recommended security countermeasures to mitigate the associated risks.

[32] https://www.rajahtannasia.com/viewpoints/singapore-launches-updated-national-operational-technology-cybersecurity-masterplan/
[33] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles
[34] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles
[35] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
[36] https://csrc.nist.gov/pubs/sp/800/82/r3/final

The guide sets out a risk-based approach to securing OT environments, including best practices such as defense-in-depth strategies, regular risk and vulnerability assessments, and robust incident response and recovery processes. It also links OT cybersecurity practices with broader frameworks such as the NIST Cybersecurity Framework and NIST SP 800-53 security controls, which enable organizations to include OT security into enterprise-wide risk management programs.[37]

Recommendations

Effective cybersecurity regulation should differentiate obligations between critical infrastructure operators and technology solution providers through a shared responsibility framework. Critical infrastructure operators—entities that directly operate essential systems like energy grids, water systems, or telecommunications networks—hold primary responsibility for protecting their operational environments, including risk assessments, incident response, and security controls appropriate to their operations. Technology solution providers such as cloud service providers, content delivery networks, and data storage services maintain security of their platforms and services through industry certifications and contractual obligations, while operators retain responsibility for security in their use of those services, including configuration and access control decisions.

Regulations should explicitly recognize the Principle of Shared Responsibility, and distribute prevention, protection, response, and recovery obligations among public and private digital system actors, according to their specific role, level of exposure, and operational capacity. This risk-based, technology-neutral approach ensures that accountability aligns with actual operational control, allows infrastructure operators to choose providers based on security capabilities rather than regulatory classification, and promotes a regulatory environment that enhances security while enabling digital transformation and access to advanced cloud security capabilities.

Learning from the survey and the best practices, the paper provides the following recommendations.

Plan for OT Security

Organizations responsible for critical infrastructure should establish clear responsibility for operational technology (OT) security. Whether OT security is managed within an existing IT cybersecurity team or through a dedicated OT security function, there must be personnel specifically tasked with protecting industrial control systems and related assets. Without defined ownership, OT cybersecurity initiatives often lose priority and are overlooked, leaving critical systems exposed to preventable risks. Establishing leadership, accountability, and a formal strategy ensures that OT environments receive consistent attention, resources, and risk management.

[37] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Map IT/OT Convergence

As IT and OT systems become increasingly interconnected, organizations must clearly map how these environments interact. Historically, industrial systems were isolated, but modernization and digital transformation have introduced new points of connectivity and potential vulnerability. A clear view of where IT and OT networks interact allows organizations to identify risks, clarify governance responsibilities, and implement appropriate security controls. Mapping convergence also enables better coordination between IT and OT teams, ensuring that policies, monitoring, and incident response processes account for the realities of integrated environments.

Secure The Supply Chain

Cybersecurity for critical infrastructure must extend beyond individual operators to include the entire supply chain. Governments and infrastructure operators should require baseline OT and IT cybersecurity standards from vendors, manufacturers, integrators, and service providers. Since different actors play different roles, requirements should be tailored accordingly. For instance, manufacturers may need to meet secure development and patching standards, while owners and operators should maintain secure configuration and monitoring practices. Establishing consistent supply chain expectations helps reduce systemic risk and prevents vulnerabilities introduced by third-party products or services.

Secure-by-Design / Secure-by-Default

The adoption of secure-by-design and secure-by-default principles helps mitigate cybersecurity risks before systems are deployed. Rather than relying solely on defensive measures after vulnerabilities are discovered, these approaches emphasize building security into technologies and processes from the outset. This includes the design of systems with strong authentication, minimal exposed services, secure configurations, and robust update mechanisms enabled by default. Encouraging manufacturers and operators to prioritize security during development and deployment reduces the likelihood of exploitable weaknesses and strengthens the long-term resilience of critical infrastructure systems.

Strengthen Coordinated Incident Response and Recovery

Effective protection of critical infrastructure requires robust, coordinated incident response and recovery capabilities across both public and private sectors. Governments and operators should establish clear frameworks for information sharing, enabling timely exchange of threat intelligence, vulnerabilities, and incident data while respecting confidentiality and legal constraints. Strengthening trusted communication channels between infrastructure operators, regulators, and cybersecurity authorities can significantly improve situational awareness and response effectiveness.

Regular testing through joint exercises, such as simulations of cyber incidents affecting IT and OT environments, helps ensure that roles, responsibilities, and response procedures are well understood and operational. In addition, recovery planning should be prioritized alongside response efforts, including the development of business continuity and system restoration strategies tailored to critical infrastructure contexts. Given the interconnected nature of digital systems, cross-border cooperation mechanisms are also essential in Latin America to address transnational threats, coordinate responses, and support rapid recovery from large-scale incidents.

Invest in a Stronger Workforce

Cybersecurity for critical infrastructure in Latin America requires sustained investment in workforce development, particularly for professionals who work at the intersection of IT and OT environments. Many countries in the region lack skilled cybersecurity practitioners with specialized expertise in industrial control systems, which leaves gaps in the protection of essential services. Governments and industry stakeholders should prioritize the development of targeted education and training programs focused on OT security, including partnerships with universities, technical institutes, and international certification bodies.

Expanding access to standardized certifications and hands-on training can help build a pipeline of qualified professionals capable of addressing evolving threats. By cultivating a highly skilled and stable cybersecurity workforce, Latin American countries can enhance their capacity to manage risk, respond to incidents, and sustain long-term resilience across critical infrastructure sectors.

Conclusion

As Latin America continues to modernize its infrastructure and expand digital connectivity, the security of critical infrastructure must remain a central priority for governments, operators, and industry partners. The convergence of IT and OT environments, increasing reliance on cloud services and artificial intelligence, and the growing complexity of global supply chains have fundamentally reshaped the risk landscape for critical sectors. At the same time, the rise of state-sponsored cyber activity—particularly from China and Russia—has introduced a more strategic and persistent threat environment, in which adversaries seek not only to exploit vulnerabilities but also to pre-position themselves within critical systems for potential disruption during geopolitical crises. The survey results presented in this paper highlight both encouraging progress and persistent gaps, particularly in the areas of OT-specific security planning, supply chain visibility, and preparedness for emerging threats.

The experiences of other jurisdictions demonstrate that effective critical infrastructure protection requires coordinated strategies that combine policy leadership, regulatory frameworks, industry standards, and public-private collaboration. National cybersecurity strategies that explicitly address operational technology, dedicated OT security frameworks, supply chain security principles, and harmonized regional regulations can all contribute to building more resilient systems. At the same time, organizations responsible for critical infrastructure should strengthen internal governance, map the intersections between IT and OT environments, and adopt secure-by-design practices that embed security throughout the technology lifecycle.

Ultimately, protecting critical infrastructure is not solely a cybersecurity challenge, it is a strategic requirement for economic stability, public safety, and national resilience. The growing prevalence of campaigns like Volt Typhoon and Salt Typhoon further illustrates that critical infrastructure is now a focal point of long-term strategic competition, requiring governments and operators to prepare for both immediate threats and latent, pre-positioned risks within their networks. By learning from global best practices and investing in stronger governance, workforce development, and cross-sector cooperation, Latin American countries can reduce systemic risk and build more secure, reliable infrastructure systems capable of supporting long-term growth and regional stability.


DIGI
AMERICAS