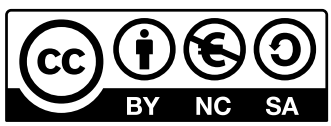
DIGI AMERICAS LATAM CISO

Duke UNIVERSITY

CYBER READINESS IN LATIN AMERICAN PUBLIC SECTORS: LESSONS FROM THE FRONTLINE

LATAMCISO REPORT 2024



For more information, please contact **info@latamciso.com**

Credits

Center for Cybersecurity Policy and Law

Belisario Contreras
Alexis Steffaro
Ines Jordan-Zoob

Duke University

David Hoffman
Camila Herrera
Lily Bermudez
Daniela Pereira Salas
Andy Kotz
Lindsay Gross
Danielle Park
Ana Martinez
Hadrian Gonzalez Castellanos

Digi Americas Alliance Members

aws Apple CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google

METABASE Q netskope paloalto NETWORKS Telefónica tenable

GRUPO RADICAL LUMU Trellix TREND MICRO Santander

Table of Contents

Executive Summary 6
Ransomware Attacks in Latin America 8
- Case Study: Colombia 9
- Case Study: Costa Rica 17
- Comparative Analysis Between Costa Rica and Colombia 23
- Case Study: Chile 24
- Case Study: Panama 30

Survey Findings 36
- Risk-Management Framework (RMF) 38
- Public Cloud 43

Results and Recommendations 47
- Policy Recommendations 47

Executive Summary

Ransomware is a prevalent cyber threat, particularly in Latin America, where organizational cybersecurity programs are in formative stages. While numerous factors can increase the risk of ransomware attacks causing serious harm in the region, the lack of cybersecurity policies and regulations across Latin America, as noted by the National Cybersecurity Index (NCSI), has further exacerbated these regional challenges.[i] Attacks on critical infrastructure may significantly disrupt the functioning of government and business alike and result in a ripple effect on the citizens of Latin American nations. This report uses the definition of critical infrastructure from the National Institute of Standards and Technology (NIST): "Systems and assets, whether physical or virtual, so vital to the State that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national health or public security, or any combination of those issues."[ii]

According to the Inter-American Development Bank (IDB), only seven of the 32 Latin American countries have plans to protect their critical infrastructure from cyberattacks, and only 20 have Computer Security Incident Response Teams (CSIRTs).[iii] The current level of cyber readiness in the region suggests that there is a notable deficit that must be addressed.

The annual cost of cyberattacks in Latin America and the Caribbean could exceed $90 million by 2025, with an average of more than 18.5 million attacks per year.[iv] Notable incidents include an attack on Costa Rica in April 2022, which affected numerous government agencies and demanded a $10 million ransom. Another attack in May 2022 targeted the Costa Rican Social Security Fund, causing disruptions in critical systems, including the completion of social security payments. These attacks caused the country to declare a state of emergency, becoming the first country to use emergency funds due to a cyberattack.[v] Similarly, Colombia experienced a significant ransomware attack from a third party in early September 2023, which severely disrupted vital services across the country. This attack directly impacted 20 public entities, while 78 additional public entities and 762 private companies were indirectly affected across Latin America as well as others in countries such as Argentina, Panama, and Chile.[vi]

Government networks, rich in sensitive information on their citizens, often lack security best practices, making them prime targets for cyberattacks. This report provides an analysis of current cybersecurity practices, identifies bottlenecks in incident response, and proposes effective measures to bolster cyber defenses in Latin America. The focus of this report is on approaches that governments in the region can adopt to help organizations in their countries mitigate risk.

The study involves both qualitative and quantitative analyses to comprehensively examine recent ransomware events in Colombia, Costa Rica, Chile, and Panama. These four countries were selected based on the extent to which they had experienced a significant incidence of cybercrime, particularly ransomware. Moreover, they were chosen based on their recent cybersecurity regulatory framework and their response to significant incidents of ransomware. The qualitative aspect comprised literature reviews and interviews, focusing on understanding the effectiveness and deficiencies of response tactics. The literature review included incident-reporting documentation, academic research, and government publications.

Through this review, an examination was conducted on the prevalence of ransomware attacks across the four countries as well as an analysis of their respective national cybersecurity policies and the cybersecurity challenges they face. Interviews with government officials provided insights into the incident-response landscape, lessons learned, and best practices. The government officials varied in both position and agency. Positions of interviewees ranged from national directors of cybersecurity and cybersecurity analysts to directors of risk management and digital transformation. They work in many different government agencies within the aforementioned countries, including ministries of technology and embassies. Topics encompassed government responses, existing policies, challenges, and the potential of risk-management frameworks (RMFs) and cloud solutions.

The quantitative analysis involved a survey that aimed to gather perspectives on the effectiveness of RMFs, such as the Cybersecurity Framework of the National Institute of Standards and Technology (NIST CSF), and the impact of migrating computing operations to cloud services in reducing ransomware risks. The survey used multiple-choice response options to increase response rates and was designed for simplicity and speed. The survey respondents comprised over 150 individuals in high-level roles across public and private sectors as well as civil society and academia who were from countries such as Colombia, Argentina, Costa Rica, Chile, and Guatemala. The combined findings, which focus on RMFs and public cloud adoption, aim to inform strategies for enhancing incident response and safeguarding critical infrastructure in Latin American countries.

One key takeaway of this study is that the constantly changing cybersecurity-risk environment is difficult to manage. Many countries in the Latin America region have relatively new but nonetheless promising cybersecurity capabilities. The findings of this report, compiled from the literature, interviews, and a survey of key stakeholders in the region, indicate substantial attack resilience in various Latin American countries. While each country have different backgrounds and cyber capabilities, they all responded to attacks and other challenges robustly, considering the limitations of their resources.

Key findings highlight potential areas of opportunity for improvement, such as a significant shortage of trained IT professionals, inadequate incident-response mechanisms, and a lack of cohesive cybersecurity policies across various sectors. Investments in cybersecurity are not keeping pace with increased digitalization and its associated risks, particularly within the government sector. Addressing the regional challenges posed by the prevalence of ransomware threats is imperative because of the early stage of organizational cybersecurity programs in Latin America and the absence of cybersecurity policy and regulation for critical infrastructure. As attacks on critical infrastructure can have far-reaching consequences on government operations, business continuity, and public welfare, the recommendations of this study focus on (1) bolstering investment in workforce development, (2) establishing voluntary RMFs, (3) investing in cybersecurity infrastructure and technologies, such as cloud-based cybersecurity infrastructure, and (4) forming centralized cybersecurity-management and reporting systems to mitigate these risks effectively.

RANSOMWARE
ATTACKS IN LATIN AMERICA

CASE STUDY:

COLOMBIA

Introduction

Strengthening cybersecurity has become an issue of profound strategic importance for nations worldwide. For countries like Colombia, which is third in the ranking of South American countries that have suffered the most ransomware attacks and simultaneously aspires to become a dominant force within the tech industry, it is imperative to develop national resilience against cyber risks.[vii] As such, this section examines Colombia's cybersecurity landscape, policies, cyberattacks, challenges, and future opportunities. It also discusses findings from interviews conducted with government officials following the ransomware attack in September 2023 and lessons learned from the incident.

Colombia defines critical infrastructure as follows. (1) The "Security Strategy: National Critical Infrastructure 2022–2032" describes critical infrastructure as the physical and virtual systems that allow the operation of essential and basic services at social, economic, environmental, and political levels.[viii] An alteration or interruption of these systems due to nature or man could have negative consequences for governments, states, and citizens, as they would not be able to conduct their daily activities, which would lead to the paralysis of the affected nation. Similarly, (2) Decree 338 of 2022 defines critical infrastructure as "Systems and assets, physical or virtual, supported by Information and Communications Technologies, whose significant impact would have a serious impact on the social or economic well-being of citizens, or in the effective functioning of the government or the economy."[ix]

Overview of Cybersecurity Policy in Colombia

Colombia manages its own digital-security policies through a series of National Council on Economic and Social Policy (CONPES) documents as well as relevant laws and regulations in the legal system. A major milestone was achieved with the passage of Law 1273 in 2009.[x] This law established provisions to combat computer crimes, including unauthorized system access, data destruction, and disruption of digital services.[xi] By defining illicit cyber activities, Law 1273 promoted a more secure and trustworthy digital environment.[xii] Complying with its statutes is essential for both public and private sector entities as Colombia continues its path toward digital transformation.

The Ministry of Information Technologies and Communications (MinTIC) has three primary plans for digital security: CONPES 3701, 3854, and 3995. In 2011, Colombia introduced the National Cybersecurity Framework, CONPES 3701, to provide guidelines and best practices for protecting critical infrastructure and core information systems.[xiii] The framework established the National Cybersecurity Committee to align cross-agency efforts and the national Computer Security Incident Response Team (CSIRT) to detect and mitigate cyberattacks.[xiv] In 2012, following guidelines established in CONPES 3701, Colombia also founded its first cyber unit by connecting three independent entities that were created to conduct distinct tasks in the cyberspace domain: the Ministry of Defense's Computer Emergency Response Team (ColCERT), the Joint Cyber Command (CCOC), and the National Police Cyber Center (CCP).[xv] The goal was to design a more coordinated effort among agencies.

CONPES 3854, enacted on April 11, 2016, established the National Digital Security Policy, which created conditions for various stakeholders to manage digital-security risks in their socioeconomic activities and fostered trust in the digital environment.[xvi] A significant contribution to this policy was the development of strategies that established an institutional framework for digital security with a preventive approach rather than reactive responses to potential threats. This policy also acknowledges the country's prior focus on cybersecurity for defense, security, and cybercrime and extends its scope to include risk management, reflecting the rising importance of information and communication technology (ICT) for socioeconomic progress. Additionally, the policy introduced the role of the national digital-security coordinator, who oversaw the Presidential Council for Digital Transformation, Management, and Compliance of the Presidency of the Republic.

Further enhancements were made through Decree 620 of 2019, which regulates Law 1273 while addressing emerging threats, such as denial-of-service attacks and critical-infrastructure protection gaps.[xvii] Decree 620 of 2020 established specific guidelines for the implementation of cybersecurity measures in the private sector to clarify and expand legal obligations alongside technological changes.[xviii]

Concerning data protection, Colombia enacted Law 1581 of 2012, and Decree 1377 to protect constitutional privacy rights[xix] This comprehensive framework imposes obligations regarding personal

data flows, access controls, and breach notifications across sectors. Colombia also instituted the National Database Registry to enable cyber-incident reporting between firms. While sectoral CSIRT's assist industries such as finance, telecommunications, and energy, the government CSIRT must overcome continuity and budget constraints. A proposed national digital-security agency aims to address such institutional capacity challenges.

In Colombia, CONPES 3995 of 2020, Decree 338 of 2022, and Decree 762 of 2022 are the most recent national cybersecurity policies and laws in force. CONPES 3995, the National Trust and Digital Security Policy, establishes measures to develop digital trust through improvements in digital security. It also seeks to generate conditions of security and coexistence to preserve and enhance national interests, independence, sovereignty, and integrity within the state. [xx] Decree 338 of 2022 establishes general guidelines to strengthen the governance of digital security in Colombia. The decree also creates the Digital Security Governance Model which aims to strengthen the management of digital security risks for essential services and critical cyber infrastructures in Colombia. Additionally, the Decree modifies the organization and operation of Colombia's internal cyber emergency response working group, ColCERT.[xxi] Decree 767 of 2022, the Digital Government Policy, aims to improve the efficiency, transparency, and quality of the services provided by the state. This policy upholds three key pillars: architecture, information security and privacy, and digital citizen services.[xxii] Additionally, a new enabler, "Culture and Appropriation," has been introduced (a technology enabler is a term used to describe a technology or set of technologies that provide a platform or foundation for the development of other technologies, products or services.[xxiii]) This enabler aims to enhance the capabilities of mandated entities and interest groups, ensuring their adeptness in utilizing and leveraging ICT for access and utility.

Overall, Colombia has strengthened its cybersecurity measures through the implementation of several laws and policies, beginning with Law 1273 in 2009 and continuing with more recent legislation, such as Decree 620 of 2019 and Decree 338 of 2022. These policies seek to protect the state's integrity, promote digital trust, and bolster defenses against cyberattacks. As Colombia proceeds with its digital transformation, adherence to these standards is crucial for organizations in the public and commercial sectors.

Private Sector Involvement and Contributions

Cyberattacks have become ubiquitous, affecting many types of systems, from corporate infrastructure to emails, applications, and private cloud-stored data. In 2023, approximately 29,000 attacks on corporate infrastructure, over 8,000 attacks related to information and database theft, and around 16,000 incidents linked to social networks and emails were reported.[xxiv]

In Colombia, the private sector actively contributes to cybersecurity efforts, prioritizing the protection of digital assets and sensitive information.[xxv] Private organizations adhere to specific international standards and regulations, such as the Cybersecurity Policy and Digital Security Policy, ensuring compliance to safeguarding against cyber threats.[xxvi] Collaborations with government bodies, including ColCERT, CCOC, and the Ministry of Information

Technologies and Communications (MINTIC), focus on advancing frameworks and integrating cybersecurity measures within critical sectors.[xxvii] Many private organizations actively participate in incident response through CSIRTs in critical sectors, ensuring resilience against cyber threats.[xxviii] These efforts demonstrate that the private sector, such as multinational tech companies, is deeply invested in strengthening Colombia's cybersecurity.

International Collaborations

In Colombia, important efforts are being made to advance the reduction of the digital divide among developed countries. Some of these international standards held as de facto references are those issued by the National Institute of Standards and Technology (NIST; Commerce, 2018) and ISO 27001.[xxix] Furthermore, Colombia passed Law 1928 of 2018,[xxx] leading to the adoption of the Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention.[xxxi] The Budapest Convention is the first international agreement aimed at combating cybercrime, or crimes involving computers and the internet, by bringing national laws into compliance, enhancing investigative methods, and fostering international cooperation.[xxxii] This incorporation introduced all the obligations related to cybercrime outlined in the Budapest Convention into the Colombian legal framework. On March 16, 2020, the Council of Europe officially announced that Colombia had acceded to the Budapest Convention, thereby becoming the 65th country to join.[xxxiii]

In 2020, Colombia implemented a free-trade agreement (FTA) with Israel, which had been signed in 2014. The FTA with Israel promoted collaboration in sectors such as technology, innovation, cybersecurity, and agricultural and industrial growth. This agreement is relevant in the context of the government's objective to make innovation the foundation of the Colombian economy.[xxxiv] Moreover, in 2022, Israel made a significant contribution to the enhancement of cybersecurity capabilities in Latin America, particularly in Colombia and the Caribbean. This contribution of $2 million was given to the Interamerican Development Bank, which will lead the cybersecurity initiative.[xxxv]

Colombia has been actively involved in the international arena, demonstrating leadership and participation in various crucial forums. In 2018, the country achieved a significant milestone by being elected as the inaugural chair of the Cyber CBMs Working Group at the Organization of American States (OAS).[xxxvi] This appointment underscores Colombia's commitment to promoting cooperation and dialogue on cybersecurity issues within the region. Moreover, Colombia maintains an active engagement in international organizations, such as the United Nations (UN) and the International Telecommunication Union (ITU), where it contributes to global discussions and initiatives related to technology, telecommunications, and cybersecurity.[xxxvii] Additionally, Colombia collaborates with multilateral financial institutions, such as the Inter-American Development Bank (IDB), the World Bank, and the Corporación Andina de Fomento (CAF), to address development challenges and advance projects that promote economic growth and sustainability both domestically and across the region. Through these engagements, Colombia has demonstrated its dedication to fostering collaboration, sharing best practices, and addressing global challenges in the digital age.

Cybersecurity Challenges in Colombia

In recent years, Colombia, like the rest of the region, has faced heightened vulnerability to cyber threats, which have been driven by rapid technological advancements and digitalization accelerated by the COVID-19 pandemic. This surge in digitalization and internet penetration elevates the likelihood of potential vulnerabilities and cyberattacks if not accompanied by appropriate security measures to protect the enlarged digital environment. In 2021, Colombia ranked among the Latin American countries most frequently attacked by malicious actors, reflecting a concerning upward trend.[xxxviii] A 2022–2023 study by the Colombian Chamber of Informatics and Telecommunications uncovered that victims registered a cyber-incident complaint every eight minutes.[xxxix] In the last two years, Colombia experienced two major ransomware attacks.

First, in December 2022, Colombia's healthcare system suffered a significant blow from a data breach.[xl] The perpetrator used RansomHouse ransomware to compromise the networks of Keralty, a large healthcare provider.[xli] The breach exposed thousands of users' sensitive health data, including names, addresses, social-security numbers, and medical records.[xlii] This healthcare breach had cascading impacts nationwide as hospital scheduling systems failed, leading to longer wait times for patients or loss of access to essential services altogether.[xliii] Spurred by this attack, Keralty invested heavily in new security measures and expert personnel to bolster its defenses.[xliv]

Second, in September 2023, Colombia's internet service provider, IFX Networks, reported being the victim of a ransomware attack.[xlv] Around 78 Colombian state entities and 762 private companies were impacted by the attack, including[xlvi] the Ministry of Health and Social Protection, the country's judiciary branch, and the Superintendency of Industry and Commerce.[xlvii] This incident significantly impacted the day-to-day operations of the Colombian government. For example, two million scheduled legal proceedings were suspended for seven days because the judicial branch's web portals were completely frozen and there was no way to determine the status of proceedings in the system.[xlviii] Many health centers also lost their online services, meaning that patients could not make medical appointments or obtain their prescriptions because doctors could not access patients' medical records.

The presidential advisor for digital transformation led the Colombian government's unified cyber command post, which oversaw the response to the 2023 attack. The advisor sent out approximately nine information bulletins before the event ended and the country returned to normal. The presidential advisor also ensured that the entities' affected platforms and applications continued to function properly during the event. According to a public press release from IFX, IFX was able to recover 90% of the information on the tenth day after the attack. Many government officials expressed that this attack was considered the "largest on infrastructure in Colombia in recent years" and has prompted the country's legislature to approve a new ministry and create the National Agency for Cybersecurity and Space Affairs.[xlix]

In November 2023, two bills were introduced to the Colombian legislature to create a technical and specialized digital-security authority.[l] The first bill, filed on July 24,

proposed the creation of the National Digital Security Agency (ANSD from its acronym in Spanish), led by members of congress. The second bill was led by the Ministry of Information Technology and Communications and aligned with the Ministry's cybersecurity strategy presented earlier that month. This bill was broader than the first, calling for both a digital security and space agency (ANSDAE from its acronym in Spanish). These proposals for managing digital security in Colombia differ in their organizational attachment and scope of responsibilities. The MinTIC suggests establishing the National Agency for Digital Security and Space Affairs under the presidency, potentially granting it "extraordinary powers." In contrast, the senators' proposal recommends attaching the agency to the ICT Ministry to oversee existing resource allocations and avoid additional expenses. Additionally, the senators' proposal emphasizes obligating both public and private entities to disclose cyberattack risks for the agency's support, while the MinTIC proposal lacks such obligations.While Colombia has developed a legal and policy foundation for national cybersecurity, challenges to achieving full implementation and addressing capability gaps persist. To navigate the evolving threat landscape, sustained efforts are needed to enhance technical expertise, improve information sharing, provide regulatory clarity, and align strategic directions.

Underscoring the Criticality of Cybersecurity and Calling for Binding Governance

Across the interviews conducted, there was unanimous consensus over the significant cyber risks around sensitive data protection and national security in Colombia, especially following the major ransomware attack experienced in September 2023. This consensus highlighted alignment around the foundational importance of cybersecurity as a national priority for continued focus and investment. Participants emphasized the importance of enacting comprehensive and enforceable legislation and policies and formalizing national cybersecurity governance. Similarly, interviewees agreed that binding rules and institutional coordination were essential measures to drive accountability, transparency, and effectiveness in preparation and response.

Grappling With Incident-Response Gaps

A major finding was that incident response is currently inefficient. Participants cited ongoing difficulties in quickly and accurately detecting attacks and determining their origin amidst the complexity of cyber threats. Additionally, participants emphasized complications in assessing and containing downstream impacts, as attacks spreading to interconnected systems become increasingly difficult to track. These systemic response deficiencies indicate important areas where developing capabilities are required to mitigate cyber risks. Moreover, input from those interviewed, coupled with responses from the survey, which will be discussed in a later section, highlighted the necessity of continued communication within and between organizations. Specifically, many interviewees indicated the need for implementing simple cybersecurity measures that allow for more effective preparation and containment of attacks when they do occur.

Recognizing Education as an Essential Cornerstone

Interviewees also uniformly agreed on the need for expanding training programs and cultivating cyber awareness across both public and private-sector entities, as well as the general population in Colombia. Developing talent and culture around cybersecurity thus emerges as a foundational investment to drive maturity, resilience, and risk reduction over time across organizations and citizens alike. Interviewees emphasized that robust software and response systems alone cannot sufficiently mitigate cyber risk and enable effective incident response. Significant investment in cultivating human talent and cybersecurity expertise across teams tasked with detection, containment, and recovery from attacks is also required.

Perspectives on Cloud Adoption to Decrease Cybersecurity Risks

Numerous participants highlighted the importance and benefits of working with best-in-class communications service providers (CSPs) to manage cybersecurity risks. Participants also highlighted that security benefits should be considered in conjunction with the ability to control how data is accessed and processed.

Evolving Cybersecurity Frameworks

The interviews revealed that evolving cybersecurity strategies and regulations are necessary to address new threats. One interviewee specifically discussed continuing initiatives to encourage the use and understanding of the most recent iteration of the NIST 2.0 framework. Furthermore, the emphasis on broader legislative development processes suggests a proactive approach aimed at bringing Colombia's cybersecurity governance in accordance with risk-management frameworks (RMFs). Doing so will allow for the integration of best practices and the preservation of flexibility in the face of evolving attack techniques.

Embracing International Collaboration

Finally, participants voiced unanimous consensus for expanded international technical exchange, assistance, and cooperation mechanisms to help expand capabilities and collective learning in managing the sophisticated global cyber threats impacting Colombia. This finding reveals an awareness that, while many vulnerabilities require internal capacity building, threat environments transcend borders and can be managed more effectively with an international effort.

CASE STUDY:

COSTA RICA

Introduction

Costa Rica has gradually adopted a strategic approach to international cooperation on cybersecurity, leveraging regional programs, treaties, bilateral partnerships, and foreign assistance to systematically build capacity. This section provides an analysis of Costa Rica's cybersecurity environment, laws, threats, difficulties, and prospects. As digitization advances, specific solutions to protect national security, business interests, and citizen rights arise. These solutions can be informed by a detailed understanding of Costa Rica's cybersecurity landscape, especially after the major ransomware attack in 2022.

Overview of Cybersecurity Policy in Costa Rica

In 2012, the Law on Cybercrime 9048, the country's first comprehensive law aimed at combating cybercrime and hacking, marked the beginning of Costa Rica's serious efforts in cybersecurity.[li] This law established legal frameworks to criminalize and prosecute different cyber breaches, such as unauthorized system access, data and system sabotage, and electronic fraud. The law's introduction sparked the establishment of specialized cyber police units and cybercrime prosecution capacities within the public sector.[lii] That same year, the Costa Rica Computer Security Incident Response Team (CSIRT-CR) was created under Executive Decree 37052-MICITT.[liii] This decree designated CSIRT-CR as the agency responsible for coordinating all matters related to informatics and cybernetics security. Furthermore, it empowered CSIRT-CR to maintain a team of ICT security experts tasked with preventing and addressing incidents affecting governmental institutions. CSIRT-CR's mission includes implementing and managing technological measures aimed at reducing the risk of attacks on community systems, integrating cybernetic security systems and information technologies into the protection frameworks of the central government and autonomous entities, and mitigating cybernetic risks and threats.

In 2011, Costa Rica approved and published Law 9868, which subsequently went into effect in 2012. This law, called the Law for the Protection of the Person Against the Processing of Their Personal Data ("Ley de Protección de la Persona Frente al Tratamiento de Sus Datos Personales"), has remained unchanged since its publication.[liv] The law applies to personal data that appears in the automated and manual databases of public and private organizations and to any subsequent use of this data.[lv]

In 2014, Costa Rica introduced a pivotal national cybersecurity policy with a national development plan that identified core public and private sector objectives, including fostering a culture of cyber-risk awareness, safeguarding vital infrastructure, and improving incident preparedness.[lvi] Additionally, mandatory cyber-incident reporting obligations were imposed on operators of critical systems to facilitate threat monitoring.[lvii]

Similarly, in 2017, the Government of Costa Rica developed its 2017–2021 National Cybersecurity Strategy, which established an institutional framework that advanced its functions and activities under the leadership of the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT, from its acronym in Spanish) and the CSIRT-CR.[lviii] This strategy outlined a strategic vision and priorities to systematically strengthen cyber defenses across government agencies and critical-infrastructure operators. Moreover, the national strategy defined critical infrastructure as "information systems and networks that, if compromised, could significantly affect citizens' health, physical and operational safety, economy, welfare, or the effective functioning of the government and the country's economy." Additionally, the strategy emphasized the need for delineating the country's critical infrastructure and establishing a policy-making committee comprising representatives from public and private entities classified as critical infrastructure.

In November 2023, the government of Rodrigo Chaves introduced a new cybersecurity plan, the 2023–2027 National Cybersecurity Strategy, following the cyberattacks in 2022, which prompted a state of emergency in the country.[lix] The effort presented a strategic vision that bolsters the leadership of the national government and intends to unite all stakeholders around human rights.[lx] This strategy outlines how to improve infrastructure protection and national cyber resilience, boost cybersecurity governance, modify the cyber legal framework, support the cybersecurity ecosystem, and collaborate actively in the digital sphere.[lxi]

Private-Sector Involvement and Contributions

The private sector has also been impacted by increasing cyberattacks in Costa Rica. In August 2020, the country's first cybersecurity cluster, the Cybersec Costa Rica Cluster initiative, was created to position Costa Rica as a leader in the Central American region.[lxii] The initiative is a public–private alliance between companies, chambers, academia, and public institutions that presents the first broad international cybersecurity cluster in the region to improve competitiveness in the country.[lxiii]

In February 2022, Executive Decree 43425-MEIC-MTSS established the National Cluster Program (PNC) as a matter of public interest.[lxiv] The decree empowers ministries to align regulatory frameworks and initiatives, allowing the PNC to positively impact productive development and job creation. The cluster model represents an innovative approach to a public–private partnership, emphasizing collaboration and trust among stakeholders.[lxv] Participants include Digi Americas members, featuring major multinational companies across different sectors, such as Amazon Web Services and Cisco.[lxvi] The cluster strategically focuses on developing and strengthening the cybersecurity ecosystem and enhancing the cybersecurity workforce. Costa Rica is the first Latin American country with a PNC program declared by executive decree.[lxvii]

International Collaborations

Costa Rica has actively pursued international cybersecurity partnerships for over a decade, beginning with the OAS Cyber Security Program in the late 2000s.[lxviii] This program involved cyber training and capacity building for Costa Rica's public and private sectors. In 2019, Costa Rica recognized the OAS Working Group's leadership in coordinating regional incident response and establishing cooperative frameworks of action for cyber threats.[lxix] In 2017, Costa Rica became a signatory to the Budapest Convention. Costa Rica also remains actively engaged in the United Nations Open-Ended Working Group (UN OEWG) forum on cyber governance and has committed to ongoing participation until 2025.[lxx] At the 2022 OEWG, Costa Rica reiterated its commitment to applying international law and norms, including principles of proportionality and humanity, to the state's use of ICTs.[lxxi]

Regarding specific collaboration with other countries, Japan supported Costa Rica's early development of a national CSIRT through the Japan International Cooperation Program (JICA) program.[lxxii] Furthermore, Costa Rica signed a memorandum of understanding (MOU) with Israel[lxxiii] on cyber capabilities and cooperation in cybersecurity.[lxxiv] This memorandum was beneficial during the ransomware attack

in 2022, when Israel provided relevant intelligence and increased the Costa Rican government's understanding of which systems were attacked and subsequently shut down.[lxxv] Another key collaboration was with Spain, which also provided technical support and donated protection tools during the ransomware attack in 2022.[lxxvi] In 2023, the United States announced plans to provide $25 million in assistance for Costa Rica to establish a cybersecurity operations center by 2026 in response to the ransomware attack, which will provide advanced equipment, specialized training, and logistics aid to Costa Rica's Ministry of Public Security.[lxxvii] Additionally, Costa Rica has formalized cyber agreements with the Dominican Republic and Panama.[lxxviii] Through MOUs, Costa Rica's MICITT and its counterparts are exchanging best practices and policies to align with Costa Rica's National Cybersecurity Strategy.

Costa Rica continues to be a focal point for cybersecurity capacity building in the region. In September 2024, the Center for Cybersecurity Policy and Law (CCPL), along with its Digi Americas Alliance, will host the Latin America Chief Information Security Officer (LATAM CISO) Summit 2024 in Guanacaste, Costa Rica. This exclusive summit brings together the most senior cybersecurity leaders, operators, and influencers from Ibero-America to discuss the most critical and challenging threats and trends in the digital world. Topics will include critical-infrastructure protection, digital identity and privacy, 5G, emerging threats and trends, and the evolution and challenges of the financial technology (fintech) industry, among other relevant issues. The European Commission, through Expertise France, has confirmed its support of this initiative, inviting high-level government officials from the EU-LAC Digital Alliance. The LATAM CISO Network comprises thought leaders involved in cyberspace and digital-policy development in the Americas region who understand the value of proactively engaging with governments, the private sector, civil-society organizations, and international organizations to shape and advance common cybersecurity and digital-policy priorities.

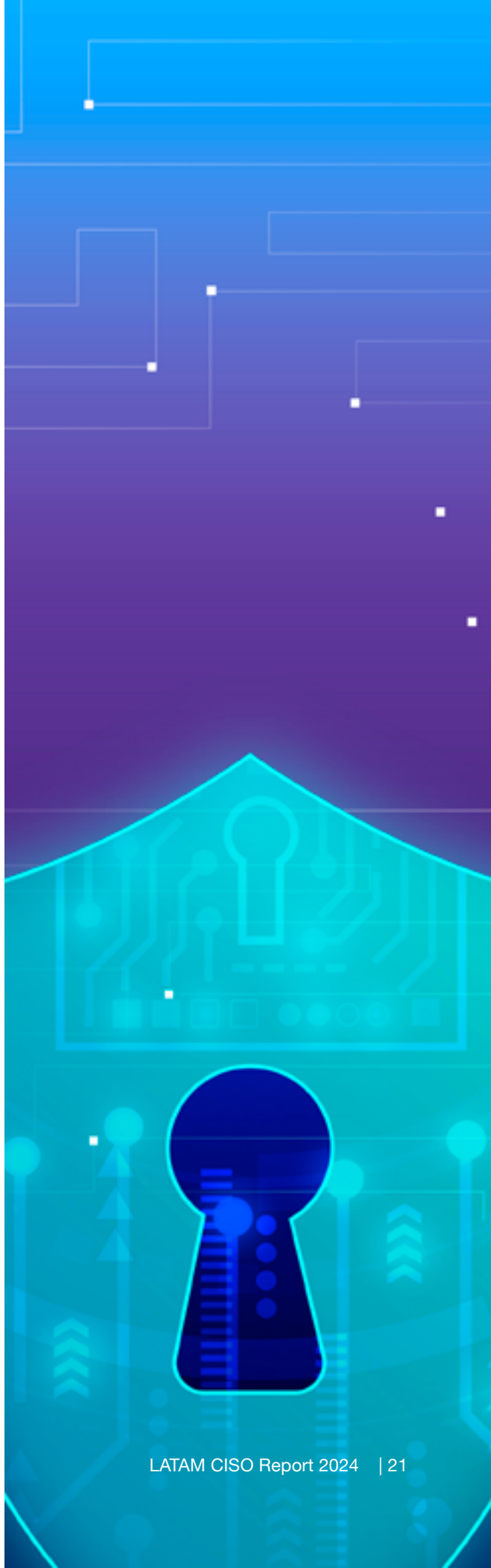
Cybersecurity Challenges in Costa Rica

In April 2022, Costa Rica was subjected to the fifth largest global cyberattack by the Russia-based ransomware group Conti.[lxxix] Specifically, Conti demanded $10 million in exchange for not leaking sensitive data stolen from the Ministry of Finance ("Hacienda"), including citizen tax records.[lxxx] Conti encrypted and stole sensitive data, causing the shutdown of critical tax-filing systems and, in turn, creating economic turmoil.[lxxxi] On May 31, 2022, Costa Rica was the victim of a second attack where the Hive group exploited stolen credentials to gain access to the Social Security Agency ("Caja Costarricense de Seguro Social" or CCSS), thus shutting down the agency's systems.[lxxxii] New attacks persisted, with another hacker disabling medical systems, which led to the cancellation of over 158,000 medical procedures.[lxxxiii] All successful attacks were on local data centers or the private cloud. Tax collection was severely impacted because the online systems dedicated to this task were compromised. Many government functions, such as the public medical system and tax-collection systems, reverted to manual documentation.[lxxxiv] Costa Rica never paid the ransom demanded.[lxxxv] While Conti disbanded after the Russian invasion of Ukraine, the country became a cautionary lesson for the region. The ransomware group explicitly called for the overthrow of the Costa Rican

government, as well as stating that this should serve as a warning to the rest of the world.[lxxxvi]

As of June 2022, the Costa Rican government has spent approximately $24 million on response operations, including money from the national emergency fund and agency resources.[lxxxvii] Around $4 million was allocated by the national emergency fund to various government agencies for recovery. Costa Rica became the world's first nation to declare a state of national emergency due to a cyberattack.[lxxxviii] The rehabilitation phase alone cost the CCSS over $18 million of its own funds, and emergency funds were not used. However, the amount of money lost due to postponed export–import regulations was reported to have ranged from $38 million per day to $125 million over 48 hours.[lxxxix] The infrastructure has not been fully repaired eight months after the catastrophe, and thousands of citizens are still experiencing its effects.

In conclusion, despite not paying ransoms, Costa Rica's government and infrastructure were rendered inoperable for months by the catastrophic cyberattacks of 2022. This vulnerability was exacerbated by the lack of a national cybersecurity law, limited progress on a modern data-protection bill, and constrained CSIRT resourcing. According to the 2020 Global Cybersecurity Index (GCI) published by the ITU, Costa Rica's regional position has deteriorated from eight to 18.[xc] Ensuring resilience and deterrence remains imperative to avoid similar crises.



Elusive Cyber-Incident-Response Preparedness

The main takeaway from the interviews was the gap in response preparedness, which was highlighted by all participants. These deficiencies ranged from inadequate staffing and technological capabilities to communication gaps between public and private-sector entities. Interviewees consistently identified cyber-incident response as an area needing immediate improvements in planning, protocols, and coordination exercises between interdependent institutions. Compounding these systemic unpreparedness issues, participants repeatedly emphasized budget and skilled-personnel deficits that critically inhibit the vital resource mobilization required to invest in robust modernized cybersecurity and rapid mitigation capacity across both public and private institutions. Overall, the gravity of the attack in 2022 prompted shifts, resulting in a mandate to grow response teams, develop protocols, and pursue international assistance.

Rippling Economic Impacts

Participants shared that the economic repercussions of the ransomware attack in 2022 affected a wide range of sectors. The disruption of payment systems managed by the Ministry of Finance, which affected financial transactions, imports, exports, and public services, underscored the far-reaching consequences experienced by all interviewees.

Recognizing Education as an Essential Cornerstone

Most interviewees stated that, in the wake of the attack, cybersecurity had become a higher priority for their organizations and agencies through initiatives including developing incident protocols, updating national strategy, and exploring outside alliances. However, while governance and capabilities require strengthening, participants also cited a prevailing lack of cyber hygiene and threat awareness among end users (person who actually uses a particular product) as factors frequently exacerbating incident success and containment difficulties. As such, awareness campaigns and cybersecurity-culture cultivation can embed an important human layer into cyber defense.

Perspectives on Cloud Adoption To Decrease Cybersecurity Risk

Interviewees mentioned that numerous government agencies have already adopted cloud services and acknowledged their value in risk mitigation. While interviewees recognized potential benefits, such as improved access and performance, some still had concerns about the costs and potential security risks associated, without specifying if the concerns were around public or private cloud services.

Evolving Cybersecurity Frameworks Centered on NIST

Interviewees expressed hope that existing RMFs, like the Cybersecurity Framework of the National Institute of Standards and Technology (NIST CSF), could be adopted in the absence of mature domestic regulations. In late 2023, the US embassy conducted

joint cybersecurity training initiatives with Costa Rican officials that were centered on the NIST CSF and engaged IT and cybersecurity personnel from across the Costa Rican government. These cooperative training sessions demonstrate that Costa Rica is actively investigating the adoption of an RMF as a crucial element of capacity building that surpasses the trainings.

The ransomware attacks illuminated the preparedness gaps facing Costa Rica and encouraged the country to invest in the construction of vital infrastructure. This spike in investment has led to a major shift in the leadership of Costa Rica's cybersecurity readiness and the development of thorough procedures.

Comparative Analysis Between Costa Rica and Colombia

The ransomware responses in Costa Rica and Colombia revealed significant internal deficiencies in the areas of impact assessment, communication, and detection. Chronic shortages in funds and expertise hinder improvement initiatives in unique ways. While Colombia seeks to improve incident tracing capabilities, Costa Rica suffers from resource deficiencies that thwart existing CSIRT operations and containment coordination. Both countries acknowledge insufficient technical preparation and the need to increase the cybersecurity workforce.

Accordingly, Colombia pursued internal capacity building, particularly around threat intelligence. Costa Rica, however, focused more on international partnerships to uplift response capacities across dimensions such as forensics and workforce training. Regarding RMF implementation, both countries are developing cyber-governance strategies centered on selectively adopting NIST frameworks as a global standard, though Costa Rica has undertaken more tangible training initiatives thus far.

Finally, both countries acknowledge the importance of strategic evolution but have taken different approaches to implementation. While they have in the past relied on assistance from foreign allies to strengthen cyber-response readiness, Columbia and Costa Rica recognize that preparing themselves for more cyber threats is the safest way to move forward.

CASE STUDY:
CHILE

Introduction

Attacks on private companies or government agencies can affect the economic and social environment of any country, especially a developing nation like Chile. Understanding a country's specific challenges, infrastructure, and resources is critical to developing a strategy for mitigating the impact of future cybersecurity incidents. This section studies the cybersecurity landscape of Chile, including its history and current concerns and challenges.

Overview of Cybersecurity Policy in Chile

Starting in the early 2000s, Chile passed multiple laws governing the security of electronic communications within the government. However, it was not until 2015 that Chile passed Decree 533, which created an Interministerial Committee for Cybersecurity to advise on national cybersecurity policy and coordination.[xci] This decree defined cybersecurity, outlined the committee's functions, and mandated the creation of a technical advisory commission.[xcii] The committee consisted of representatives from relevant government bodies and met regularly to propose coordination protocols and provide technical advice. Through this committee, Chile ensured that it would spearhead the efforts of cybersecurity on a national level rather than developing it through private actors.

In 2017, Chile presented its first National Cybersecurity Policy of 2017–2022.[xciii] The policy presented two policies on implementing long-term objectives for Chile to achieve a safer cyberspace. Specific objectives included developing a robust information infrastructure to resist and recuperate from cyber incidents, developing a national cybersecurity industry, and participating in international forums.[xciv] In 2018, Congress passed a law establishing October as the country's Cybersecurity Month, which aimed to create public awareness and education on the issue, signaling a shift by Chile's government towards prioritizing cybersecurity.[xcv]

In 2019, the Department of Interior and Public Safety proclaimed a resolution that established a subdivision called the Cybersecurity Coordination Unit.[xcvi] The department then expanded and updated the unit in 2023.[xcvii] The purpose of this unit was to conduct the president's cybersecurity recommendations for policies, laws, and regulations.[xcviii] These recommendations included best practices, ideal protocols and infrastructures, greater coordination among sectors, and training.[xcix] Through this new unit, the CSIRT was created.[c] This team is tasked with coordinating the response to incidents within the country and supporting different government departments with incidents that may affect their operations.[ci]

Chile continues to develop standards and goals for its cybersecurity and related infrastructure, especially with the passage of the Chile Digital Agenda 2035 in 2022. This digital strategy aims to digitize 95% of public services by 2025 and 100% by 2035.[cii] The strategy's explicit focus on cybersecurity outlines five goals: (1) establishing a dynamic cybersecurity ecosystem, (2) creating an institutional framework to disseminate cybersecurity across the population, (3) improving high-quality cybersecurity training and education programs, (4) addressing current legislation on cybersecurity, and (5) ensuring the existence of mechanisms that allow for cooperation between borders. Recognizing the critical importance of cybersecurity, Chile is prioritizing collaborative efforts among the private, academic, government, and international sectors to manage these challenges effectively.

On December 4, 2023, the National Cybersecurity Policy 2023–2028 came into effect.[ciii] Understanding that technology changes rapidly, Chile has put this Policy in effect only during the period of 2023–2028.[civ] Furthermore, this policy encouraged the passing of the Cybersecurity Framework Law ("Ley Marco de Ciberseguridad") to

further combat security concerns. The Chilean Congress passed the proposed law, which will create a new cybersecurity agency: the National Cybersecurity Agency (ANCI).[cv] This proposed law was approved by the Constitutional Tribunal and published in the Official Gazette. Ramón Molina, executive director of the UC Innovation Center and co-chair of the initiative, said that "the law also highlighted that the agency may fine violators of cybersecurity regulations, where the sanctions are categorized as light, ranging between 0 to 5000 UTM for Essential Services (SE)."[cvi] In Chile, essential services encompass those provided by the administration, the National Electrical Coordinator, and public-service concessions. Other essential services may include the generation of electricity; the transportation of fuels; the supply of drinking water; telecommunications, digital infrastructure, and information technology managed by third parties; air, rail, or sea transportation; financial services; health services; and pharmaceutical products.[cvii]

In addition to the creation of the ANCI, the law will also create the National CSIRT, the CSIRT of National Defense, the Multisector Council on Cybersecurity, and the State Secure Connectivity Network. As described by the Minister of Internal Affairs and Public Security, Carolina Tohá, this new law will define standards for providers of essential services with the help of institutions specifically designed and certified to validate those standards.[cviii] Moreover, the law will provide education and workshops for workers, tabletop exercises, simulations and analyses of the networks, and information and detection systems.[cix] These institutions will have an active duty to report any incident or breach to the CSIRT.[cx] Furthermore, the new law will enable the creation of different sector-specific CSIRTs to manage the cybersecurity of the corresponding industries, such as the new defense CSIRT.

The ANCI's purpose is to improve and extend the work of the CSIRT through the consolidation of tasks and increased resourcing.[cxi] The agency will advise the president of Chile on the national cybersecurity policy and any related programs.[cxii] Key provisions include specific reporting obligations, fines for non-compliance, mandates for private companies to address incidents, and enhanced coordination between public and private sectors.[cxiii] Furthermore, it will create a special category of vitally important operators for providers of essential services that depend on information networks and systems.[cxiv] The law, through the ANCI and other actors, will require special duties from these operators, such as security systems, training, and constant analysis.[cxv] By establishing the standards for essential services and operators, the agency would ensure the protection of digital assets and citizen information.[cxvi] Overall, the law aims to strengthen Chile's cybersecurity posture and position the country as a leader in the region.

Private-Sector Involvement and Contributions

As described above, the proposed law will apply to companies within the private sector that provide essential services. The private sector is heavily involved in the development and application of different cybersecurity measures. Many private organizations have surfaced to address the cybersecurity concerns of private companies, specific sectors, and other industries. One of these organizations is the Alianza Chilena de Ciberseguridad, which was founded by nine

institutions representing important industries in Chile, such as transportation and defense. This organization includes collaborative efforts by different government, private, and educational organizations.[cxvii] Another organization is the Instituto Nacional de Ciberseguridad de Chile, which educates and raises awareness of information security to increase societal trust from individuals and companies.[cxviii] Similarly, the emergence of regionally focused trade associations has sought to strengthen the development of the technology industry in Chile. An example of one of these associations is Chiletec, a group of over 100 Chilean companies in the technology sector.[cxix]

International Collaborations

Chile is a signatory to the Budapest Convention, which is "a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergencies, beyond the specific provisions foreseen in this Convention."[cxx] Through these conventions, Chile seeks to align its efforts with international norms, standards, and best practices and universally accept the definition of cybercrime.

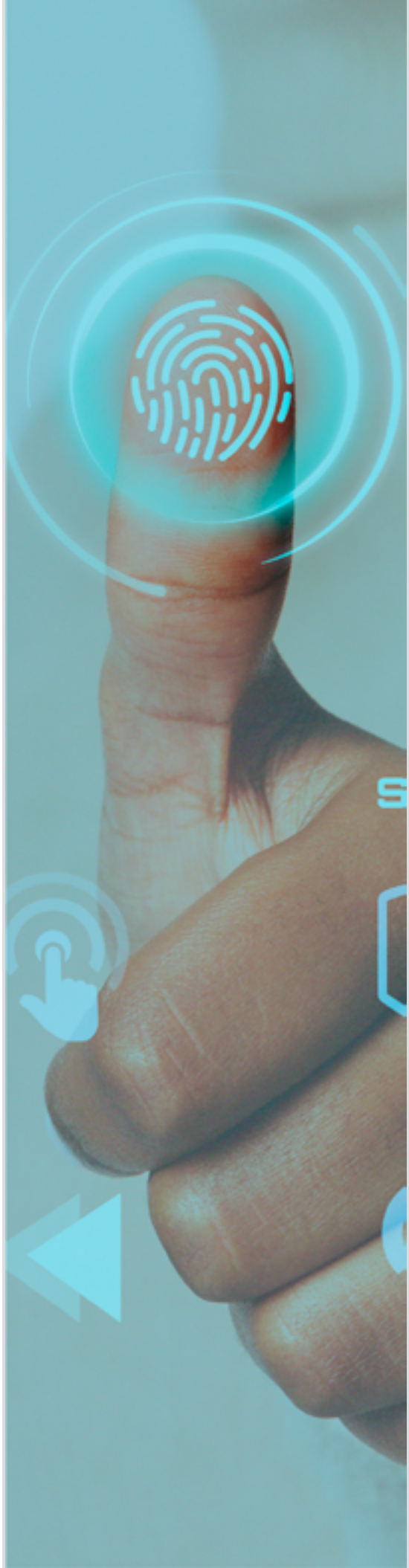
Furthermore, Chile is attempting to spearhead the cybersecurity movement in Latin America by hosting international stakeholder engagement. The 9th Congreso Latinoamericano Tecnología y Negocios America Digital 2024 will occur in Santiago in April, where more than 5000 C-suite professionals are expected to attend sessions on technology and business.[cxxi]

Cybersecurity Challenges in Chile

The increasing digitalization of Chile will present cybersecurity risks if services and structures are not properly secured and incident response is not prioritized. In addition to the severe consequences suffered from the IFX network attack in Colombia, Chile has also experienced substantial cyberattacks in recent years.[cxxii] For example, in May 2023, the Chilean Army suffered a cyberattack by a ransomware group called Rhysida, which affected the army's internal networks and led to a data breach.[cxxiii] During the attacks, the army's websites were intermittently unavailable, and Rhysida published 30% of the stolen data to their leak site after the attack.[cxxiv] The root cause of this attack is still unclear, but an arrest was made against a member of the army for his alleged participation in the attack.[cxxv] Similarly, in October 2023, the ransomware group Black Basta infected part of the digital infrastructure of Chile's National Customs Service.[cxxvi] The Ministry of Interior and Public Security's CSIRT issued a warning upon detecting the infection but specified that the incident occurred in a limited part of the digital infrastructure.[cxxvii] Despite the network disconnection, it was ensured that the incident did not disrupt customs' operations, and preventive measures were taken to avoid breaches.[cxxviii]

Another cybersecurity challenge in Chile is a shortage of specialized workers in the IT industry. The National Training and Employment Service (SENCE) predicted that by mid-2022 there would be an annual deficit of about 6,000 IT professionals in Chile.[cxxix] According to a study conducted by Fundacion Pais Digital and Accenture, Chile could lose nearly $13 billion in growth by 2030 if the Chilean population is not prepared for the market skills needed in the sector.[cxxx]

Overall, Chile's cybersecurity architecture and infrastructure have greatly improved in recent years. Chile demonstrates a commitment to managing cyber risks holistically, as seen by the creation of the Interministerial Committee for Cybersecurity and the passing of legislation such as the National Cybersecurity Law. Cybersecurity resilience has been further improved by cooperation with international partners and the commercial sector. However, issues such as the lack of qualified IT workers and persistent cyberthreats emphasize the significance of continual attention to detail and financial support for cybersecurity initiatives.



Chile's Cybersecurity Posture

The interviewees shared that some existing laws have gaps related to enforcement mechanisms, although they share optimism for the Cybersecurity and Critical Infrastructure Framework Law to combat some of these issues. The interviewees believed there have been efforts to shift regulations towards flexible principles rather than specific technologies, given the rapid rate of change in the industry.

Many interviewees also observed a lack of efficiency in the existing legal framework but a sense of optimism for laws that are in the process of being passed. The Cybersecurity and Critical Infrastructure Framework Law will provide a more updated framework and the creation of a new federal agency for cybersecurity. However, concerns still exist among experts that an agency of that size and scope will need more resources than are currently given to achieve its goals.

Perspectives On Regional Trends

Chile shares the reactive strategy seen across Latin America: experiencing attacks, responding accordingly, and enhancing resilience afterward rather than undertaking proactive prevention. Like other countries in the region, Chile's rushed pandemic digitization exacerbated security gaps in a more interconnected society. These gaps were addressed by a robust law on cybersecurity passed in December 2023.

Evolving Cybersecurity Frameworks Centered on NIST

Interviewees expressed that Chile values RMFs for baseline best practices but emphasized that these frameworks require localization. With different operational models and legal systems, one-size-fits-all approaches cannot address country-specific policy- and threat-landscape issues. Nonetheless, global frameworks can inform Chile's efforts to develop agile regulations focused on enduring principles rather than temporary technologies.

Perspectives on Cloud Adoption to Decrease Cybersecurity Risks

In 2023, the Chilean government released a guide[cxxxi] for the use of cloud services in the public sector. This guide seeks to provide uniform definitions, guidelines, and best practices for public bodies using cloud services within the framework of a "cloud smart" approach. This approach recommends public bodies to adopt public cloud solutions where it is suitable for their objectives, provides adequate data protection, and offers financial value.

CASE STUDY:

PANAMA

Introduction

This literature review emphasizes Panama's commitment to creating a strong and flexible cybersecurity infrastructure. It examines Panama's distinct approach to protecting national security, economic interests, and the rights of its citizens in a world that is becoming increasingly reliant on digital technology. This review lays the groundwork for an in-depth analysis of Panama's methods, obstacles, and advancements in the field of cybersecurity.

Overview of Cybersecurity Policy in Panama

Over the past decade, Panama has emphasized the protection of essential services with their "strategy focused on building confidence in the use of cyberspace in order to derive benefits of connectivity with minimal risk."[cxxxii] Beginning in 2011, Panama established a comprehensive national cybersecurity strategy, with a notable effort being the creation of a CSIRT.[cxxxiii] This team was tasked with addressing cybersecurity incidents impacting both the public and private sectors.[cxxxiv] In 2013, Panama also established six pillars of their cybersecurity strategy: (1) protecting privacy and human rights, (2) preventing and punishing cybercrime, (3) fortifying national critical infrastructure, (4) building a national cybersecurity industrial base, (5) developing a culture of cybersecurity, and (6) improving the security and response capability of public entities.[cxxxv] In alignment with these six pillars, the CSIRT states that their objectives include the "prevention, treatment, identification, and resolution of attacks on security incidents on the computer systems that make up the country's critical infrastructure and access to information from Panamanian citizens."[cxxxvi] In addition to meeting these objectives, CSIRT Panama is also responsible for increasing the nation's general understanding of cybersecurity to not only raise awareness and digital literacy but also actively combat cyber threats and online service disruption.[cxxxvii]

In March 2019, Panama enacted Executive Order 285/2021, which regulates privacy and data-protection laws in the country. This law requires data processors to obtain the prior consent of data subjects and be duly informed of the proposed use of their personal data. Panama's National Assembly passed Personal Data Protection Law Executive Order 285/2021, which regulates the principles, rights, obligations, and procedures regarding personal-data protection.[cxxxviii] This law was created with the purpose of protecting Panamanians' data. An additional provision to this law even provides compensation to Panamanians for improper use of their data. In 2020, Panama's National Authority for Government Innovation (AIG) announced the new "2022–2023 National Digital Agenda" as a strategic instrument to promote economic reactivation, involving entities in improvement processes, and increasing innovation and collaboration between the public and private sectors.[cxxxix] Building on these foundations, Resolution 17/2021 was enacted, outlining the National Strategy for Cybersecurity for the period 2021–2024.[cxl] This strategy emphasizes several critical areas, including preventing and prohibiting criminal behavior in cyberspace, fostering innovation and training in cybersecurity, and protecting personal-information privacy.

The current cybersecurity infrastructure largely depends on the success of Panama's National Digital Agenda. Through increased collaboration, Panama called for each sector to create its own digital agenda aligned with the new 2022–2023 National Digital Agenda and aimed to achieve other objectives, such as defining standards and conditions for the use of ICTs, especially the cloud and 5G.[cxli] However, the country is facing several challenges in successfully implementing the 2022 agenda. Some of these challenges include difficulty "securing critical infrastructure and services, boosting private investment in the digital ecosystem, and strengthening national and sectoral interoperability platforms."[cxlii]

Over the past decade, Panama has enacted pivotal cybersecurity laws and strategies that prioritize reliable digital-ecosystem growth through incident response teams, data/privacy safeguards, and cybercrime deterrence. However, Panama's National Digital Agenda, intended to spur innovation and economic activity, has been confronted by concerning implementation obstacles around delivering robust critical-infrastructure security and integrated technologies. With ambitious transformation timelines challenged by lingering capability gaps, sustained governance commitment alongside public–private partnerships remains essential for Panama to realize its cyber-resilience vision.

International Collaborations and Private-Sector Involvement

Legal frameworks have also been strengthened to combat cybercrime. Law 79 of 2013 led to Panama's adoption of the Budapest Convention. The Panamanian Criminal Code, particularly Articles 289–292, specifically criminalizes various forms of cyber misconduct, such as unauthorized access, interference, and data misuse, by imposing sanctions for these offenses.[cxliii] Additionally, Panama has been actively pursuing cybersecurity partnerships worldwide, signing cooperation treaties with countries including Israel, Spain, and Costa Rica. Looking ahead, Panama aims to further increase training, capacity building, and coordination through international collaboration. Recent efforts include joining the OAS and global FIRST incident response teams as well as signing a working arrangement with Eurojust ''to enable structured and closer cooperation in the fight against organized crime."[cxliv] Last, as mentioned in Costa Rica's literature review, Panama has formalized cyber agreements with the Dominican Republic and Costa Rica.[cxlv]

Cybersecurity Challenges in Panama

In Panama due to the pandemic, the need for cybersecurity services and software in public and private sectors has grown significantly over the last two years, which saw a 421% increase in cybercrime and attacks.[cxlvi] Most of the cases occurred in 2021 with 794 complaints, 68% of which were frauds, while extortion cases totaled 423 by the end of 2020. According to cybersecurity experts, U.S. companies have dominated the cybersecurity sector with approximately 60% of the total market.[cxlvii]

The Basel AML Index is an annual ranking and risk-analysis tool focused on assessing money-laundering and terrorist-financing vulnerabilities at a national level. It draws from 18 reputable sources, including the Financial Action Task Force (FATF), Transparency International, and the World Bank. In 2023, "Panama scored high in this index, making it the most susceptible to cyber threats."[cxlviii] Specifically, Panama registered a high-risk score on the 2023 Basel Anti-Money Laundering Index (AML), per Fortra's Global Cybercrime Report analysis.[cxlix] Although Panama has enacted laws targeting financial crimes, deficient enforcement is highlighted as a factor perpetuating systematic weaknesses that enable money laundering and terrorist financing threats.[cl] According to the same report, Panama was the country with the lowest digital-development score, which is based on its ICT development and network readiness.[cli] While Panama is diligently progressing toward the resolution of its existing challenges, the nation still faces a considerable journey in its ambition to emerge as a globally competitive technology hub.

Regulatory Concerns

Panama's role as a hub for sophisticated fiber-optic communications and its status as a financial center with numerous international banks require a robust cybersecurity regime. The introduction of Law 159 of 2020, which aims to establish logistics centers for manufacturing and repackaging, further underscores the need for stringent cyber protections. The IDB emphasizes that a comprehensive strategy, balancing security needs with economic growth and respecting rights to freedom of expression and privacy, is crucial for sustainable cybersecurity. Panama's commitment to protecting critical infrastructure, adopting best-practice frameworks, and ensuring data privacy and confidentiality is increasingly imperative for its continued advancement in the digital age. [clii]

Socio-Economic Impacts of Cybersecurity Breaches

The 2023 Global Cybercrime Report indicates that Panama is the country most at risk from cybercrime, money laundering, and terrorist financing, with a Basel AML Index of 5.81/10.[cliii] This position was determined by calculating a 5.81 for the Basel AML Index. [cliv] Panama's cybersecurity consistently scored poorly, with the worst digital development level and Basel AML Index. Money laundering has affected Panamanian business operations in particular, "with $935 billion estimated to be laundered yearly. Despite having laws in place to address money laundering, authorities rarely enforce them."[clv] This lack of implementation has exacerbated cybercrime, especially money laundering conducted online. If this lack of enforcement continues, it may impact Panama through decreased foreign economic investment and societal trust.

Panama's Perspectives on Colombia's Ransomware Response

Participants noted that when ransomware first struck the region, Colombia shared threat warnings to help Panama's most at-risk entities. Panama closely observed Colombia's public communications during the incident response. This information exchange allowed fear to be minimized in the country, given Panama's close relationship with Colombia. Post incident, Colombia collaborated with regional CSIRTs, providing Panama with an opportunity to learn from their experience. For Panama, Colombia's experience highlighted the need to implement mandatory cyber-incident reporting laws domestically.

Perspectives on Cloud Adoption to Decrease Cybersecurity Risks

Although currently restricted by recent data-sovereignty laws, Panama is open to potential collaborations with providers to establish local cloud solutions. These solutions would aim to harness the efficiencies of digitization while retaining domestic control over critical systems and data storage. In 2024, Panama's AIG published Resolution 52, which establishes guidelines for the location of databases that operate under the concept of computing cloud or cloud services. This approach underscores the acknowledgment of cloud benefits while addressing perceived concerns.

Evolving Cybersecurity Frameworks Centered on NIST

Participants shared that Panama follows approaches such as the NIST CSF, the EU GDPR requirements, and ISO security controls as references while customizing policies and regulations to its unique risk environment and existing software-inventory constraints. This tailored localization of established global best practices, combined with flexibility across government agencies, enables Panama to cover rapid technological shifts within its cyber governance.

In conclusion, Panama seeks to steadily advance towards cyber maturity through global collaboration and the customized adoption of new cybersecurity standards and technologies. The nation recognizes the critical importance of robust cyber defenses and resilience in today's digital age. However, Panama understands that a one-size-fits-all approach is unlikely to be successful, and is instead pursuing a pragmatic and methodical strategy. This involves capitalizing on the experiences of other countries in the region that are further along the cyber maturity curve, while carefully assessing its own unique risk landscape, infrastructure, resources, and cyber workforce to tailor solutions to its specific requirements. By learning from others through strategic partnerships and knowledge sharing, yet making calibrated implementations customized to its environment, Panama aims to continually reduce risks and improve capabilities over time, safeguarding its critical systems and data assets. Ultimately, this balanced approach allows Panama to enhance its cyber preparedness in a manner befitting its socioeconomic aspirations, achieving a resilient and secure cyber posture for the digital era.

Interview Takeaways

Drawing from interviews conducted in Colombia, Costa Rica, Panama, and Chile, the following summarizes the main findings and trends related to cybersecurity attitudes and ransomware response readiness:

- Overall acknowledgment of increased ransomware risks and critical-data security requirements for both public- and commercial-sector organizations.
- Substantial gaps persist around cyber-incident readiness, response protocols, coordination, staffing, and technical capabilities.
- Budgetary and skills deficits constrain security investments and rapid response mobilization.
- Understanding the need for increased governance priorities and capacity building due to cyber threats.
- Embracing cyber workforce development as a fundamental component of awareness and culture.
- Enabling flexible security policies by locally customizing global frameworks.
- Consensus on the cybersecurity risk and benefits of public cloud-service adoption and a need to address perceived data-control concerns.

Ultimately, the interviews indicated common ransomware-response challenges and opportunities for collective growth through workforce development and capability increases, even while cyber perspectives varied in some areas. These insights open new possibilities for coordinated security advancement.

To better understand the cybersecurity landscape in Latin America, over 150 CISOs and other high-level professionals in the region were surveyed. The goal of the survey was to attain an overview of what cybersecurity professionals in the region think about topics such as RMFs, the use of public cloud-based cybersecurity infrastructure to mitigate risk, and more. The respondents worked in the public and private sectors and came from a variety of different countries. Respondents to the survey were from Colombia (19%), Argentina (14%), Costa Rica (13%), Chile (8%), Guatemala (6%), and Bolivia (5%) as well as Brazil, Cuba, Ecuador, El Salvador, Haiti, Honduras, Mexico, Nicaragua, Panama, Peru, the Dominican Republic, and Uruguay. Most respondents work in the private sector (67%) or the government/public sector (27%), with others representing civil society (2%) and academia (3%).

A common theme in this research is the need for investment in the cybersecurity workforce and training. Of those that responded to the survey, 84% were male. This highlights the need for, within a comprehensive workforce-training regiment, increased diversity in the cybersecurity workforce. Increasing access to technology and cybersecurity for women and minorities should be a priority for every country.

The survey analysis is divided into two key categories: 1) Risk Management Frameworks (RMFs) and 2) the use of public cloud-based cybersecurity infrastructure. The RMF section examines the adoption of various risk management framework models like NIST and ISO across different industries and organization sizes. It explores the perceived effectiveness, challenges, and benefits of employing RMFs for risk assessment and mitigation. The cloud security section focuses on the trend of leveraging public cloud-based cybersecurity solutions such as SIEM, vulnerability management, and IAM. It investigates the extent of cloud security adoption, drivers like scalability and cutting-edge tech access, as well as concerns around cloud security, data privacy, and compliance. This overview provides a roadmap for understanding the state of RMF implementation and use of public cloud-based cybersecurity infrastructures based on the survey findings.

Risk-Management Framework (RMF)

Question 9: On a 5-point scale of strongly agree to strongly disagree, how would you rate your belief that implementing an RMF can enhance your organization/government agency's efforts against cyber threats such as ransomware?

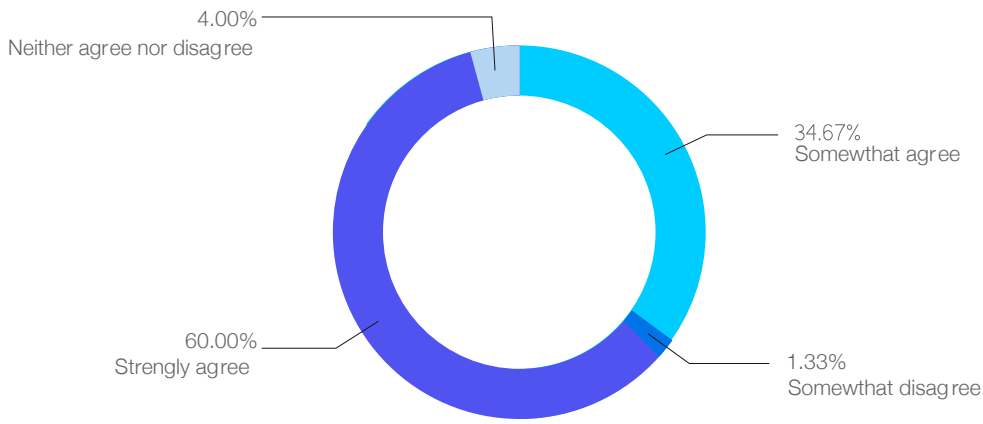


Figure 1: RMF Capabilities

Question 7: Please describe what you see as being of most value in a cybersecurity framework.

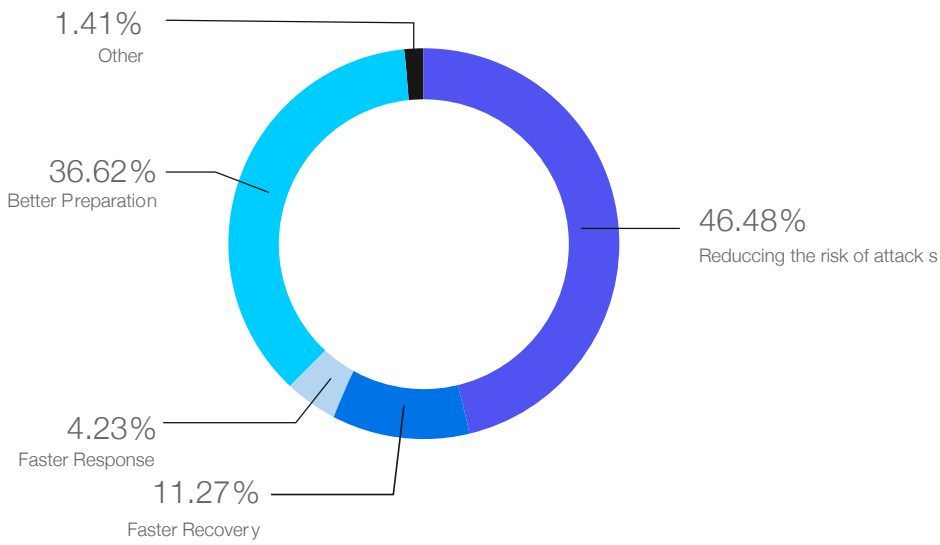


Figure 2: Value of Cybersecurity Framework

Question 8: Do you currently employ any of the following frameworks?

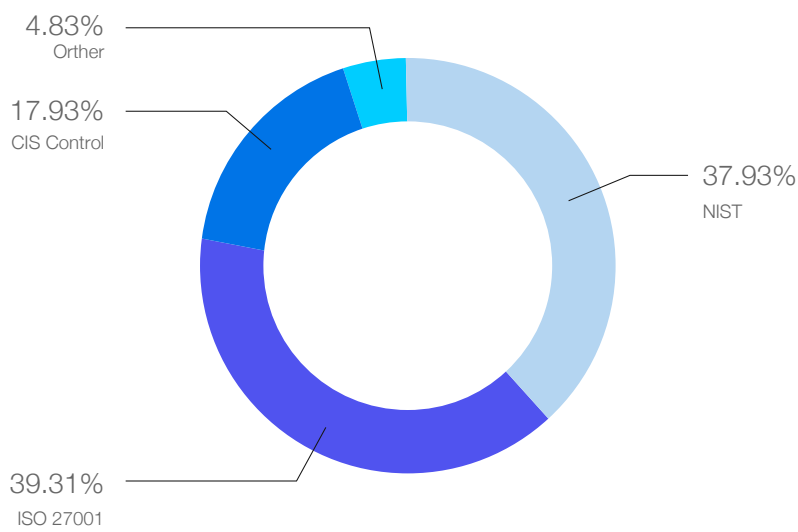


Figure 3: Frameworks Used

Question 10: Have you implemented an RMF in your organization/company/government agency's cybersecurity strategy?

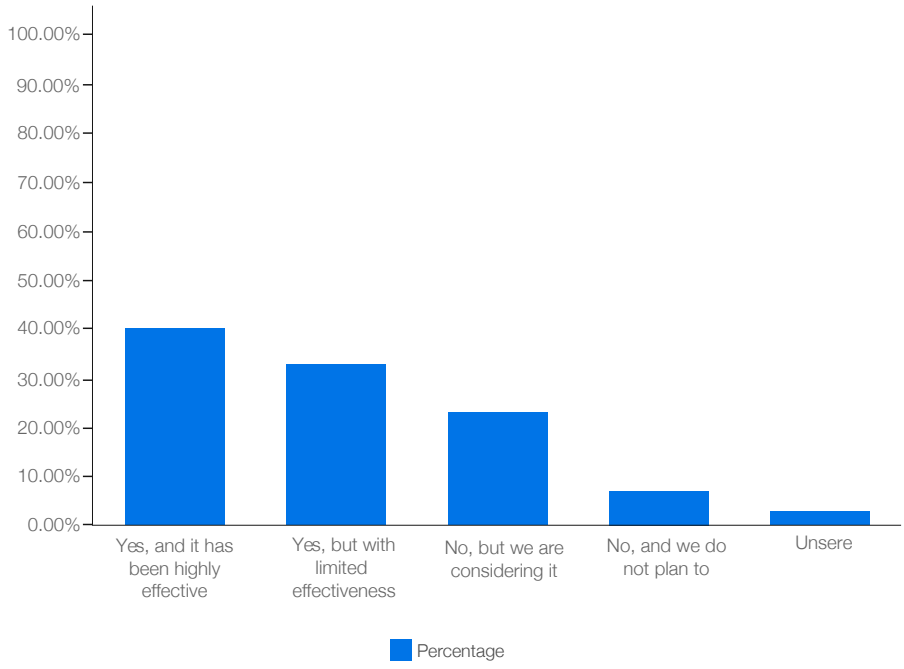


Figure 4: RMF Implementation and Efficacy

Question 11a: What challenges, if any, have you encountered when considering creating an RMF?

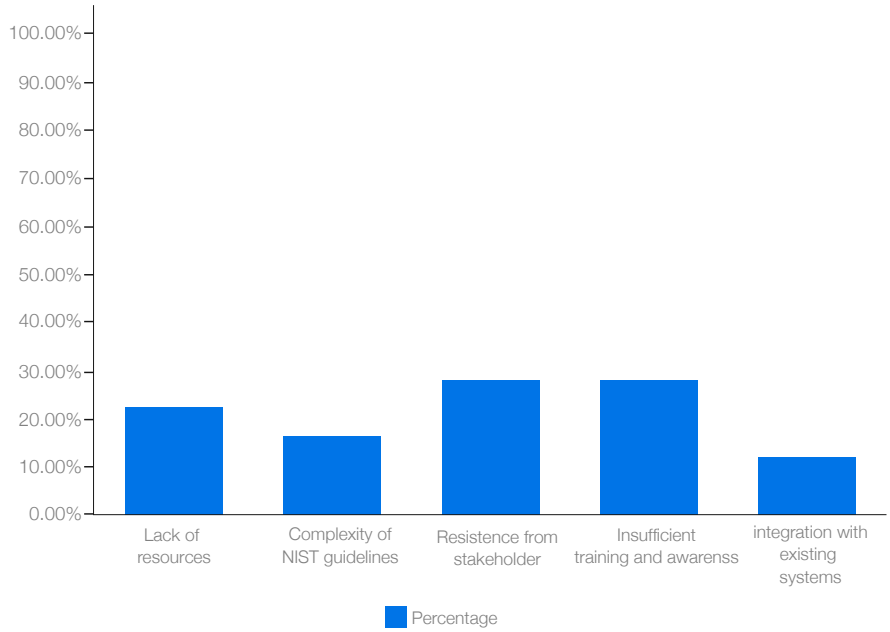


Figure 5: RMF Challenges, Creation

Question 11b: If you are not planning on creating an RMF, why not?

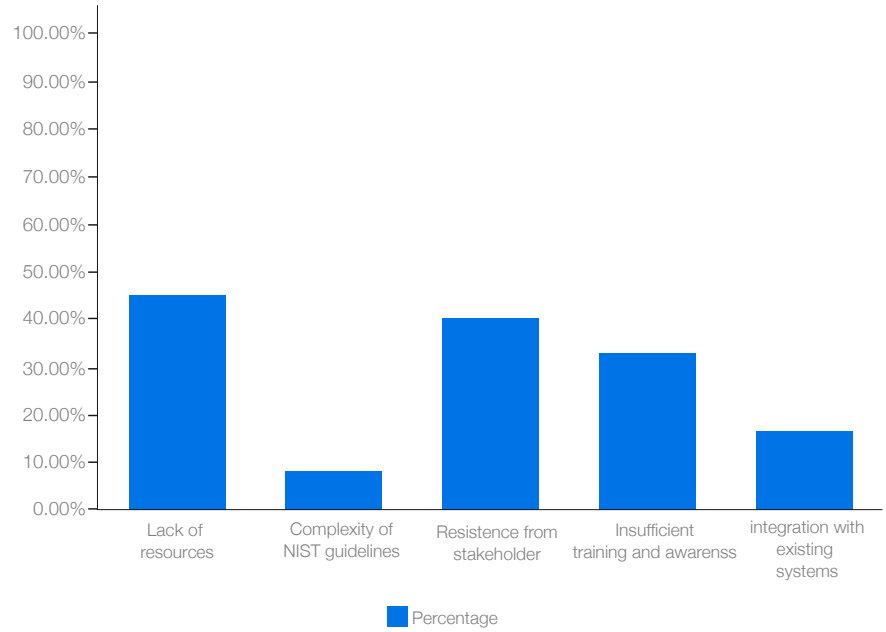


Figure 6: RMF Challenges, Barrier to Entry

Overall, 94% of respondents at least somewhat agreed that implementing an RMF can enhance their organization's resilience against cyber threats such as ransomware. This highlights the consensus among professionals on the importance of an RMF and how it can decrease risk. Of the respondents who employed an RMF, the majority used ISO 27001 (39%) and NIST (38%), with another 17% using CIS Controls. The three most popular frameworks all provide similar but unique capacities to an organization, depending on size, budget, location, and more. One recommendation of this report is to employ what fits the given organization but to ensure that it enables interoperability, depending on the organization's field, country, and other factors.

The implementation of an RMF can help an organization in many ways. Most respondents (83%) believed that an RMF does more for proactive security than having a better or faster response/recovery (15%). Most respondents (46%) answered that "Reducing the risk of attacks" is the most valuable part of an RMF, with another large group (36%) stating that "Better preparation" provides the most value. "Faster Recovery" (11%) and "Faster Response" (4%) were seen as less important than proactivity. Understandably, CISOs and other professionals would rather prevent an attack than manage its repercussions. One of the benefits of the NIST CSF and other RMFs is that they prepare an organization for both. Proactivity and preparedness, both in terms of software and training, are essential. It is impossible, however, to prevent every attack from occurring. As such, the implementation of an RMF that mitigates risk and prepares one for an attack is highly recommended.

Of those who responded to the survey, 72% stated that they had implemented an RMF in their organization's cybersecurity strategy. More of them (40% of total) agreed that it has been highly effective, and some (30% of total) stated that it has been of limited effectiveness. Another 23% of respondents claimed that they had not implemented an RMF but are considering it, with only 4% of respondents stating that they had no plan to implement one. This outcome emphasizes the consensus in the region about utilizing some RMF to mitigate risk and prepare for a potential attack.

When filtering by public versus private sector, a slight difference appears. Of those who worked in the public sector, 60% had implemented an RMF, with a relatively even split between highly effective and limited effectiveness. In the private sector, however, 80% of respondents reported having implemented an RMF, with more (46% vs 34%) reporting high effectiveness over limited effectiveness. This difference in results most likely can be attributed to a difference in resources, mindset, or personnel between the public and private sectors.

Regarding the challenges faced by those who had implemented an RMF and the challenges expected by those who had not implemented an RMF, the complexity of regulations or the difficulty in implementing them was rated extremely low. The least represented response to Question 11a, “What challenges, if any, have you encountered when considering creating an RMF,” was “The complexity of NIST guidelines” at just 11%. What people have had difficulty with is completely fixable.

The two most common challenges faced were “Resistance from stakeholders” and “Insufficient training and awareness,” each at 25%, whereas “Integration with existing systems” was at 16%. The somewhat equal distribution of these issues highlights the fact that there is no singular problem facing organizations attempting to implement an RMF. Furthermore, most problems are institutional (resistance from stakeholders or lack of training, awareness, and resources), as opposed to issues with the framework itself. Increasing awareness, training programs, and budgeting are all ways to improve the outcome of an RMF.

Of the respondents who reported that they were not planning to create an RMF, their beliefs about potential issues matched relatively well with what others reported as real issues. The main difference is that, of those not intending to create an RMF, the largest issue was “Lack of Resources” (33%). In many instances, a lack of resources can be a significant barrier to entry for implementing an RMF. Notably, the complexity of the NIST framework, for example, is not the reason that people had chosen not to create an RMF.

Public Cloud

Question 12: Does your organization currently use a public cloud?

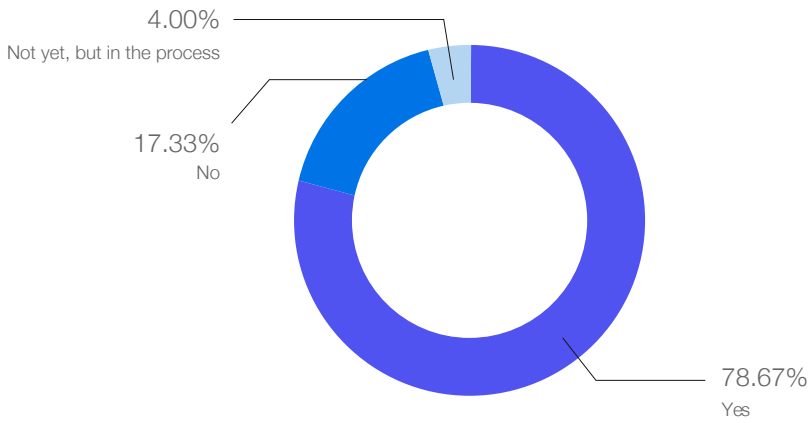


Figure 7: Public Cloud Adoption

Question 13: Was security a primary motivator for migrating to the cloud?

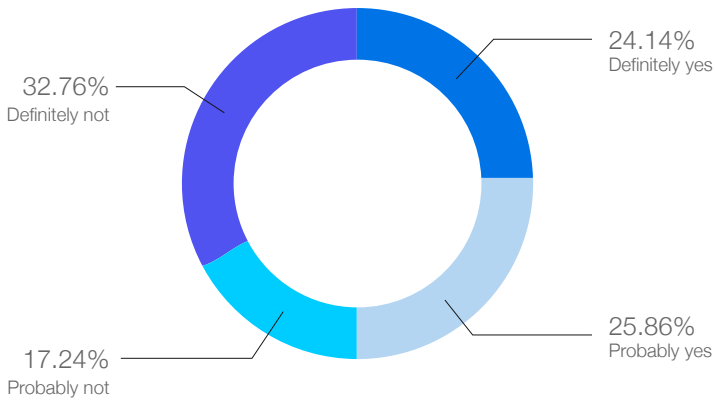


Figure 8: Security as a Motivator

Question 14: Do you feel that your systems are more secure in the cloud?

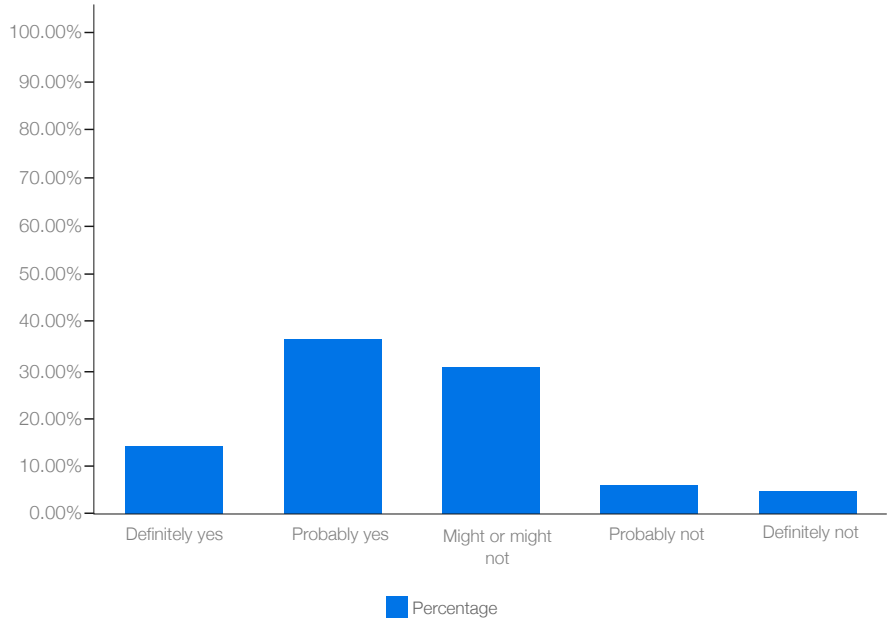


Figure 9: Security in the Cloud

Question 15: Do you believe that cloud computing is more effective in mitigating ransomware attacks?

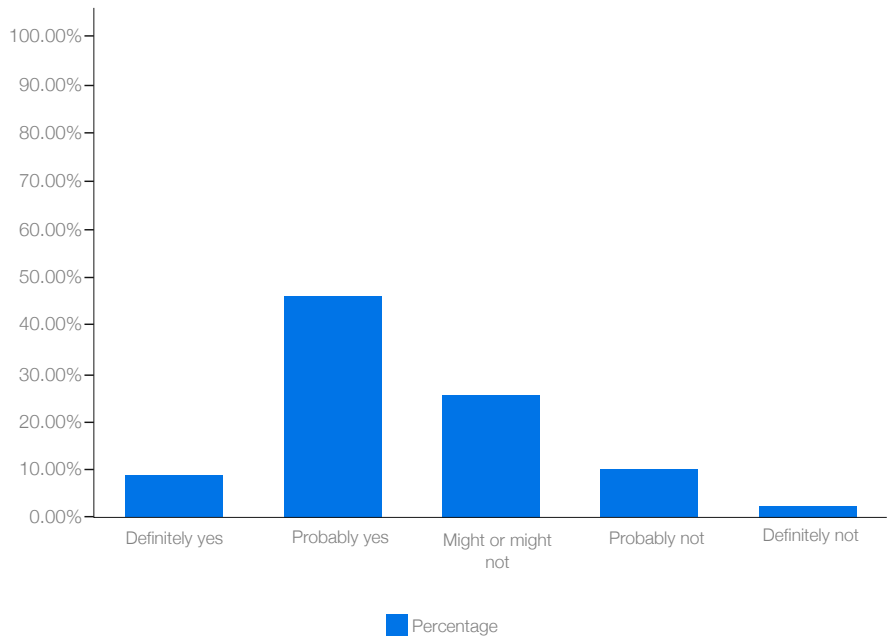


Figure 10: Cloud Computing to Mitigate Ransomware

Question 18: If you were to migrate to the cloud, would you feel that it is more secure?

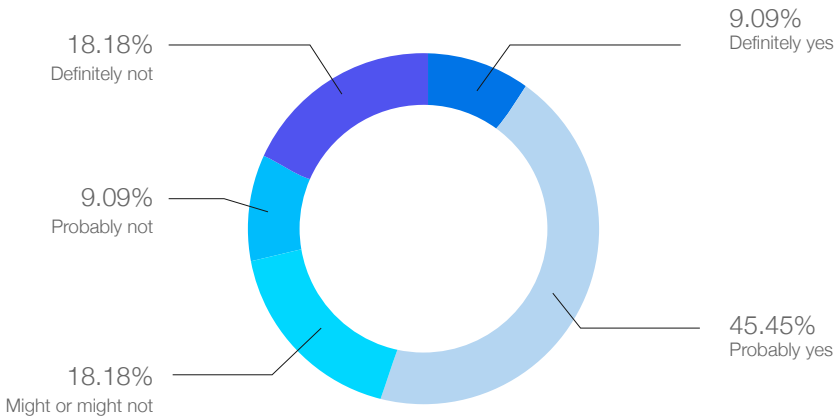


Figure 11: Cloud Security, Potential

Question 19: Is ransomware a concern when deciding whether to migrate to the cloud?

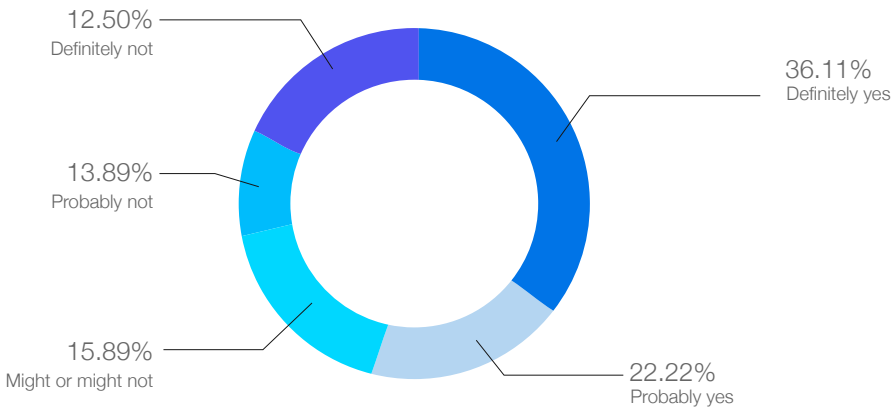


Figure 12: Ransomware as a Barrier to the Cloud

Over 82% of those surveyed stated that their organization currently used cloud-based cybersecurity-infrastructure services (public cloud; 78%) or were in the process of implementing them (4%). Again, there is a difference between the public and private sectors with respect to public cloud services. The public sector, perhaps with fewer resources or more government requirements to meet, reported less implementation. Specifically, only 62% reported currently using public cloud services, while another 5% were in the process of implementing them. In the private sector, however, over 88% of respondents had implemented a public cloud, with another 2% in the process.

Responses indicate a belief that the use of commercially available cloud services could provide more security against attacks. For example, 50% of respondents stated that security was a primary motivator for migrating to the cloud. There are many factors to consider when migrating to the cloud, but improved security seems to have been a priority for those surveyed. Supporting this, most respondents felt that their systems were more secure in the cloud, with 36% responding “probably yes” and another 12% saying “definitely yes” to the question: “If you were to migrate to the cloud, would you feel that it is more secure?” However, a large percentage (36%) were unsure.

Similarly, more than half (57%) of respondents believed that cloud computing is “probably” (48%) or “definitely” (9%) more effective in mitigating ransomware attacks, while 29% stated that it might or might not be. As such, most of those questioned had some confidence in the capabilities of migrating to the cloud to mitigate ransomware and other cyberattacks more effectively.

To finalize the thoughts of those surveyed, it seems there is a consensus on migrating to the cloud. There is still some uncertainty regarding the exact amount of increased security it provides, but the respondents to this survey, comprising CISOs and others with knowledge of their organizations’ systems, are optimistic.

Respondents agreed on the importance of implementing an RMF and on the potential of migration to commercially available public cloud services. To emphasize a common theme between questions regarding RMFs and the cloud, complexity and difficulty of implementation are not the greatest challenges faced. Rather, institutional issues, such as personnel shortages, training issues, or resistance from stakeholders, are what prevent organizations from protecting themselves from, and preparing for, cyberattacks, such as ransomware.

Policy Recommendations

Recommendation #1: Investment in Human-Capacity Building

It was evident from the interviews and survey responses that CISOs across Latin America share a deep concern about insufficient training and cyber-threat awareness. This study recommends that governments allocate funding in their fiscal year to equip government employees with cybersecurity tools and knowledge in cybersecurity risk mitigation. This integrated approach would address the current skills gap and lack of capability in cybersecurity practices by ensuring continuous skill and knowledge updating in cybersecurity risk mitigation. This recommendation would also leverage cost-effective methods of risk mitigation through heightened staff awareness.

Recommendation # 2: Establishment of a Voluntary RMF

Several LATAM countries have taken steps to develop cybersecurity frameworks as part of their digital agendas. However, many government agencies are not obligated to report incidents or follow best practices. The recommendation of a voluntary RMF would combine the establishment of a mixed-governance cybersecurity agency, a national CSIRT, in countries that have yet to implement one, and the creation of sector-specific incident databases. The creation of the agency and response team would combine with legislative and regulatory actions, such as enacting comprehensive cybersecurity laws, implementing mandatory reporting requirements for cybersecurity incidents to a centralized location, and providing incentives for private-sector participation in cybersecurity initiatives. This dual approach would provide focused protection for critical infrastructure and mandate necessary cybersecurity practices, such as incident reporting and budget allocation for cybersecurity training.

Latin American countries can use established structures from different countries as a starting point or directly base their frameworks on these structures. While Latin American countries have differences in workforces, existing cyber strategies, geopolitical allies/enemies, and more, constructing similar RMFs would benefit the region in many ways. One approach is to develop an RMF directly based on NIST, like Israel's Cyber Defense Methodology or Italy's National Framework for Cyber Security. Another approach is to follow the example of some Latin American countries, such as Uruguay and Colombia, by analyzing NIST and using its central ideas in customized cybersecurity strategies. The CSF's five main pillars are "Identify, Protect, Detect, Respond, and Recover." No matter the size of an organization or which RMF is chosen, following these main principles and establishing an RMF will increase cybersecurity robustness.

Recommendation # 3: Strategic Investment in Cybersecurity Infrastructure and Technologies

Third, strategic investment in cybersecurity infrastructure and technologies encompasses investment in cybersecurity technology and the adoption of public cloud solutions while considering the stakes of who has control. This recommendation recognizes the need to adapt to evolving cyber threats and the increasing digitization of sectors. Hence, this study advocates for investment in technologies that balance security needs with operational efficiency, including the adoption of public cloud services to decrease cybersecurity risk while promoting a safe transfer of data. Moreover, governments could adopt cloud-first policies as a means to leverage the enhanced security benefits that public cloud offerings provide. A significant portion of the respondents reported seeing decreases in risks associated with public cloud adoption. Therefore, organizations and government entities should carefully evaluate these benefits and consider leveraging cloud solutions as part of their cybersecurity strategy.

Recommendation #4: Centralized Cybersecurity Management and Reporting Systems

Centralized reporting and training systems enhance collaboration across different sectors and agencies, streamlining communication and responding to cybersecurity incidents. Through this centralized reporting and training, different sectors and agencies can more effectively observe trends and respond with greater accurately. This recommendation also includes centralizing response mechanisms, enhancing effectiveness in managing cyberattacks, and facilitating dynamic information exchange and cooperation at both national and regional levels. One approach is for governments to mandate reporting of cyberattacks within a reasonable timeframe. This approach would help destigmatize being the victim of attacks and encourage companies to disclose attacks rather than keeping them confidential. Moreover, this approach would improve situational awareness and cybersecurity posture through collective knowledge and shared resources.

[i] e-Governance Academy Foundation. “NCSI :: Ranking.” Ncsi.ega.ee, ncsi.ega.ee/ncsi-index/.
[ii] Editor, CSRC Content. “Critical Infrastructure - Glossary: CSRC.” CSRC Content Editor, csrc.nist.gov/glossary/term/critical_infrastructure.
[iii] Inter-American Development Bank, and Organization of American States. “Report: Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean.” 27 July 2020, https://doi.org/10.18235/0002513.
[iv] Inter-American Development Bank, and Organization of American States, 2020.
[v] Vicens, A. J. “Latin America Governments Are Prime Targets for Ransomware due to Lack of Resources, Analysis Argues.” CyberScoop, 16 June 2022, cyberscoop.com/latin-america-ransomware-recorded-future/.
[vi] Greig, Jonathan. “Several Colombian Government Ministries Hampered by Ransomware Attack.” Therecord.media, 15 Sept. 2023, therecord.media/colombia-government-ministries-cyberattack..
[vii] Sweigart, Emilie, and Jack Quinn. “Why Is Latin America so Vulnerable to Cyberattacks? We Ran the Numbers.” Americas Quarterly, 25 July 2023, americasquarterly.org/article/why-is-latin-america-so-vulnerable-to-cyberattacks-we-ran-the-numbers/.
[viii] “Estrategia de seguridad: de la infraestructura crítica nacional 2022-2032.” Brigadier General Edgar Alexander Salamanca Rodríguez, General (R) Fabricio Cabrera Ortiz, Stefan Reit - Bogotá: Editorial ESDEG, Fundación Konrad Adenauer KAS, 2022.
[ix] “Lineamientos Generales Para Fortalecer la Governanza de la Seguridad Digital, la Identificación de Infraestructuras Críticas Cibernéticas y Servicios Esenciales, la Gestión de Riesgos y la Respuesta a Incidentes de Seguridad Digital.” Decreto Number 338.
[x] “Ley 1273 de 2009 -Legislacion Colombiana Lexbase.” Www.lexbase.co, www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text=%22%20LEY%201273%20DE%202009%20(enero.
[xi] “Ley 1273 de 2009 -Legislacion Colombiana Lexbase.
[xii] “Ley 1273 de 2009 -Legislacion Colombiana Lexbase.
[xiii] Díaz Acevedo, Martín. (2023). La evolución de la estrategia de ciberseguridad de Colombia 2011-2021. 10.13140/RG.2.2.22241.58723.
[xiv] Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación. “Documento CONPES 3701 Número 1.” 14 Jul. 2011.
[xv] Díaz Acevedo, Martín. (2023).

[xvi] “Autorizacion A La Nacion Para Contratar Operaciones De Credito Externo Hasta Por La Suma De Us$ 500 Millones O Su Equivalente En Otras Monedas.” Republica De Colombia, Departamento Nacional de Planeacion.
[xvii] Secretaria Juridica Distrital. “Decreto 620 de 2019 Alcaldía Mayor de Bogotá, D.C.” Www.alcaldiabogota.gov.co, 18 Oct. 2019, www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=87246.
[xviii] Ministerio De Tecnologias de la Información y Las Comunicaciones. “DECRETO N° 620 de 2020.” Dapre.presidencia.gov.co, 2 May 2020, dapre.presidencia.gov.co/normativa/normativa/DECRETO%20620%20DEL%202%20DE%20MAYO%20DE%202020.pdf.
[xix] Ministerio de Ambiente y Desarrollo Sostenido. “Política de Protección de Datos Personales.” Ministerio de Ambiente Y Desarrollo Sostenible, 13 Oct. 2022, www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos.
[xx] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA. “CONPES 3995- POLÍTICA NACIONAL de CONFIANZA Y SEGURIDAD DIGITAL .” Colaboracion.dnp.gov.co, 1 July 2020, colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf.
[xxi] “ABC SEGURIDAD DIGITAL Decreto de Decreto 338 de 2022.” MinTic. 2022.
[xxii] “Decreto 767 del 16 de mayo de 2022: la Nueva Política de Gobierno Digital.” MinTiC.
[xxiii] Sandoval, Cath. “Everything You Should Know about Technology Enablers in Insurance.” LISA Insurtech, 9 Feb. 2021, lisainsurtech.com/know-everything-about-the-impact-of-technology-enablers/#:~:text=A%20technology%20enabler%20is%20a. Accessed 2 Apr. 2024.
[xxiv] “Ciberseguridad a La Medida, La Apuesta de Claro.” Www.claro.com.co, 2 Nov. 2023, www2.claro.com.co/empresas/sectores/noticias-interes/ciberseguridad-a-la-medida/.
[xxv] Puentes León, Sthefanie. Colombia: ¿Es Un Estado Efectivo En Términos De Seguridad Digital Con Énfasis En El Sector Privado? June 2019.
[xxvi] Puentes León, Sthefanie. (2019).
[xxvii] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro & Páez, Rafael V. & Contreras Fernández, Aristides & León, Ivonne. (2019). La Seguridad en el Ciberespacio, Un desafío para Colombia. Capítulo V. Gestión de Riesgo en Seguridad Digital en el Sector Privado y Mixto - Contexto General.. 10.25062/9789585216549.
[xxviii] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro & Páez, Rafael V. & Contreras Fernández, Aristides & León, Ivonne. (2019).
[xxix] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro & Páez, Rafael V. & Contreras Fernández, Aristides & León, Ivonne. (2019). La Seguridad en el Ciberespacio, Un desafío para Colombia. Capítulo V. Gestión de Riesgo en Seguridad Digital en el Sector Privado y Mixto - Contexto General. 10.25062/9789585216549.
[xxx] “LEY 1928 de 2018.” Suin-Juriscol.gov.co, 2018, www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501.
[xxxi] Council of Europe. “Budapest Convention and Related Standards.” Cybercrime, 2014, www.coe.int/en/web/cybercrime/the-budapest-convention.
[xxxii] Council of Europe. Convention on Cybercrime. 23 Nov. 2001.
[xxxiii] Council of Europe. Convention on Cybercrime. 23 Nov. 2001.
[xxxiv] “ABC Del Acuerdo Comercial Con Israel | TLC.” Tlc.gov.co, 2021, www.tlc.gov.co/preguntas-frecuentes/abc-del-acuerdo-comercial-con-israel.
[xxxv] Inter-American Development Bank. “IDB | Israel Commits to IDB Cybersecurity Initiative in Latin America and the Caribbean.” Www.iadb.org, 24 Feb. 2022, www.iadb.org/en/news/israel-commits-idb-cybersecurity-initiative-latin-america-and-caribbean#:~:text=Through%20a%20%242%20million%20contribution.
[xxxvi] Ministerio de Relaciones Exteriores. “Colombia Fue Elegido Como Primer Presidente Del Grupo de Trabajo Sobre Medidas de Fomento de Cooperación Y Confianza En El Ciberespacio de La OEA | Cancillería.” Www.cancilleria.gov.co, 2 Mar. 2018, www.cancilleria.gov.co/newsroom/news/colombia-fue-elegido-primer-presidente-grupo-trabajo-medidas-fomento-cooperacion.
[xxxvii] “International Telecommunications Union | Misión Permanente de Colombia.” Ginebra-Onu.mision.gov.co, ginebra-onu.mision.gov.co/en/international-telecommunications-union#:~:text=ITU%20was%20founded%20in%20Paris%20in%201865.
[xxxviii] International Trade Administration. “Colombia Cybersecurity Outlook.” Www.trade.gov, 25 Feb. 2021, www.trade.gov/market-intelligence/colombia-cybersecurity-outlook.
[xl] Kiuwan. “Data Breaches & LATAM Countries | Kiuwan.” Www.kiuwan.com, 14 Mar. 2023, www.kiuwan.com/blog/latam-data-breaches-top-3-countries-affected/.
[xli] Kiuwan. “LATAM Data Breaches: Top 3 Countries Affected.”
[xlii] Kiuwan. “LATAM Data Breaches: Top 3 Countries Affected.”
[xliii] Greig, Jonathan. “Several Colombian Government Ministries Hampered by Ransomware Attack.”
[xliv] Greig, Jonathan. “Several Colombian Government Ministries Hampered by Ransomware Attack.”
[xlv] Reuters. “More than 50 Colombian State, Private Entities Hit by Cyberattack -Petro.” Reuters, 18 Sept. 2023, www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-

cyberattack-petro-2023-09-18/.
[xlvi] Reuters. “More than 50 Colombian State, Private Entities Hit by Cyberattack -Petro.”
[xlvii] Thomas, Roland. “Colombia Fights Back from Devastating Ransomware Attack | Thomas Murray.” Thomasmurray.com, thomasmurray.com/insights/colombia-fights-back-devastating-ransomware-attack..
[xlviii] Thomas, Roland. “Colombia Fights Back from Devastating Ransomware Attack”
[xlix] Thomas, Roland. “Colombia Fights Back from Devastating Ransomware Attack”
[l] Díaz, Laura Lesmes. “Los Pilares y Claves Del Proyecto Para La Creación de La Agencia de Seguridad Digital.” El Tiempo, El Tiempo, 26 July 2023, www.eltiempo.com/tecnosfera/novedades-tecnologia/los-pilares-y-claves-del-proyecto-para-la-creacion-de-la-agencia-de-seguridad-digital-790038.
[li] Trade European Commission. Cybersecurity Sector in Central America. Nov. 2022.
[lii] Sistema Costarricense de Información Jurídica. “Reforma de La Sección VIII, Delitos Informáticos Y Conexos, Del Título VII Del Código Penal N° 9048.” Www.pgrweb.go.cr, 7 Oct. 2012, www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583.
[liii] “National Cybersecurity Strategy – Costa Rica.” Ministry of Science, Technology and Telecommunications. 2017.
[liv] “LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES”, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf
[lv] S-COM: Davinsson Nunjar Flores. “Sistema Costarricense De Información Jurídica.” S-COM, www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC.
[lvi] OECD. Public Governance In Costa Rica. PUBE. 2021.
[lvii] OECD. (2021).
[lviii] Ministry of Science, Technology and Telecommunications. (2017)
[lix] Ministry of Science, Innovation, Technology and Telecommunications. Costa Rican National Cybersecurity Strategy 2023 - 2027. 10 Nov. 2023.
[lx] Ministry of Science, Innovation, Technology and Telecommunications. (2023).
[lxi] Ministry of Science, Innovation, Technology and Telecommunications. (2023).
[lxii] Cybersec: The Cluster That Brought Together The Region’s Top Cybersecurity Companies And Organizations.” CINDE Costa Rica’s Investment Promotion Agency, www.cinde.org/en/essential-news/cybersec-the-cluster-that-brought-together-the-regions-top-cybersecurity-companies-and-organizations.
[lxiii] Cybersec: The Cluster That Brought Together The Region’s Top Cybersecurity Companies And Organizations.” (2022)
[lxiv] Society, European Foundation for Information. “Ministerio de Economia, Industria y Comercio de Costa Rica.” Ministerio de Economia, Industria y Comercio de Costa Rica -, 28 Feb. 2022, www.meic.go.cr/comunicado/1120/programa-nacional-de-clusteres-recibe-declaratoria-de-interes-publico.php.
[lxv] CINDE | Invest in Costa Rica.” Cinde.org, 2020, www.cinde.org/en/our-services..
[lxvi] “CINDE | Invest in Costa Rica.” (2020)
[lxvii] Society, European Foundation for Information. (2022)
[lxviii] “OAS and Trend Micro Sign Agreement to Enhance Cyber Security in the Americas.” Organization of American States, 13 Oct. 2015, www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/15.
[lxix] Inter-American Cooperation Portal on Cyber-Crime (Ailing Initiative).” Organization of American States, https://scm.oas.org/pdfs/2019/CICTE1301B.pdf.
[lxx] UN OEWG 2021-2025 2nd Substantive Session.” Geneva Digital Watch, dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-international-law.
[lxxi] Geneva Digital Watch. “[Event] UN OEWG 2021-2025 2nd Substantive Session.”
[lxxii] “Costa Rica.” Japan International Cooperation Agency, www.jica.go.jp/english/overseas/costarica/index.html.
[lxxiii] https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008
[lxxiv] “Costa Rica will host the third regional conference of Budapest Convention on Cybercrime.” Ministry of Foreign Affairs and Worship, Government of Costa Rica, www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008.
[lxxv] Tornaghi, Cecilia. “El Dramático Ciberataque Que Puso a América Latina En Alerta.” Americas Quarterly, 25 July 2023, americasquarterly.org/article/el-dramatico-ciberataque-que-puso-a-america-latina-en-alerta/..
[lxxvi] “Costa Rica agradece a España y Estados Unidos el apoyo en ciberseguridad.” Forbes Centroamérica. December 2023.
[lxxvii] “United States Announces $25 Million to Strengthen Costa Rica’s Cybersecurity.” U.S. Embassy in Costa Rica, cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/#:~:text=Today%2C%20the%20United%20States%20and,bolster%20Costa%20Rica-’s%20digital%20infrastructure.
[lxxviii] “CCrif and Central America’s Regional Disaster Risk Management Agency Cepredenac Sign

Memorandum." United Nations Office for Disaster Risk Reduction, UNO.ORG, www.preventionweb.net/news/ccrif-and-central-americas-regional-disaster-risk-management-agency-cepredenac-sign-memorandum.
[lxxix] Sherman, Christopher. "Costa Rica Declares Emergency in Ongoing Cyberattack." AP NEWS, Associated Press, 10 May 2022, apnews.com/article/russia-ukraine-technology-business-gangs-costa-rica-9b2fe3c5a1fba7aa7010eade96a086ea..
[lxxx] Sherman, Christopher. "Costa Rica Declares Emergency in Ongoing Cyberattack." (2022).
[lxxxi] Sherman, Christopher. "Costa Rica Declares Emergency in Ongoing Cyberattack." (2022).
[lxxxii] "Costa Rica Ransomware Attack (2022)." CCDCOE, https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#cite_note-8.
[lxxxiii] Costa Rica Ransomware Attack (2022).
[lxxxiv] Costa Rica Ransomware Attack (2022).
[lxxxv] Datta, P. M., & Acton, T. (2022). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. Journal of Information Technology Teaching Cases, 0(0). https://doi.org/10.1177/20438869221149042
[lxxxvi] Burgess, Matt. "Conti's Attack against Costa Rica Sparks a New Ransomware Era." WIRED UK, 12 June 2022, www.wired.co.uk/article/costa-rica-ransomware-conti.
[lxxxvii] Pratim Milton Datta & Thomas Acton, 'Ransomware and Costa Rica's National Emergency: A Defense Framework and Teaching Case' (2023) Journal of Information Technology Teaching Cases 1.
[lxxxviii] "US commits $25 million to Costa Rica for Conti ransomware recovery." The Record. March 2023.
[lxxxix] Pratim Milton Datta & Thomas Acton. (2023).
[xc] (Trade European Commission)
[xci] Biblioteca del Congreso Nacional de Chile. "DECRETO 533 CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD." www.bcn.cl/Leychile, 17 July 2015, www.bcn.cl/leychile/navegar?idNorma=1079608&idVersion=2023-08-14..
[xcii] Biblioteca del Congreso Nacional de Chile. "DECRETO 533 CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD."
[xciii] Barrios Achavar, Verónica. "Política Nacional de Ciberseguridad: 2017-2022." Biblioteca Del Congreso Nacional de Chile, July 2018, pp. 1–7, obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf.
[xciv] Barrios Achavar, Verónica. "Política Nacional de Ciberseguridad: 2017-2022."
[xcv] Biblioteca del Congreso Nacional de Chile. "Historia de La Ley No 21.113." www.bcn.cl, www.bcn.cl/historiadelaley/nc/historia-de-la-ley/vista-expandida/7585/#h2_4_1.
[xcvi] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006. 20 Aug. 2019, www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf.
[xcvii] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 1661. 30 May 2023, https://www.csirt.gob.cl/media/2023/12/Rex-2023-RESOLUCI%C3%93N-EXENTA-1661-deja-sin-efecto-Rex-11.536-DE-2020-y-modifica-Rex-N5.006-DE-2019-ambas-de-la-SSI.pdf.
[xcviii] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[xcix] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[c] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[ci] Cyber Security Incident Response Team (CSIRT). "Quiénes Somos." Www.csirt.gob.cl, 2 Oct. 2019, www.csirt.gob.cl/quienes-somos/.
[cii] International Trade Administration. "Chile - Information Technologies."
[ciii] "Diario Oficial publica nueva Política Nacional de Ciberseguridad 2023-2028." CSIRT, 6 Dec. 2023, https://csirt.gob.cl/noticias/diario-oficial-publica-nueva-politica-nacional-de-ciberseguridad-2023-2028/.
[civ] Equipo Actualidad Jurídica. "Nueva Política Nacional de Ciberseguridad 2023-2028 Para Proteger La Seguridad Digital Del País." DOE | Actualidad Jurídica, 4 Dec. 2023, actualidadjuridica.doe.cl/nueva-politica-nacional-de-ciberseguridad-2023-2028-para-proteger-la-seguridad-digital-del-pais/.
[cv] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN. 12 Dec. 2023, www.csirt.gob.cl/media/2023/12/Boletin14847-TextoFinal.pdf.
[cvi] "Avanza La Ciberseguridad En Chile: Nueva Ley Marco de Ciberseguridad E Infraestructura Crítica de La Información Es Despachada a Ley." Centro de Innovación, 21 Dec. 2023, centrodeinnovacion.uc.cl/noticias/avanza-la-ciberseguridad-en-chile-nueva-ley-marco-de-ciberseguridad-e-infraestructura-critica-de-la-informacion-es-despachada-a-ley/.
[cvii] Fuenzalida, Cesar. (2023).
[cviii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT, 13 Dec. 2023, www.csirt.gob.cl/noticias/congreso-aprueba-ley-marco/.
[cix] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.
[cx] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.

[cxi] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxiii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxiv] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxv] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxvi] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional." CSIRT.
[cxvii] "Alianza Chilena de Ciberseguridad." Alianzaciberseguridad.cl, alianzaciberseguridad.cl/.
[cxviii] "Nosotros – INCIB Chile." Instituto Nacional de Ciberseguridad de Chile, 2021, incibchile.cl/nosotros/.
[cxix] "Nuestra Asociación." Chiletec. https://chiletec.org/sobre-chiletec/nuestra-asociacion.
[cxx] "The Budapest Convention (ETS No. 185) and Its Protocols." Council of Europe, 2014, www.coe.int/en/web/cybercrime/the-budapest-convention.
[cxxi] "9o Congreso Latinoamericano Tecnología Y Negocios America Digital 2024." Congreso America Digital, 2021, congreso.america-digital.com/.
[cxxii] Techbound Technology, "Cybersecurity Alert: IFX Networks Cyberattack Shakes Colombia, Chile, and Argentina,"15 September,, 2023, https://www.linkedin.com/pulse/cybersecurity-alert-ifx-networks-cyberattack-shakes/.
[cxxiii] "Ejercito de Chile Es Atacado Por La Nueva Banda de Ransomware Rhysida." CronUp Ciberseguridad, 29 May 2023, www.cronup.com/ejercito-de-chile-es-atacado-por-la-nueva-banda-de-ransomware-rhysida/.
[cxxiv] Gatlan, Sergiu . "Rhysida Ransomware Leaks Documents Stolen from Chilean Army." BleepingComputer, 15 June 2023, www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/.
[cxxv] "Ejercito de Chile Es Atacado Por La Nueva Banda de Ransomware Rhysida." CronUp Ciberseguridad.
[cxxvi] "Alerta de Seguridad de La Información | Ransomware En Aduanas." CSIRT, 17 Oct. 2023, www.csirt.gob.cl/noticias/10cnd23-00112-01/.
[cxxvii] "Alerta de Seguridad de La Información | Ransomware En Aduanas." (2023); "Superada Alerta Informática en sistemas de Aduanas," Chile Aduanas, 10 November 2023, https://www.aduana.cl/superada-alerta-informatica-en-sistemas-de-aduanas/aduana/2023-11-10/140942.html.
[cxxviii] "Alerta de Seguridad de La Información | Ransomware En Aduanas." (2023)
[cxxix] International Trade Administration. "Chile - Environmental Technologies." Www.trade.gov, 30 Sept. 2022, www.trade.gov/country-commercial-guides/chile-environmental-technologies.
[cxxx] Fundacion Pais Digital. "Chile Desaprovecharía Hasta US$13 Mil Millones En Crecimiento Si No Prepara a Las Personas En Habilidades Del Mercado Del Futuro Según Informe de Accenture Y Fundación País Digital – Fundación País Digital." Fundacion Pais Digital, 15 May 2020, paisdigital.org/2020/05/15/chile-desaprovecharia-hasta-us13-mil-millones-en-crecimiento-si-no-prepara-a-las-personas-en-habilidades-del-mercado-del-futuro-segun-informe-de-accenture-y-fundacion-pais-digital/.
[cxxxi] "Consulta Ciudadana: Guía Para El Uso de Servicios En La Nube Para La Administración Del Estado." Digital.gob.cl, 2024, participacion.digital.gob.cl/es-CL/projects/consulta-ciudadana-guia-para-el-uso-de-servicios-en-la-nube-para-la-administracion-del-estado/1.
[cxxxii] Newmeyer, Kevin. "Elements of National Cybersecurity Strategy for Developing Nations." National Cybersecurity Institute Journal, vol. 1, no. 3, 2015, publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=11.
[cxxxiii] "Sobre Nosotros - CSIRT Panama." CSIRT Panama - Equipo de Respuesta a Incidentes de Seguridad de La Información, 28 July 2015, cert.pa/?page_id=33.
[cxxxiv] "Sobre Nosotros - CSIRT Panama." CSIRT Panama - Equipo de Respuesta a Incidentes de Seguridad de La Información, 28 July 2015, cert.pa/?page_id=33.
[cxxxv] "Estrategia Nacional de Seguridad Cibernética Y Protección de Infraestructura Crítica." Autoridad Nacional Para La Innovación Gubernamental, aig.gob.pa/descargas/2019/06/Estrategia_Nal_de_Seguridad_Cibernetica_y_Proteccion_Infraectructura_Critica.pdf.
[cxxxvi] "Sobre Nosotros - CSIRT Panama." CSIRT Panama - Equipo de Respuesta a Incidentes de Seguridad de La Información.
[cxxxvii] "Panama: ICT Sector Fiche." Acuerdo de Asociación UE-Centroamérica.
[cxxxviii] "Panama: ICT Sector Fiche." Acuerdo de Asociación UE-Centroamérica.
[cxxxix] "AGENDA DIGITAL ESTRATÉGICA DEL ESTADO PANAMEÑO." Autoridad Nacional Para La Innovación Gubernamental, 2022, aig.gob.pa/documentosaig/agenda-digital/.

[cxl] Lorenzo, Siaska. “Panama: Developments in Cybersecurity.” DataGuidance, 3 May 2022, www.dataguidance.com/opinion/panama-developments-cybersecurity.
[cxli] “Panama: ICT Sector Fiche.” Acuerdo de Asociación UE-Centroamérica, June 2023, trade.ec.europa.eu/access-to-markets/en/country-assets/Sector%20Fiche%20Panama%20ICT%20fv%202.pdf.
[cxlii] Código Penal de La República de Panamá (Adoptado Por La Ley N° 14 de 18 de Mayo de 2007, Con Las Modificaciones Y Adiciones Introducidas Por La Ley N° 26 de 2008). 21 May 2008, www.wipo.int/wipolex/en/text/189272.
[cxliii] Código Penal de La República de Panamá (Adoptado Por La Ley N° 14 de 18 de Mayo de 2007, Con Las Modificaciones Y Adiciones Introducidas Por La Ley N° 26 de 2008). 21 May 2008, www.wipo.int/wipolex/en/text/189272.
[cxliv] “Eurojust and Panama Sign Working Arrangement to Step up Cooperation against Organised Crime.” EuroJust: European Union Agency for Criminal Justice Cooperation, 12 Jan. 2024, www.eurojust.europa.eu/news/eurojust-and-panama-sign-working-arrangement-step-cooperation-against-organised-crime.
[cxlv] “CCrif and Central America’s Regional Disaster Risk Management Agency Cepredenac Sign Memorandum.” United Nations Office for Disaster Risk Reduction, UNO.ORG, www.preventionweb.net/news/ccrif-and-central-americas-regional-disaster-risk-management-agency-cepredenac-sign-memorandum.
[cxlvi] “Panama - Cybersecurity.” Www.trade.gov, 5 Apr. 2023, www.trade.gov/country-commercial-guides/panama-cybersecurity#:~:text=Due%20to%20dramatic%20increases%20in.
[cxlvii] (International Trade Administration, “Panama - Cybersecurity”)
[cxlviii] Shank, Stefanie. “The 2023 Global Cybercrime Report: A Look at the Key Takeaways” Tripwire, 17 Jan. 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cxlix] Shank, Stefanie. “The 2023 Global Cybercrime Report: A Look at the Key Takeaways” Tripwire, 17 Jan. 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cl] Shank, Stefanie. “The 2023 Global Cybercrime Report: A Look at the Key Takeaways” Tripwire, 17 Jan. 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cli] Shank, Stefanie. “The 2023 Global Cybercrime Report: A Look at the Key Takeaways” Tripwire, 17 Jan. 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[clii] Lorenzo, Siaska. “Panama: Developments in Cybersecurity.”
[cliii] “Global Cybercrime Report.” Proxyrack, 12 Oct. 2023, www.proxyrack.com/blog/global-cybercrime-report/.
[cliv] “Global Cybercrime Report.” (2023).
[clv] Shank, Stefanie. “The 2023 Global Cybercrime Report: A Look at the Key Takeaways.”

LATAMCISO REPORT 2024

DIGI AMERICAS LATAM CISO

Duke UNIVERSITY