INFORMATION SHARING IN LATAM:

UNDERSTANDING THE ROLE OF ISACS IN THE REGION

DIGI AMERICAS

The contents expressed in this document are presented exclusively for informational purposes and do not represent the official opinion or position of the Center for Cybersecurity Policy and Law, or any of its members.

For more information, please contact admin@digiamericas.org

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andrea Escobedo
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Ryan Goss

Editors

Belisario Contreras
Alexis Steffaro
Pallavi Bhargava

DIGI AMERICAS ALLIANCE MEMBERS

aws
Apple
CHECK POINT
CISCO
CLOUDFLARE
CROWDSTRIKE
fluid attacks we hack your software
Google
kriptos
LUMU
METABASE Q
netskope
paloalto NETWORKS
Resecurity
Santander
Schneider Electric
Telefónica
tenable
Trellix
TREND MICRO

Abstract

The Latin American and Caribbean (LATAM) region's rapid digital transformation has significantly increased its vulnerability to cyber-attacks, and the current fragmented approach to cybersecurity information sharing limits incident-response capabilities. This paper explores the role of Information Sharing and Analysis Centers (ISACs) as a solution to enhancing regional resilience. It provides an overview of ISAC structures, governance models, and the benefits they offer to members, emphasizing their potential to address LATAM's unique cybersecurity challenges. By examining existing information-sharing initiatives in the region, the paper highlights key gaps, such as siloed public and private efforts. The analysis underscores the need for scalable, formalized ISACs tailored to LATAM's operational and cultural dynamics. While this paper does not prescribe a specific ISAC structure, it underscores the critical need for ISACs in a form that best suits the region's unique context. In addition to establishing formalized ISACs, it is recommended to leverage existing information-sharing efforts and integrate with global ISAC networks where appropriate. These approaches aim to foster multistakeholder engagement, reduce cybersecurity maturity gaps, and empower regional stakeholders to implement collaborative mechanisms that enhance resilience and address LATAM-specific threats.

Table of Contents

Introduction

The Latin America and Caribbean (LATAM) region has rapidly increased its reliance on digital infrastructure. Following the COVID-19 pandemic, many daily essential services, such as banking and health care, became digitized, making them increasingly more vulnerable to cyber-attacks. In Colombia alone, 72% of all financial transactions are conducted through digital channels.[1] With expanding digital dependence, innovative digital strategy and security protocols are needed; private actors throughout the region have echoed these sentiments in their calls for change. Centro Mexico Digital revealed that "47% of Latin American companies recognize the need for a digital strategy and the essential role of information technology in business continuity." By 2023, 72% of companies in the region had begun digitizing their operations, with Mexico and Brazil ranking in the top 10 globally for countries with the most internet users.[2] However, in 2021, only three countries in Latin America had devised a national digital strategy, and although that number has since grown, a significant disparity between public- and private-sector progress persists.[3]

LATAM's digital dependence and expanding cybersecurity market have made it highly vulnerable to cyber-attacks. By 2025, LATAM could experience an average of more than 18.5 million attacks per year, with annual costs for those attacks exceeding $90 million.[4] Ransomware attacks have been the most common and detrimental attacks, with Colombia, Brazil, Costa Rica, Chile, Panama, and more experiencing large-scale, extremely disruptive ransomware attacks in the last few years.[5] Ransomware is a type of malware that prevents users from accessing their device and the data stored on it, usually by encrypting the files. Criminals will then demand a ransom in exchange for decryption. Panama alone experienced a 421% increase in cyber-attacks in the last two years.[6] In 2023, the cybersecurity market in Latin America was valued at $8.34 billion. Moreover, it was estimated that from 2023 to 2028 the overall market would grow at a compound annual rate of around 6.95%, exceeding $11 billion by 2028.[7]

[1] La Republica, Las transacciones digitales ya representan 72% dentro de las operaciones de los bancos, June 21, 2021, https://www.larepublica.co/finanzas/las-transacciones-digitales-ya-representan-72-dentro-de-las-operaciones-de-los-bancos-3187260#:~:text=Es%20decir%20m%C3%A1s%20de%2072,y%20con%20dat%C3%A1fonos%20692%20millones.

[2] BN Americas, Companies Embracing Change in Latin Americas Digital Transformation, January 24, 2024, https://www.bnamericas.com/en/news/companies-embracing-change-in-latin-americas-digital-transformation.

[3] Financial Services ISAC, Emerging Trends to Cyber Risks: a Latin American Perspective, https://www.fsisac.com/insights/emerging-trends-to-cyber-risks-latin-american-perspective, (last accessed July 26, 2024).

[4] Digi Americas, Cyber Readiness in Latin American Public Sectors, 2024, https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf.

[5] Ibid.

[6] Ibid.

[7] Statista, Value of the Cybersecurity Market in Latin America in 2023 and 2028, Jan. 2, 2024, https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/.

There are significant cyber maturity gaps in overall cybersecurity resilience between LATAM countries, which leads to inconsistent incident response across the region. A 'cyber maturity gap' refers to the difference between an organizations or country's current cybersecurity capabilities and the level of maturity they need to achieve, typically measured against a recognized cybersecurity framework. Countries in LATAM are at different stages of cybersecurity policy development, resulting in substantial variations in identification tactics and incident response practices from one nation to another.

A cohesive information-sharing mechanism is needed in LATAM to generate regional resilience.

By rapidly sharing critical information about cyber-attacks and widespread vulnerabilities, the scope and magnitude of cyber events can be significantly decreased.[8] As LATAM continues to be targeted by malicious threat actors, the region needs a cohesive forum that unites all relevant stakeholders, from both public and private sectors, to share relevant threat information and best practices. Information Sharing and Analysis Centers (ISACs) are prevalent in the US and Europe and provide a central body for gathering and disseminating information on cyber threats to critical infrastructure within a particular critical-infrastructure sector.[9] Both government stakeholders and private-sector participants have identified the need for a similar initiative in LATAM but note that it will require a unique approach.

Current information-sharing efforts in LATAM are fragmented, with public and private sectors operating in silos rather than in collaboration. This dynamic limits opportunities for the comprehensive exchange of valuable information. These challenges are further compounded by regional nuances, including concerns over appearing vulnerable by sharing threat information; cultural preferences for informal exchanges; and the need to address threats unique to LATAM, such as region-specific malware like the Mekotio banking trojan.[10] This paper seeks to explore the considerations necessary for the formation of ISACs in LATAM. Rather than advocating for a single model, this paper emphasizes the need for formalized, scalable initiatives to complement and enhance existing ad hoc approaches. Whether sector specific or country based, ISACs in LATAM should align with the region's cultural and operational dynamics, leveraging existing information-sharing practices and connecting to global ISAC networks where appropriate.
This paper aims to empower stakeholders to decide on the ISAC structure that meets their needs by highlighting the benefits,

[8] Cybersecurity and Infrastructure Security Agency (CISA), Information Sharing, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing#:~:text=By%20rapidly%20sharing%20critical%20information,events%20can%20be%20greatly%20decreased. (Last accessed Sept. 27, 2024).
[9] National Council of ISACs, About ISACs, https://www.nationalisacs.org/about-isacs, (last accessed Jul. 19, 2024).
[10] Trend Micro, Mekotio Banking Trojan Threatens Financial Systems in Latin America, July 4, 2024, https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html.

challenges, and existing foundations for information sharing in LATAM. Enhanced collaboration in the region can help close maturity gaps, improve resilience, foster trust, and address threats in a way that is tailored to the unique characteristics of the region.

The remainder of this paper begins with an introduction to ISACs, including their background, purpose, key benefits and challenges, different structural models, roles and responsibilities, governance and funding options, and core capabilities. Subsequently, the need for formalized ISACs in LATAM is critically assessed, using region-specific examples to demonstrate its alignment with emerging policies and the desire for greater multistakeholder collaboration. The paper continues with an overview of the existing ad hoc information-sharing initiatives within LATAM, identifying their major successes and pain points. Finally, the conclusion offers the recommendation that, regardless of its structure, the LATAM region would benefit from enhanced formalized information-sharing mechanisms that leverage existing efforts and surpass just information sharing by also incorporating workforce education and development initiatives. With these changes, it would be possible to work towards closing the wide cybersecurity maturity gaps that exist in the region.

50%
90%
100%
80

Components of an ISAC

An ISAC, as defined in the US, is a nonprofit, membership-driven organization that provides a central resource for collecting, analyzing, and disseminating actionable threat intelligence to members while enabling a two-way sharing of information between the private and public sectors. ISACs can adopt various structures, which range from models that include only private-sector industry representatives to those that incorporate government participants and civil-society stakeholders. While many existing ISACs operate within the private sector, this paper advocates for a multistakeholder approach that builds on current practices to enhance inclusivity and collaboration. ISACs create an ecosystem of trust amongst members, allowing critical-infrastructure owners and operators to better protect themselves and their customers from cyber and physical threats. ISACs provide around-the-clock threat-warning and incident-reporting capabilities in addition to annual meetings, technical exchanges, workshops, and webinars. ISACs are a type of public-private-partnership (PPP) but are considered a more formal mechanism than traditional PPP's as members follow a clearly defined framework for sharing both information and analysis. While most ISACs in the US and EU follow a sector-based approach, the following section explores the different structural models for building an ISAC that will be pertinent for the LATAM community to consider when beginning to formalize information sharing in the region.

HISTORY AND INTERNATIONAL ADOPTION

The concept of ISACs was first introduced and promulgated pursuant to the US Presidential Decision Directive-63 (PDD-63), signed May 22, 1998, after which the federal government asked each critical-infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities.[11] Prominent US ISACs include the Financial Services ISAC (FS ISAC), Health ISAC (H-ISAC), Information Technology ISAC (IT-ISAC), and Multi-State ISAC (MS-ISAC), among many more.[12] The sector-based ISACs collaborate with each other via the National Council of ISACs, a coordinating body designed to maximize information exchange across private-sector critical infrastructures and with the government. [13] The NCI provides a forum for sharing threats and mitigation strategies among ISACs and with government and private-sector partners during incidents requiring cross-sector response. Through a regular cadence of meetings, the NCI coordinates between ISAC operations centers and holds its own exercises and activities as needed.[14] The division of ISACs by critical-infrastructure sectors allows the platform to maintain specific sector-wide situational awareness and to consider the unique realities of each sector. While most ISACs in the US

[11] National Council of ISACs, About ISACs.
[12] National Council of ISACs, Member ISACs, https://www.nationalisacs.org/members, (last accessed Jul. 19, 2024).
[13] Ibid.
[14] National Council of ISACs, About NCI, https://www.nationalisacs.org/about-nci (last accessed Oct. 9, 2024).

focus membership on US-based entities, more mature ISACs, such as the FS-ISAC, have member companies located internationally and in LATAM.[15] For example, large multinational companies are often members of US ISACs and may be members of more than one based on their scope of interest.

As ISACs have grown in number and maturity throughout the US, they have also been adopted throughout the European Union (EU) in many different forms. Across the EU, ISACs exist in both formal and informal structures and can be country focused, sector based, or international. The first ISACs in the EU focused on the finance and energy sectors. The EU approach to ISACs is unique in that governmental support is often expected, primarily for facilitating functions in addition to offering expertise and professional knowledge as an ISAC partner.[16] Additionally, European legislation supports the establishment of ISACs. Notably, the NIS 2 Directive separates the operators of essential services in sectors and tasks the operators with implementing requirements on incident reporting.[17] The creation of sectoral ISACs at a national level could support the implementation of these provisions by being the placeholder for the interaction between public- and private-sector stakeholders.[18] As the LATAM region continues to develop cybersecurity legislation, governments should consider how they can include provisions that support the creation of information-sharing mechanisms in ways similar to the EU.

However, it is important to note that this approach has created controversy because many US-based ISACs already have a significant presence in the EU, resulting in confusion and a need to reconcile overlapping roles and responsibilities. LATAM should note this complexity as the region continues to develop cybersecurity legislation and initiatives. Governments and stakeholders in LATAM may benefit from proactively identifying opportunities to partner with existing global information-sharing communities to minimize fragmentation, leverage established expertise, and address budgetary constraints. Such partnerships can reduce the need to build new systems from scratch, ensuring cost-effective solutions that draw on proven models. By considering these factors, LATAM can design information-sharing mechanisms that balance the need for regional relevance with opportunities for international cooperation, learning from both the successes and challenges of the EU's experience.

[15] Financial Services ISAC, Emerging Trends to Cyber Risks: A Latin American Perspective.
[16] ENISA, ISACs Cooperative Models.
[17] The NIS 2 Directive, https://www.nis-2-directive.com/ (last accessed Oct. 22, 2024).
[18] Ibid.

KEY BENEFITS

Improved Security Posture and Collective Defense

The main benefit of an ISAC is providing collective defense. If one organization is experiencing a cyber-attack, there is a strong likelihood that other organizations in the region, or even globally, are as well. Sharing information, best practices, or remediation measures from previous attacks can help ISAC members adjust their defenses accordingly. Doing so also encourages members to take proactive measures against vulnerabilities that are shared within an ISAC, preventing members from waiting for disaster to strike.[19]

Community-Based Cybersecurity Expertise

Smaller entities often lack the resources necessary to consistently monitor threats, evaluate impacts, and develop robust mitigation plans. Resources, financing, and staffing for cybersecurity initiatives are often difficult to obtain, so engaging in an ISAC allows organizations to leverage the pooled expertise of partner entities. ISAC members participate in educational webinars and workshops and are in communication channels and secure group chats that facilitate quick and reliable access to information. If a member organization of an ISAC has a question specific to their industry, the ISAC communication channels enable them to ask a reliable network of their peers rather than resorting to time-costly research. ISACs also have a history of responding to and sharing actionable and relevant information more quickly than government partners.[20]

Enhanced Community Trust and Resilience

ISACs foster greater trust and a sense of community among their members, by creating an environment where collaboration and mutual support are prioritized. This trust is crucial in addressing ever-evolving cyber threats, as it encourages the proactive and timely sharing o actionable intelligence. Beyond intelligence sharing, ISACs enable their members to collectively achieve a robust security posture by pooling resources, and expertise – elements often inaccessible to individual organizations alone. By leveraging this shared connection, ISACs enhance information security and resilience against cyber threats while minimizing additional costs to their members. [21] Moreover, ISACs play a vital role in promoting digital literacy and

[19] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing Best Practices, Aug. 2023, https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.
[20] National Council of ISACs, About ISACs.
[21] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing

fostering communication, collaboration, and problem-solving skills among their members – key principles aligned with UNESCO's digital-literacy framework. [22] This sense of community, coupled with practical benefits, makes ISACs invaluable in the increasingly interconnected digital landscape.

Improved Cybersecurity Innovation

By enhancing sector-wide situational awareness through information sharing, organizations will receive advanced threat warnings and can take proactive steps to mitigate potential intrusions. As innovations in attacks continue, especially with the integration of generative AI enhancing the abilities of attackers, security teams must ensure their organizations evolve alongside unique sector challenges, standards, and best practices to keep their operations safe. Engaging with sectoral partners through ISACs will enable entities to do so.

Government Benefits

Close cooperation with private-sector members allows public government entities to gain a deeper understanding of industry-specific challenges, which is invaluable when shaping cybersecurity legislation and strategy. By participating in ISACs, public entities may gain insights into the cybersecurity posture of key sectors through shared information about threats, incidents, and vulnerabilities. This participation, when approached with respect for varying levels of tolerance for information sharing with the government, can help public entities better understand the evolving cyber landscape and enhance their ability to support critical sectors. Furthermore, this collaboration helps streamline communication and coordination, ensuring that policies and strategies are well-informed and more aligned with the practical needs of the sectors they aim to protect.

ISAC CHALLENGES

While participating in an ISAC can produce many benefits to the participants and the overall cybersecurity ecosystem, there are various challenges that can present obstacles to the success of the information sharing.

Lack of Resources/Funding

The largest overarching challenge for both public and private members of ISACs is the lack of human resources and finances dedicated to information sharing and analysis. This is an

Best Practices, Aug. 2023, https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.

[22] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 118, April 2024, https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.

issue generally for the cybersecurity ecosystem, but it is exacerbated in information analysis. Specifically, it affects organizations that do not have enough personnel to dedicate to actively participating in the ISAC and for governments that may not have the capacity to fill a secretarial or facilitator role. This lack of funding and dedicated personnel can pose a barrier to entry for smaller- and medium-sized entities. It is likely that larger, more mature companies will have the means to afford membership, which could potentially skew membership concentration away from smaller entities that would benefit the most from joining. Additionally, due to the wide array of members' maturity levels and preexisting cyber knowledge, information shared within the ISAC may not be understood by some members. It is the job of the ISAC to contextualize the resources shared so that it is digestible by all actors within the group regardless of their size and maturity. Many ISACs invest membership fees in training and capacitybuilding programs to give members access to higher levels of technical expertise.[23] However, a lack of funding can impact the level of analysis delivered to participants.

Minimum Level of Expertise/Participation

Because of varying levels of maturity, ISAC participants must have a minimum level of technical and organizational skills to participate actively in the information sharing and exercise activities. A successful collaboration scheme should be structured with incentives for active information sharing so that all members are actively engaged. It is also critical to involve C-level executives in addition to technical personnel in information exchange and training exercises. As such, the value of an ISAC is demonstrated to executive leadership, and dedicated business funds can be allocated to such resources.

Building Trust/Cultural Differences

Privacy and confidentiality concerns are consistently present for prospective ISAC members, but existing ISACs implement significant data-privacy protection measures. These commonly include strict access controls, anonymization techniques, and secure communication channels.[24] ISACs also consult with legal experts to devise plans for adhering to privacy regulations, and ISACs consult with external policy experts to remain up to date on changing laws and regulations.[25] ISACs are conscious of striking the balance between open and productive information sharing and privacy concerns. Other common concerns may include language barriers, cultural differences, or differing levels of expertise across various fields.

[23] Ibid.
[24] Blue Goat Cyber, The Impact of Information Sharing Analysis Centers on Cybersecurity, https://bluegoatcyber.com/blog/the-impact-of-information-sharing-and-analysis-centers-on-cybersecurity/, (last accessed July 26, 2024).
[25] Ibid.

ISACs can offer translation services and tend to standardize information-sharing formats and protocol to make the process as accessible as possible across sectors.[26] Consequently, sharing information in an ISAC is one of the only ways to communicate across sectors with a mandated baseline of privacy and security involved. The idea of openly sharing information to prevent threat actors may seem counterintuitive, but ISACs are environments where confidentiality and ethical sharing are routine guidelines, and all members are treated equally.

Clear Roles and Responsibilities

The flexibility inherent in the various models for an ISAC's structure, governance, and roles and responsibilities can present significant challenges for organizations seeking to establish or participate in such initiatives. While this flexibility allows for customization based on specific industry needs and regional contexts, it can also lead to inconsistencies in how information is shared and managed. Diverse governance frameworks may create confusion regarding decision-making processes and accountability, making it difficult for members to understand their roles and responsibilities. Additionally, differing levels of commitment and resource allocation among members can create uneven participation, potentially hindering the effectiveness of the ISAC. This lack of standardization may complicate collaboration and reduce the overall trust necessary for successful information sharing. These challenges are further heightened in regions such as Latin America, where significant disparities exist in organizational maturity regarding cybersecurity understanding and readiness. However, these challenges can be mitigated by adopting a mixed approach that leverages country-based models while focusing on key sectors with higher maturity levels, such as the financial sector. This strategic alignment allows for tailored solutions that foster collaboration, enhance trust, and ultimately strengthen the region's overall cybersecurity posture.

STRUCTURAL MODELS

While there are many approaches one can take to organize an ISAC, two overarching models have emerged:

- Country-focused model and
- Sector-specific model.

Country-Focused Model

This cooperation model focuses on a single country, uniting all relevant experts and computer security incident response teams (CSIRT) under a single initiative. The countryfocused model

[26] Ibid.

can produce informal arrangements governed by the CSIRT community itself or more formalized engagements orchestrated by a country's government. Government-facilitated ISACs are characteristic for smaller countries, where it is easier for the public sector to facilitate an ISAC due to the smaller number of stakeholders. See below for examples of country-focused ISACs:

- **CERT.LU** – A country-based initiative for all computer emergency response teams (CERTs) in Luxembourg that was created to exchange information between the network of CSIRTs in the country.[27] This ISAC is governed by the CERT community itself.[28]

- **Finland** – Multiple ISACs are orchestrated under the National Cyber Security Centre (NCSC-FI). The NCSC-FI collects and analyzes security-threat information from various sources, such as ISACs and early-warning and detection systems, then shares that information with NCSC-FI constituents through multiple channels, including ISACs.[29]

Sector-Specific Model

This model focuses on the sectoral level of critical infrastructure with the goal of sharing information and analysis with other experts active in the sector. Generally, this approach is led by private-sector stakeholders with minimal funding from the government, particularly in the US, where public funding for ISACs is uncommon. However, there are no restrictions on government funding, and governments in LATAM could provide financial support on a case-by-case basis, especially in scenarios like sharing information on specific incidents. The sector-specific model is widely used in larger countries that have a strong private sector with clearly defined cybersecurity goals and larger budgets allocated to information-sharing efforts. See below for examples of sector-specific ISACs:

- **Financial Services (FS-ISAC)** – Founded in 1999 to advance cybersecurity resiliency in the global financial system by protecting financial institutions and the individuals they serve. While the FS-ISAC is headquartered in the US, the ISAC now has members in over 75 countries, demonstrating the flexibility and reach that a single ISAC can have.[30]

- **Banking Cybersecurity Center (BCC) Poland** – A platform for banks to communicate and exchange information on vulnerabilities and relevant threats. Membership is open to any commercial bank in Poland.[31] The BCC is an example of an ISAC that is both sector specific and country focused.

[27] The terms **CSIRT (Computer Security Incident Response Team)** and **CERT (Computer Emergency Response Team)** are often used interchangeably, but there are subtle differences in their origins and branding.
[28] CERT.LU, About CERT.LU, https://www.cert.lu/ (last accessed Oct. 18, 2024).
[29] ENISA, Information Sharing and Analysis Centres (ISACs) Cooperative Models, 2017, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models?v2=1.
[30] FS-ISAC, What We Do, https://www.fsisac.com/ (last accessed Oct. 18, 2024).
[31] ENISA, ISACs Cooperative Models.

Sector-specific ISACs can also be structured to have international participation, expanding the scope of the ISAC beyond a single country. International ISACs face challenges with building trust, which can be more difficult due to the cultural differences of stakeholders.[32] See below for examples:

- **EU FI-ISAC** – The European Financial Institutes ISAC was created in 2008 to exchange information on cyber-criminal activity affecting the European financial community. Membership comprises country representatives from the financial sector, national CERTs, and law-enforcement agencies. Other organizations represented are ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC), and the European Commission. The EU FI-ISAC is actively supported by ENISA.[33]

- **EE-ISAC** – The European Energy ISAC aims to improve the resilience and security of the European energy infrastructure by sharing trust-based information and enabling a joint effort for threat analysis. Members include technical and service providers, utilities, academia, research institutes, and governmental and nonprofit organizations.[34]

ROLES AND RESPONSIBILITIES

An ISAC is an effective mechanism for facilitating public-private cooperation, but it is important to define the roles and responsibilities of all entities involved so that the organization can function effectively. In every ISAC, there will be a "facilitator," the "members," and ISAC "partners." The facilitator fills the secretarial role of establishing the logistics for the group, such as setting the meeting cadence, recruiting new members, and marketing.[35] Most facilitators also provide the technical and process infrastructure necessary to enable information sharing, ranging from simple tools, such as email lists, to sophisticated platforms for sharing and analyzing indicators of compromise (IOCs). A member is an entity that is actively sharing and receiving information as a benefit from membership and is actively paying membership fees to participate. Finally, ISAC partners include subject-matter experts and entities that participate in dedicated sessions, usually to offer specific expertise on a particular topic. Below, the activities of each relevant stakeholder in an ISAC are explored. It is important to note that unclear roles and responsibilities impede the ability of an ISAC to properly function.

[32] ENISA, ISACs Cooperative Models.
[33] ENISA, European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance/european-fi-isac-a-public-private-partnership (last accessed Oct. 18, 2024).
[34] European Energy Information Sharing & Analysis Centre, Home, https://www.ee-isac.eu/ (last accessed Oct. 18, 2024).
35 ENISA, ISACs Cooperative Models.

Public Sector

Public-sector government institutions can have different roles in an ISAC depending on the circumstance. An administration may fulfill the facilitator role by providing places for the group to meet in addition to other secretarial functions. Governments may even allocate direct funding to help further develop the ISAC. Alternatively, public administrations may create a legal framework for both the exchange of information and the creation of an ISAC.[36] However, the role of public administration varies according to the entity's task. For example, National Cybersecurity Agencies (NCAs) are organizations that are typically involved in ISACs, either through the facilitation of the ISAC itself or by actively participating in the information exchange and analysis. Most NCAs operate a CSIRT, which is also a critical body to involve in an ISAC. It is common for around one to two public bodies to participate in an ISAC, whether on a regular or ad hoc basis.

Law Enforcement and the Intelligence Community

Law-enforcement agencies and intelligence services can be valuable partners in ISACs because of their specialized missions and access to valuable information. In the US, law enforcement and ISACs engage routinely as much of the information shared by law enforcement is not classified in the traditional sense, even if it is not publicly available. However, intelligence community (IC) agencies generally limit their engagement with ISACs due to the classified nature of their information. It is nevertheless important to maintain ties with these communities and incorporate them as partners in dedicated topical sessions.

Industry and Critical-Infrastructure Owners and Operators

Industry should be the main driving force behind all ISACs, both as facilitators and members. Even when public administration is involved, it is industry that should determine the shape and functionality of their cooperation.[37] The private sector owns most critical infrastructure. As critical-infrastructure technology and service delivery become more efficient through digital transformation, asset owner/operators become increasingly dependent on the smooth and secure functioning of both information technology (IT) and operational technology (OT). This makes cybersecurity a business imperative that is necessary to ensure the safe delivery of services, public trust, and business continuity. Moreover, the participation of industry companies should span a wide breadth of entities, including critical-infrastructure asset owner/operators and the operational technology vendors on whose technology products those owner/operators rely.

[36] ENISA, ISACs Cooperative Models.
[37] Ibid.

Academia

ISACs typically introduce academia as a partner so that government and industry can clearly communicate their needs in research and development.[38] The interaction with academia may result in new solutions for critical sectors and the overall cyber landscape. It is also an effective forum for researchers to verify the viability or outcomes of their research in practice while receiving feedback from critical-infrastructure owners and operators.

GOVERNANCE AND FUNDING

Consistent with their flexible nature, ISACs can be governed in many ways. Some have a clear governance structure with well-defined roles, such as the secretariat and a management board, while others have no clear structure and are flexible communities where volunteers organize the meetings. The main activities of the ISAC (meetings, exercises, etc.) are defined by the governance structure. The more structured an ISAC, the more specific the tasks to deliver. However, with less structure, an ISAC may be less active and focus on ad hoc specialty cases. Both are valid governance models and can be adjusted to the needs of the ISAC members.

Structured Governance Approach

The management structure of an ISAC can vary. Some are led by a chair and vice-chair, while others opt for a management board or steering committee. These leadership roles are typically not elected and may include a combination of paid and volunteer work, depending on the size and scope of the ISAC itself. These positions are usually assigned to private-sector members or organizations that are deeply engaged with the ISAC. Once in place, their main role is to develop a strategic plan to guide the community’s goals. These structures often include clear election rules and terms of reference.[39]

Governance with Support Body

In other cases, an ISAC may designate a single entity to fill the secretariat role. This is most common when the public sector is involved with an ISAC. In this scenario, the public administration oversees frequent group interactions to correspond with a detailed agenda.

[38] ENISA, ISACs Cooperative Models.
[39] Ibid.

Flexible Governance

Some ISACs have no clear governance structure and no defined roles, which results in a highly flexible community, usually led by volunteers. A different organization or representative volunteers to host each meeting, rotating the responsibility every time. These ISACs do not typically have a formal action plan, and decisions are made on an ad hoc basis to address challenges as they arise. In this flexible approach, meetings are held in various locations, which allows the community to gain insights into the cultures of their peers. However, the lack of formality can lead to lower engagement from stakeholders.

Funding

Like structure and governance, there are multiple ways to fund an ISAC, which will be important for LATAM to consider as they begin to formalize information sharing in the region.[40]

- **Mandatory Fees** – This is the most typical funding model for an ISAC. Fees are paid annually and vary based on the size and involvement of the entity.
- **Voluntary Contributions** – In this model, members provide monetary assistance in addition to necessary resources, such as hosting meeting locations, providing dedicated staff towards ISAC activities, developing working groups, etc.
- **Government Subsidies** – While rare, governments may provide funding when there is a program or legal framework in place. This funding usually covers facilitation, such as running a secretariat or providing meeting spaces, and is meant to encourage industry participation rather than sustain the ISAC long term.

CORE CAPABILITIES

In this section, the key capabilities that an ISAC may provide to its members are highlighted:

Information Sharing – Information sharing is the core function of an ISAC, allowing members to exchange critical intelligence that helps them collectively defend against cyber threats. This includes threat indicators (such as IP addresses or malware signatures); incident details (such as attack techniques, intent, and impact); vulnerabilities (in software, hardware, or business processes); and mitigation strategies (such as security patches or antivirus updates). Members also share best practices, from incident-response strategies to security controls. Information is shared through secure platforms, including anonymous web portals like MISP,41 encrypted emails, and face-to-face meetings. By facilitating the timely and secure exchange of this information, ISACs enable organizations to quickly adapt to emerging threats, improving their overall resilience, and reducing the potential for widespread cyber incidents.

[40] ENISA, ISACs Cooperative Models.
[41] MISP Threat Sharing, https://www.misp-project.org/ (last accessed Oct. 23, 2024).

Regular Meetings and Working Groups – Regular meetings and topic-specific working groups are essential for maintaining communication and fostering collaboration among ISAC members. These gatherings unite industry experts and partners to tackle pressing cybersecurity issues. By providing a platform for continuous dialogue and knowledge exchange, ISACs enable deeper expertise and more proactive problem-solving, ensuring members are prepared to handle evolving cyber risks.

Conferences and Side Events – Conferences and side events raise awareness about the ISAC's activities and broaden stakeholder engagement. These events allow participants to learn about emerging trends, technological advancements, and cybersecurity strategies. Side events, which can include workshops, roundtable discussions, and training sessions serve as targeted platforms to address specific areas of interest or challenges within the industry. They also provide opportunities for networking and collaboration, increasing the influence and reach of the ISAC within the industry. These gatherings are crucial for keeping stakeholders informed and connected.

Exercises – ISACs conduct exercises to assess and improve their members' cybersecurity readiness. These exercises can range from governance-level tabletops, ensuring executives are prepared to make critical decisions, to operational and technical drills that test an organization's ability to implement procedures and use cybersecurity tools effectively.[42] Such exercises are vital for identifying gaps, validating preparedness, and enhancing incident-response capabilities across all organizational levels.

Analysis – Analysis is a key value-added service provided by ISACs, helping members understand and prioritize cyber risks. ISACs perform vulnerability and threat analysis by pooling expertise from participating organizations, often through joint working groups. This collaborative approach allows for the development of comprehensive insights into emerging threats, assisting members with anticipating and mitigating risks. Although conducting detailed analysis can be resource-intensive, members recognize its value and are typically willing to bear the costs.

Additionally, ISACs offer vital **legal and regulatory knowledge** related to information sharing. Understanding the legal landscape is critical as privacy laws and regulatory obligations like mandatory incident reporting can both pose barriers to and create new demands for effective information sharing. ISACs provide guidance on how to share information while remaining compliant with these regulations, offering members peace of mind and encouraging more open exchanges of data.

[42] ENISA, Cross-Sector Exercise Requirements, March 2022, file:///C:/Users/acs07/Downloads/Cross-sector%20exercise%20requirements%20(1).pdf.

For ISACs lacking a dedicated analysis team, the task of providing consistent threat analysis can be overwhelming, with large volumes of data requiring significant time and resources. In such cases, collaboration with government agencies—for example, ENISA in pan-European initiatives—can help enhance ISACs' analytical capacity.[43]

Trust Building – Trust is the foundation of any effective ISAC. By facilitating frequent interaction, ISACs encourage open communication and collaboration between members. Building personal relationships and establishing formal mechanisms, such as non-disclosure agreements, codes of conduct, the use of Chatham House rules, and Traffic Light Protocol (TLP), ensures members feel confident in sharing sensitive information. Trust enhances the overall effectiveness of information sharing, making an ISAC more resilient and reliable.

[43] ENISA, ISACs Cooperative Models.

Assessing the Need for a LATAM ISAC

Latin America is a highly targeted region for cyber threats, driven by unique regional characteristics that act as "accelerators," such as the widespread use of unlicensed software; high rates of software piracy; and the rapid digitization of its financial markets, including the emergence of numerous fintech companies.[44] The wide maturity gaps in incident-response and cybersecurity capabilities that exist among LATAM countries make it a prime target for threat actors, with some countries experiencing over 1,000 cyber-attacks per second.[45] The total value of the 2024 Cybersecurity Market in Latin America was $8.92 billion, and that number is expected to increase to exceed $12.48 billion by 2029.[46] Growing cyber threats in LATAM present a significant need to enhance formalized information sharing in the region. This section reviews how the creation of ISACs in LATAM would benefit the threat landscape and align with stated policy goals related to digital governance, multistakeholder collaboration, and workforce development.

The creation of ISACs in LATAM would benefit the threat landscape and align with stated policy goals related to digital governance, multistakeholder collaboration, and workforce development.

THREAT LANDSCAPE

The LATAM region is highly integrated: cyber-attacks may impact entities far beyond the original scope of an attack, which makes regional resilience crucial. Some LATAM countries are already beginning to mirror the proactive efforts of each other. For example, after the 2023 series of ransomware attacks on Costa Rica, El Salvador acted to develop a robust cybersecurity program and update their subsequent policies to avoid a similar situation.[47] An ISAC would provide a formalized method for sharing the lessons learned and facilitating the development of stronger national cybersecurity policies throughout LATAM.

Currently, LATAM relies on countries actively engaged in information sharing for incident-response assistance, funding, and direction in developing cyber strategies. When cyber incidents occur, countries participating in formalized information-sharing networks are better positioned to respond and recover from attacks. For instance, the US has the

[44] Americas Quarterly, How Latin America's Governments Compare on Anti-Piracy, January 17, 2019, https://www.americasquarterly.org/article/how-latin-americas-governments-compare-on-anti-piracy/.
[45] Jamaica Major Organized Crime and Corruption Agency, Combatting Cyber Crime, https://www.moca.gov.jm/cyber-crime, (last accessed Jul. 25, 2024).
[46] Mordor Intelligence, Latin America Cybersecurity Market Size (2024-2029), https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market/market-size, (last accessed Jul. 25, 2024).
[47] Telecommunications Industry Association, Costa Rica Takes Bold and Decisive Stance on Cybersecurity, Sept. 6, 2023, https://tiaonline.org/press-release/costa-rica-takes-bold-and-decisive-stance-on-cybersecurity/.

most robust network of ISACs in the world and ranks first on the global cyber index with a score of 100.[48] When Costa Rica experienced a crippling ransomware attack, costing them the equivalent of $30 million per day, the US, Israel, and Spain stepped in. These countries engage in cyber ISACs and were equipped to help the situation in Costa Rica in part due to the resources and knowledge they gained because of their enhanced information sharing.[49] As such, beginning to invest in forming ISACs in LATAM will enhance regional resilience and lessen the region's reliance on external partners.

Not sharing information can be more dangerous than the risks taken with sharing because many hackers now operate by sharing their own strategies with each other to yield greater value.[50] As such, participating in an ISAC levels the playing field against malicious actors who already engage in their own information sharing. As much as building trust is a challenge, it is also an opportunity for greater regional unity. ISAC participants can proactively alert peers of prevalent threats and learn from the shared experiences of others. While building trust is a longer-term process, the success of ISACs in other parts of the world demonstrates the positive potential of ISACs to enhance regional cyber resilience.

POLICY ALIGNMENT

Developing ISACs in LATAM aligns with the region's growing attention to digital governance. Multiple countries have begun developing National Cybersecurity Strategies or proposing legislation for a National Digital Security Agency, which includes information sharing and greater multistakeholder collaboration as stated initiatives. For example, Chile implemented a new national cybersecurity policy in March of 2024, "The Chilean Law on Cybersecurity and Critical Infrastructure."[51] As a groundbreaking law in LATAM, its goal is to promote risk management; implement security standards to improve prevention, including responses to cyber-attacks through public-private partnerships (PPPs); and establish cybersecurity obligations resulting in sanctions if not complied with. The law additionally created a National CSIRT and a Multisectoral Council, resulting in all organizations, whether public or private, falling under the scope of the CSIRT if they provide services that impact critical infrastructure. An ISAC, by definition, is the sharing of information between public/private entities, the use of multistakeholder engagement, and sharing threat and incident response to cybersecurity pertaining to critical infrastructure. These three things were outlined as goals in the Chilean Law but implemented in different, decentralized

[48] ITU Publication, Global Cybersecurity Index.
[49] Cytek Security, Enhancing the National Security Posture of Costa Rica with an Integrated Approach, Jan. 9, 2024, https://cytek-security.com/resources/enhancing-the-national-security-posture-in-costa-rica-with-an-integrated-approach/.
[50] Computer Security Online, What is an ISAC or ISAO?, July 26, 2022, https://www.csoonline.com/article/567485/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.
[51] National Cybersecurity Coordination, Chilean Government Enacts Cybersecurity Law, Mar. 26, 2024, https://ciberseguridad.gob.cl/en/news/chile-enacts-cybersecurity-law-creates-cybersecurity-agency/#:~:text=The%20digital%20security%20of%20Chileans,cybersecurity%20actions%20of%20State%20agencies.

ways. Establishing an ISAC would directly appeal to existing Chilean goals and unify their implementation, making it easier to track progress.[52]

Mexico engaged in efforts to increase coordination and information exchange when, in August of 2022, Mexico and the US established a "Cyber Issues Working Group" to promote a "shared commitment to an open, interoperable, secure, reliable internet and a stable cyberspace."[53] A prominent initiative in the working group was strengthening technical coordination mechanisms for addressing cyber threats. This is the core goal of an ISAC, further demonstrating how a LATAM ISAC would seamlessly align with efforts already underway across the region. Additionally, industry experts in Brazil recently called for the establishment of a National Digital Security Agency to centralize resources and enable the implementation of Brazil's National Cybersecurity Strategy. The agency would retain cybersecurity at the top of the Brazilian government's priorities, which is crucial considering Brazil ranks as the second most vulnerable country to cyber-attacks globally.[54]

It is important to note that policies vary heavily in their development, creating significant gaps in cyber-readiness throughout LATAM. According to the GCI (ITU's Global Cybersecurity Index), Mexico received a cybersecurity preparedness score of 81.75, while Honduras received a score of 2.2.[55] The variability in cybersecurity preparedness is substantially higher in LATAM compared to other global regions, indicating that enhanced information sharing could yield significant results for LATAM countries falling behind on cyber-readiness.[56] An ISAC can bridge this maturity gap between LATAM countries by sharing lessons learned and encouraging smaller actors to take proactive steps in securing their systems.

MULTISTAKEHOLDER COLLABORATION

ISACs clearly align with existing global information-sharing and PPP initiatives. As of 2022, 99 countries have signed or ratified a multilateral agreement on information sharing, and over 140 countries have participated in international activities, such as cybersecurity conferences, workshops, partnerships, and conventions with other countries.[57] Additionally, 86 countries have engaged in either international or domestic PPPs, while 62 countries worldwide have engaged in both.[58] Information sharing has demonstrated its value at an international level, with governments worldwide committing to increase participation

[52] Lexology, Stepping up in Latin America: Chile enacts a new Cybersecurity Law, https://www.lexology.com/library/detail.aspx?g=82a52636-a23c-4b8b-9158-3203f69a3fb0#:~:text=Chile%20has%20also%20approved%20its,legislation%20and%20regulation%20in%20Chile, (last accessed July 25, 2024).

[53] Carnegie Endowment for International Peace, Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO, May 28, 2024, https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en¢er=russia-eurasia.

[54] Center for Cybersecurity Policy and Law, Hearing Highlights Industry Calls for Brazilian National Digital Security Agency, July 16, 2024, https://www.centerforcybersecuritypolicy.org/insights-and-research/hearing-highlights-industry-calls-for-brazilian-national-digital-security-agency.

[55] ITU Publications, Global Cybersecurity Index 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (last accessed July 24, 2024).

[56] ITU Publications, Global Cybersecurity Index.

[57] ITU Publications, Global Cybersecurity Index.

[58] ITU Publications, Global Cybersecurity Index.

in PPPs and information-sharing mechanisms. For example, an analysis of Jamaica's digital economy by The World Bank Forum found that a lack of information sharing with the private sector was a contributing to weakening the country's cybersecurity architecture. The research noted that the "absence of formal forums and channels of communication for cooperation to further digital trust, and limited shared knowledge," limits Jamaica's cyber resiliency.[59] Thus, a LATAM ISAC aligns with the global movement towards greater information sharing and could increase the resiliency of LATAM's less cyber-ready countries.

Current information-sharing efforts in LATAM (which are explored in greater detail below) would not be considered formal mechanisms like an ISAC, as they do not engage the full spectrum of relevant stakeholders and often limit participation to other national-level government counterparts. Additionally, there is no single centralized platform to connect the various initiatives mentioned above. The OAS CSIRT Americas Network exemplifies this issue as participation is limited to other government CSIRTs but does not include stakeholders from the private sector or academia.[60] Another example is the Forum of Incident Security and Response Teams (FIRST), which aims to unite incident-response and security teams in the region and is based on a peer-to-peer network-governance model of CSIRTs.[61] Progress in creating national CSIRTs is extremely positive and has produced a significant amount of cyber intelligence across many vendors. However, either this information is not visible to most organizations because they are excluded from current information-exchange efforts, or organizations lack the maturity and mechanisms to process and understand the threat information that has been collected.

Limiting participation in information-sharing efforts will only further restrict LATAM's ability to combat increasing cyber-attacks. As a region, when incidents occur, it is crucial that all sectors have access to pertinent information. A LATAM ISAC would bridge this information gap and engage stakeholders from private industry and academia to participate in the exchange of threat information and best practices, creating a cohesive environment where all relevant parties are included. ISACs also enable less mature actors, like small- and medium-sized entities, to understand and implement the information shared. Without a centralized hub for information sharing, many of the resources LATAM countries are investing large sums of time and money into may not be fully utilized as participation is limited. A dedicated LATAM ISAC would also enable the information shared to have a true LATAM context rather than relying on international partners without the same insight into regional issues to strengthen cybersecurity.[62]

[59] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 153, April 2024, https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.
[60] CSIRT Americas, https://csirtamericas.org/en (last accessed July 24, 2024).
[61] FIRST, Vision and Mission Statement, https://www.first.org/about/mission (last accessed Jul. 26, 2024).
[62] Trade EC Europa, Cybersecurity Sector in Central America, November 2022, https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf.

TALENT ATTRACTION AND EDUCATIONAL OPPORTUNITIES

The benefits of information sharing surpass incident response: a LATAM ISAC could be a steppingstone to increasing cyber-talent attraction and retention alongside fostering a more cyber-conscious community. LATAM experiences wide disparities in internet access across the region, impacting the feasibility of building a cyber workforce. While there has been some progress in creating educational cyber initiatives, it is fragmented, with most efforts being made in concentrated areas. Although over 1,600 universities in the region offer graduate and postgraduate programs in digital-technologies training, they are limited to specific countries: Argentina, Brazil, Chile, Colombia, Mexico, Peru, Ecuador, Costa Rica, and Uruguay.[63] Moreover, within these countries, Argentina houses 66% of the universities offering such courses.

Educating the general LATAM public on cyber initiatives, opportunities, and basic skillsets has the potential to create job opportunities for the ~60% of workers across the region whose employment is informal.[64] Yet, this will require that a higher percentage of the population is digitally connected and educated in order to increase the cyber workforce. In a CEPAL survey from 2020, 75% of the wealthiest areas across Latin America and the Caribbean used the internet, while only 37% of the poorest quintile had internet access.[65]

Several countries in the region have begun offering free online digital-skills training, such as the Digital Skills Development Plan "IFT teaches you," the Centros de Transformación Digital Empresarial in Colombia, and the Infocentros Comunitarios in Ecuador. In Brazil, the National Research and Education Network (RNP), SENAI-SP, and Softex created a free cybersecurity course called "Hackers do Bem" for those interested in working in the cybersecurity field.[66] However, these efforts are ad hoc, and LATAM lacks overarching, regional resources for enhancing digital literacy.[67] To make meaningful change in the region, educational opportunities must have a wider outreach, enhancing collective understanding throughout all LATAM. As a hub for academics, government officials, and private-sector organizations, an ISAC can expand the effective work being done, collectively bridging the educational divide and increasing talent attraction for a cyber workforce. ISACs offer the unparalleled opportunity to meet the unique needs of Latin America and the Caribbean, surpassing just information sharing to facilitate other important initiatives, such as educational opportunities and workforce development.

[63] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 105.
[64] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020.
[65] The World Bank, The Digital Economy Initiative for Latin America and the Caribbean, April 2024 https://www.worldbank.org/en/programs/de4lac.
[66] Hackers do Bem, About the Program, https://hackersdobem.org.br/o-programa.
[67] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 108.

EXISTING INFORMATION-SHARING INITIATIVES

Many LATAM countries have implemented preliminary initiatives towards fostering greater information sharing. Most initiatives are country based, and while some have made strides to incorporate private-sector involvement, many lack the formality and wide engagement of a true ISAC. This section provides an overview of the various initiatives in place.

Brazil's Federal Cyber Incident Management Network – In Brazil, federal public-administration institutions are mandated to participate in the Federal Cyber Incident Management Network, through which threat, incident, and vulnerability information is shared.[68] Public companies, mixed-capital companies, and their subsidiaries may join the network on a voluntary basis.[69] While the network is open to public companies, it is primarily aimed at facilitating information sharing between federal public institutions. However, alternative mechanisms exist within Brazil. For example, in the telecommunications sector, a working group established by Anatel uses a malware information-sharing platform (MISP) to share information on threats and vulnerabilities.[70] Additionally, financial organizations, such as The Brazil Federation of Banks, have reported participating in international information-sharing networks, such as the Financial Services Information Sharing and Analysis Network (FS-ISAC). The financial sector has noted that information sharing between all critical-infrastructure sectors could be automated leveraging the use of MISP, for example.[71]

Belize – Smaller LATAM nations, such as Belize, have also begun to prioritize and commit to increased information sharing. Belize released their Cybersecurity Strategy 2020–2030, which includes a stated priority for "developing a national capacity for incident response and critical information infrastructure protection."[72] Within this priority area, Belize will develop a dialogue with key sectors in a "phased approach to adopt an information sharing protocol."[73] A regional ISAC would complement these regional initiatives and facilitate greater regional resiliency.

CSIRT Americas Network – The Organization of American States (OAS) operates a regional Computer Security Incident Response Team (CSIRT) Americas Network, which promotes the exchange of information on security

[68] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil, p. 46, Aug. 2023, https://www.gov.br/gsi/pt-br/ssic/eventos/CMMreportBrazil2023_finalversoemingls.pdf.
[69] Brazilian-American Chamber of Congress, Brazil creates cyber-attack response network, Jul 27, 2021, https://brazilcham.com/brazil-creates-cyberattack-response-network/.
[70] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil.
[71] Ibid.
[72] Government of Belize, National Cybersecurity Strategy Towards a Secure Cyberspace 2020-2030, pg. 27,https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf (last accessed Jul. 25, 2024).
[73] Ibid.

threats, provides technical assistance to strengthen CSIRT services, and offers training to cybersecurity specialists.[74] The CSIRT Americas Network demonstrates the willingness of regional governments to participate in information sharing and serves as a foundational example for information exchanges within the region. The network is primarily targeted at existing CSIRTs in the region but also has outside industry partners that engage with the group.

CSIRT Financiero (Asobancaria) – CSIRT Financiero is led by the Banking and Financial Institutions Association of Colombia, Asobancaria, a nonprofit representative association of the Colombian financial sector. It supports financial institutions to anticipate and mitigate risks arising from cyber threats through information exchange and cooperation with national and international organizations.[75] It is the vision of the CSIRT to be the financial sector's focal point for the exchange of cyber-threat information based on the principles of trust and to be the research and innovation center that strengthens threat prevention for the sector. This initiative may be well-placed to serve as an official pan-LATAM financial sector ISAC that engages entities from all Latin America and the Caribbean, beyond just Colombia.

Dominican Republic "Cyber Drill" – During the summer of 2023, the Dominican Republic conducted their annual "Cyber Drill," which convened various organizations within the region and additional international stakeholders from the US and Canada.[76] The Cyber Drill operated similarly to an in-person ISAC session, with the purpose being to "offer a space for analysis and discussion about national needs, actions, and initiatives, plus capacity building through cyber incident simulation labs towards the protection of national critical infrastructures, and the cybersecurity of the region, among other important national critical aspects." Governments, institutions, and/or national CIRTs/CERTs collaborated with technicians and representatives on cybersecurity, and sharing sessions provided a platform for cooperation and discussions on cybersecurity.[77]

FIRST – The Forum of Incident Response and Security Teams is a premier organization and recognized global leader in incident response. FIRST unites a wide variety of security and incident-response teams from government, commercial, and academic sectors. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate a rapid reaction to incidents, and to promote information sharing among members and the wider community.[78] Currently, FIRST has more than 700 members across Africa, the Americas, Asia, Europe, and Oceania. While FIRST is not solely dedicated to the LATAM region, its robust network of members should be leveraged for subsequent LATAM-focused information-sharing efforts.

[74] CSIRT Americas, https://csirtamericas.org/en (last accessed July 24, 2024).
[75] CSIRT Asobancaria, https://www.csirtasobancaria.com/quienes-somos (last accessed Oct. 28, 2024).
[76] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023, June 19, 2023, https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2023/cyberdrill-23-Dominican-Republic.aspx#gsc.tab=0.
[77] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023.
[78] FIRST, https://www.first.org/ (last accessed Oct. 28, 2024).

FEBRABAN – The Brazilian Federation of Banks (FEBRABAN) was founded in 1967 as a nonprofit association that engages with stakeholders for the purpose of contributing to the economic, social, and sustainable development of Brazil.[79] In 2020, the FEBRABAN Cybersecurity Laboratory was created with the aim of facilitating collaboration between the teams of associated banks in actions to prevent, identify, and combat cybercrime. This initiative could be a useful starting point to enhance cooperation and information sharing in the region's financial sector.

LACNIC – The Internet Address Registry for LATAM is an international non-governmental organization established in Uruguay in 2022. Its mission is to manage the digital resources of the internet in LATAM by maintaining standards of excellence and transparency and promoting a participatory model for policy development. LACNIC leads the ongoing construction of the regional community by strengthening technological capabilities and applied research for the development of a stable and open internet.[80]

LACNIC is managed and directed by a sevenmember board of directors elected by its members, a group of more than 12,500 entities that operate networks and provide services in 33 territories in LATAM. LACNIC also runs a CSIRT, which conducts the "coordination functions necessary to strengthen the response capabilities to incident related to Internet numbering resources (Ipv4, Ipv6), Autonomous Numbers and Reverse Resolution in Latin America and the Caribbean, within the framework of the specific goals established by the LACNIC mission aimed at achieving the constant strengthening of a secure, stable, open and continuously growing internet."[81]

[79] FEBRABAN, https://portal.febraban.org.br/paginas/10/pt-br/# (last accessed Nov. 27, 2024).
[80] LACNIC, https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic (last accessed Oct. 28, 2024).
[81] CSIRT LACNIC, https://csirt.lacnic.net/acerca (last accessed Oct. 28, 2024).

Conclusion

The fragmented nature of information-sharing initiatives in Latin America highlights the urgent need for a centralized regional ISAC to address ongoing cyber threats. Given LATAM's vulnerability to cyber-attacks, a regional ISAC would provide a tremendous opportunity to strengthen LATAM's cyber resilience and digital literacy and enable collaboration with existing ISACs and international partners. Currently, most countries in the region rely on mutual aid and assistance from international partners when responding to cyber threats. Moreover, incident response throughout LATAM varies, with some countries having more advanced response mechanisms than others. Creating a LATAM ISAC would help streamline incident response in the region by creating a trustworthy, secure network for peers that can share up-to-date information on threats identified, best practices, and other relevant information. Eventually, the ISAC would also elevate the general cybersecurity knowledge of the LATAM public.

ISACs have demonstrated their effectiveness globally, with the best-equipped countries being those that participate in such initiatives. A LATAM ISAC would reduce reliance on external allies, such as the US and EU, by strengthening local incident-response capabilities. The desire for such an initiative already exists, with preliminary information-sharing efforts underway. Existing CSIRT networks and collaborations with mature ISACs can serve as valuable models for establishing a LATAM ISAC, integrating stakeholders from industry and academia to ensure the comprehensive visibility of threat information.

To maximize its effectiveness, LATAM must thoughtfully consider the different structure and governance models of an ISAC. Due to varying maturity levels, a hybrid approach may work best for the region. LATAM could begin with a sector-based model for the most advanced sectors (e.g., finance) while also expanding existing country-based initiatives. LATAM-based organizations already engaged in ISACs located in the US or EU should leverage their expertise to guide the development of ISACs in LATAM. These organizations can play a pivotal role in fostering collaboration, knowledge sharing, and capacity building as new, region-specific ISACs are established. LATAM-specific ISACs would be able to provide unique regional analysis and insights, addressing threats, vulnerabilities, and trends specific to the region's digital landscape that may not be fully captured by global or non-regional ISACs. This localized focus would allow for more targeted threat-intelligence analysis and better-tailored incident-response strategies. Building personal relationships will be essential to establish trust among participants, and adequate resources must be allocated to ensure that roles and responsibilities are clearly defined, enabling the group to produce meaningful analysis.

ISACs exist globally and have a track record of being effective in increasing cybersecurity resilience. An ISAC integrates all relevant stakeholders and can help bridge the maturity gaps that exist between so many LATAM nations. Efforts aimed at enhancing information sharing are already ongoing in the region but will need to be nurtured with additional resources and expanded to incorporate all relevant stakeholders. Given the state of wide maturity gaps in LATAM's cybersecurity policy, digital training, and education, ISACs stand to benefit the region. Specifically, they can provide access to lessons learned and actionable threat intelligence for less mature entities as well as raising the collective resilience of the region in the face of rigorous cyber threats.

DIGI AMERICAS ALLIANCE MEMBERS

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

kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity

Santander Schneider Electric Telefónica tenable Trellix TREND MICRO

DIGI AMERICAS