2023

Evolution of Cybersecurity

Latin America and the Caribbean

Secure Horizons in the Digital Ecosystem

LAC4

Latin America and
Caribbean Cyber
Competence Centre

LAC4
Latin America and Caribbean Cyber Competence Centre

Content

SUMMARY

The region is undergoing rapid technological advancement that is changing the way we do things. As more countries embrace digital technology, it is crucial to ensure that we are safeguarding our online space through the identification and treatment of threats, known as cybersecurity.

This technological advancement has brought both opportunities and challenges. On one hand, it has created new opportunities for economic growth, innovation, and social development. On the other hand, it has exposed organizations to new online risks.

In this report, we will explore how cybersecurity has evolved in Latin America and the Caribbean, from its beginnings to the current situation. We will analyze how cyber defenses are strengthening and how digital inclusion and economic resilience are being promoted.

The region is unique due to its cultural and economic diversity, making it particularly challenging in terms of cybersecurity. As countries work to create a secure digital environment, they must address issues ranging from lack of internet access to increasingly sophisticated cyber threats.

In this analysis, we will delve into the challenges and opportunities facing governments, businesses, and society as a whole in terms of cybersecurity. We will also examine how regional and international cooperation, policies and regulations, and education play a crucial role in strengthening our digital resilience.

The goal of this analysis is to shed light on the complexity of cybersecurity in the region and underscore the importance of ensuring a secure digital environment to fully harness the potential of our connected society while safeguarding our online future.

CYBERSECURITY OVERVIEW IN LATIN AMERICA AND THE CARIBBEAN

Cybersecurity is one of the most strategically significant risks facing the world today. Next-generation technologies have the potential to introduce new cyber risks, some of which may lead to significant consequences, some known, and others we can't currently imagine.

In Latin America and the Caribbean, there is a clear need for urgent collective action, as well as political intervention and efforts to improve the accountability of governments and businesses.

The rapid and disruptive technological advancements in the region, driven by the social dynamics of the Fourth Industrial Revolution, call for a reevaluation of cybersecurity and collective efforts to address regional needs. Without these interventions, it will be challenging to maintain the integrity and trust in emerging technologies that are crucial for global future growth.

In Latin America and the Caribbean, cybersecurity is at a critical juncture, driven by the exponential growth and development of digital transformation, with the focal point being the aftermath of the COVID-19 pandemic, crisis that brought both opportunities and new challenges to the region.

During this global crisis and uncertainty, cybercriminals exploited human vulnerabilities to breach systemic defenses. Throughout the pandemic, we witnessed how individuals made mistakes they wouldn't have made under normal circumstances. Inadvertently risky online behavior, such as spending more time online, clicking on the wrong link, or expanding browsing habits, can be extremely dangerous and costly. In this regard, detection or exploration alone is not sufficient for ensuring protection; prevention is the key to greater security.

It is essential to maintain the underlying digital infrastructure of our social fabric. However, in Latin America and the Caribbean, as in the rest of the world, there is a risk of exposing digital divides in terms of cybersecurity, where the cost of essential security capabilities, competencies, and services exceeds the purchasing power of their users. This also applies to crucial services for other dependents.

Recent estimates indicate that the vast majority of cyberattacks, approximately 98%, employ social engineering methods. Cybercriminals are highly creative when it comes to devising new ways to exploit users and technology to gain access to passwords, networks, and data, often leveraging popular topics and trends to entice users to adopt unsafe online behaviors.

Undoubtedly, in Latin America and the Caribbean, in today's digital world, we are becoming increasingly dependent on digital services, infrastructure, and the need for more reliable information, often overlooking the importance of cybersecurity. While a significant portion of society saw the arrival of the COVID-19 pandemic as a moment for collective action, cybercriminals, taking advantage of the crisis, launched malicious strategies across the region. Ultimately, they leveraged this context to spread cyber threats such as malware or malicious code, as well as fraudulent websites that preyed on users' vulnerabilities with the intent to deceive and defraud others.

In less than a decade, cybersecurity has become one of the most critical systemic issues for the global digital economy. Collective spending has reached $145 billion per year, and it is projected to exceed a trillion dollars between 2017 and 2021. Undoubtedly, incidents and cyberattacks continue to rise, marking just the beginning of a new and growing challenge.

It's essential to note that Information and Communication Technologies (ICT) are the driving force behind the evolution of modern societies, and cybersecurity is a vital component for sustaining a technologically robust and trustworthy model. Events like power supply disruptions or interference in ICT networks leading to financial system deterioration are a reality in most countries in the region, constituting a threat to the national security of each country within the region. Cybercriminals are numerous and highly organized, coming from diverse backgrounds, including political, economic, criminal, terrorist, and hacktivist. Therefore, information security focuses on three primary objectives: availability, confidentiality, and integrity.

In 2015, the United Nations (UN) defined seventeen Sustainable Development Goals (SDGs) to be achieved by 2030, ranging from eradicating poverty and ensuring stability and peace to combating discrimination and climate change. Digital technologies, particularly the Internet of Things (IoT) and Artificial Intelligence (AI), facilitate the achievement of these SDGs and go hand in hand with cybersecurity, which plays a crucial role. As an example, AI can help detect malnutrition using photographs of people living in a specific area. However, if these photographs were stolen or the AI model becomes corrupted, using AI to combat hunger would become problematic. Cybersecurity is the foundation of trust and, therefore, the adoption of digital technologies for humanitarian and environmental purposes.

According to recent reports from Fortinet's Intelligence Analysis Laboratory, Latin America and the Caribbean experienced over 360 billion attempted cyberattacks in 2022, with Mexico receiving the highest number of attack attempts (187 billion), followed by Brazil (103 billion), Colombia (20 billion), and Peru (15 billion).

According to recent reports and statistics provided by countries in the region, the Global Cybersecurity Index of the International Telecommunication Union indicates that 28 countries in the region have not offered incentives to improve private cybersecurity, and 17 countries lack a national cybersecurity strategy to address critical infrastructure. These indices reflect and highlight the significant regional disparities. While Brazil is the highest-ranked country in the region, at 18th place globally, Honduras is at the bottom, ranked 178th out of 193 countries.

Cybersecurity as a New Domain

The deep connection and advances in disruptive and emerging digital transformation and innovation through Information and Communication Technologies (ICT), due to globalization, have led economic, commercial, strategic, social, and governmental activities and interactions at all levels, including individuals and other socio-productive development sectors, to be conducted in cyberspace.

Maintaining a secure digital ecosystem in a landscape of constantly evolving threats is a challenge for all organizations. Traditional reactive approaches, where resources are allocated to protect systems against the most well-known threats while lesser-known threats are undefined and unmapped, are no longer sufficient and effective. To stay up-to-date with changing security risks, a more proactive and adaptive approach focused on the constant management of cyber risk is needed.

According to the National Institute of Standards and Technology (NIST), cybersecurity is the prevention of damage, protection, and restoration of computers, electronic communication systems, electronic communication services, cable communications, and electronic communications, including the information contained therein, to ensure their availability, integrity, authentication, confidentiality, and non-repudiation. This involves a combination of people, policies, processes, information, and technologies.

On the other hand, it states that Information Security is the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction, with the aim of providing confidentiality, integrity, and availability.

Furthermore, it defines cyberspace as a global domain within the information environment consisting of the interdependent network of information system infrastructures, including the Internet, telecommunications networks, computer systems, and integrated processors and controllers.

Clearly, robust systems engineering has both a direct and indirect impact on information societies. It enables critical and essential national infrastructures and services to function, allows citizens to carry out their daily routines, and can promote socially beneficial outcomes of digital technologies.

For these reasons, cybersecurity should not be framed and managed as an exclusive or separate good but rather as a public good, that is, a non-rival good that is also non-excludable (meaning that no user can prevent others from using it).

The importance of Cybersecurity in the Region

Cybersecurity as a public policy is essential to protect the rights of citizens in the digital sphere. It involves safeguarding the privacy of personal data and the intellectual property of algorithms, software, platforms, and systems, increasing public trust in digital technology, and ensuring secure access to the digital ecosystem. Underestimating the importance of cybersecurity in these times exposes one to significant risks.

In the region, the challenge of cybersecurity weighs heavily on organizations of all sizes. Across the spectrum, they regularly contend with incidents such as breaches, data leaks, advanced persistent threats, and ransomware attacks. The substantial costs affect those unfortunate enough to be targeted, and the attacks can be devastating. Moreover, cybersecurity attacks are ruthlessly agnostic. Cybercriminals do not care about the size of an organization and target anyone, from large and medium-sized enterprises to the smallest shops, using the same techniques as those directed at major corporations. Cybercriminals also do not discriminate based on the type of product or service being sold.

Regional dialogues and cooperation in cybersecurity are still in their infancy and fragmented. The most prominent regional has been the Organization of American States (OAS). For over a decade, the OAS has conducted cyber simulations, participated in capacity-building, and supported the development of cybersecurity national strategies of member states. Additionally, OAS member states established a Working Group on Confidence-Building Measures in 2017 focusing on ensuring cooperation, transparency, predictability, and stability among cyber-space states.

Other regional forums have caught up on cybersecurity issues as well. Since 2020, the Economic Commission for Latin America and the Caribbean (ECLAC), for example, has been seeking to further integrate the development agenda with cybersecurity as part of its Digital Agenda for Latin America and the Caribbean (eLAC). The 2022 edition of eLAC emphasized that countries should promote regional harmonization of cybersecurity policies and norms, while the 2024 edition highlighted the need for states to promote cybersecurity policies consistent with human rights and set the goal of having 20 countries (out of 33 in the region) with national cybersecurity strategies by 2024.

While the developments point towards a gradual recognition of the importance of cybersecurity within the region, it is still too early to consider what a regional agenda for this topic would look like. Since cybersecurity is not necessarily a partisan agenda, changes, divisions, as well as diplomatic conflicts, may not directly impact discussions on cybersecurity. This means that there would be little resistance to maintaining cybersecurity as an agenda for technical cooperation or expanding it to new levels depending on the regional appetite.

Challenges and Threats in Cybersecurity

Cybersecurity Landscape

According to a recent cybersecurity report by Fortinet, there were 137 billion cyberattack attempts in Latin America during the first half of 2022 . The primary type of cyberattack was ransomware attempts, which aim to encrypt an organization's information and block access to the system until a ransom is paid. These attempts doubled compared to 2021. The report identifies Mexico as the country with the most cyberattacks in the region, followed by Brazil and Colombia. This increase is not only in terms of quantity, but also sophistication. New variants of this malicious program have been created, as well as "ransomware as a service" (RaaS), where developers sell or distribute ransomware to third parties (usually on the dark web) in exchange for a percentage of the profits.

Additionally, the 2022 report by the cybersecurity software company ESET named Peru, Mexico, Colombia, Argentina, and Ecuador as the Latin American countries where the most malicious attacks were detected.

It can be said that 2022 was a critical year for information security for both public and private Latin American companies, not only due to the increase in the number of attacks but also their level of sophistication. Unlike Europe (with its General Data Protection Regulation or GDPR), data protection laws in Latin America are established by each country and are mostly outdated and designed for reaction rather than prevention. This, along with impunity and the lack of strong state agencies or bodies dedicated to cybersecurity, makes it easier for cybercriminals to carry out illegal activities without significant penalties, making Latin America a preferred target for cyber attackers.

Prevention is the first line of defense against cyberattacks, although this is not a common practice in much of Latin America. Cyberattack attempt statistics reveal that, for the most part, small and medium-sized enterprises lack security measures on their employees' mobile devices, and this is precisely where many cyberattacks begin.

Given this perspective, companies must take cybersecurity seriously, focusing on prevention through protection and reaction. Organizations should not only invest in technological tools to monitor and control threats but also constantly train their employees on how not to fall victim to attacks by malicious actors who exploit users' lack of knowledge to extract information that could be used for cyberattacks.

It is not expected that small or medium-sized enterprises allocate all their efforts to cybersecurity, which is often unrealistic as many businesses do not have sufficient time or resources. Therefore, it is recommended that companies use third-party providers specializing in cybersecurity services, including consulting, implementation, integration, maintenance, and managed services. Such organizations are growing in Latin America, and their assistance is highly valued due to their expertise and professionalism. Additionally, acquiring insurance in case of cyber incidents can help prevent the bankruptcy of any company, as the cost of cybercrime is immensely high and challenging to determine with precision.

The Kaspersky Report identified ransomware, as well as viruses and trojans downloaded from the internet, as a constant threat with over 2 million detections per year. Phishing (i.e., fraudulent messages sent via email, SMS, and, especially, through social networks and messaging apps like WhatsApp) seems to be a persistent infection vector, with an average of around 10,000 daily detections.[1]

1 https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

On the other hand, in a report published by Kaspersky, Brazil stands out as the market with the most malware attacks, with 1,554 attempts per minute, followed by Mexico (298 attempts per minute), Peru (123 attempts per minute), and Colombia and Ecuador with 84 each.

Latin America and the Caribbean continue to face significant challenges, according to a 2020 study by the Inter-American Development Bank (IDB) and the Organization of American States (OAS). Many countries in the region still have ad hoc cybersecurity activities and initiatives without a strategic vision. Only 13 countries have national cybersecurity strategies, and only 9 have critical infrastructure protection plans.

According to several international cybersecurity firms, Latin America and the Caribbean is one of the regions with the highest incidence of cyberattacks in the world, with more than 1,600 cyberattacks per second. This can be seen in the fact that during the first half of 2022, the global distribution of ransomware attacks reached 384,000, representing 14% of the total for the region

The financial sector is an important infrastructure in the region. Recent advances in digitization have made this area one of the most relevant in terms of cybersecurity. Figures show a significant increase in the number of financial transactions through digital means in the region since the start of the COVID-19 pandemic.

It is estimated that the region's financial sector invests 10% of its technology budget in this important area. As the sector becomes more digitized, greater investment may be required.

Furthermore, a significant part of the challenge lies in the integration and formalization of CSIRTs (Computer Emergency Response Teams), national and international cooperation mechanisms, formal education, and cybersecurity measures so that the financial sector can mitigate the risks associated with increasingly digital and consumer-centric businesses.

Critical Infrastructures

Furthermore, some entities in Latin America and the Caribbean have already experienced a cyberattack on their water and sanitation infrastructure that affected their operations, although recovery was achieved quickly. However, an entity's ability to classify an operational event as a cyber incident depends largely on its digital infrastructure, forensic capabilities, and cyber awareness.

In recent years, several countries in the region have updated their regulatory frameworks for cybersecurity, thanks to increased awareness of the growing importance of this issue, especially concerning critical infrastructure systems. However, legislative efforts at the national and subnational levels in many countries in the region have not yet translated into consistent implementation of cybersecurity strategies and action plans. While improvements have been made in this regard, activities in this area should be accelerated further. Therefore, there is a need to prioritize the consistent implementation of cybersecurity strategies and action plans, with a focus on critical infrastructure.

Healthcare Sector

Cybersecurity in the healthcare sector is particularly relevant due to the sensitivity of the information it handles. The technologies that support Electronic Health Records (EHR), telemedicine, and other advanced medical devices are critical systems and have unfortunately fallen victim to multiple attacks in recent years. Personal Health Information (PHI) is the most valuable data on black markets, with values tens of times higher than, for example, credit card numbers.

Several countries in the region already have Electronic Health Records (EHR), with ten countries having legislation that defines and validates electronic health records, Other countries are making progress in their regulatory frameworks for implementation, considering patient data protection, secondary use of information, actions of healthcare professionals, the role of patients in relation to their health data, and health interoperability standards.

Cyberattacks are also on the rise in the region. In Brazil, the average cost of cyberattacks increased by 10.5% between 2019 and 2020. It's important to note that 80% of compromised information consists of personal data, which is why the healthcare sector takes the longest to detect data breaches. On average, it takes 329 days after a successful attack to detect a data breach. In fact, our region has one of the highest attack detection times in the world. The region has witnessed several incidents in recent years, such as data leaks involving sensitive information in Mexico, Chile, Argentina, and other countries.

Another relevant point observed internationally is the growing use of new technologies in the industry, especially the Internet of Medical Things (IoMT). This poses new challenges and risks for the field that can impact the security of people receiving medical care and treatment. The penetration of IoMT in Latin America and the Caribbean is considered low, but it is expected to change in the coming years, and the field must prepare for new challenges.

REGULATORY FRAMEWORK AND CYBERSECURITY POLICIES IN LATIN AMERICA AND THE CARIBBEAN

Existing Legislation and Regulations

Cybercrime Convention

The Budapest Convention is a global treaty aimed at addressing cybercrimes and promoting international cooperation in investigating and prosecuting criminal activities. Despite its origins in Europe and the signing of European nations, the principles and purposes of the Convention have become known and used in various regions of the world, including Latin America and the Caribbean.

Latin American signatories to the Budapest Convention include Argentina, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Ecuador, Panama, Paraguay, and Peru. These countries demonstrate and reaffirm their commitment to addressing cybercrime globally by creating legal frameworks that adhere to the provisions established by the Convention. Because cybercriminals operate globally, it is imperative to collaborate with other countries to address global cyber threats and ensure effective prosecutions.

In the region, the adoption of the Budapest Convention underscores the need for more comprehensive efforts against cybercrime. The treaty provides an environment for nations in the area to harmonize their legal codes, enhance their law enforcement capabilities, and facilitate collaboration with other signatories.

Currently, there is a growing recognition in the region of the need for comprehensive and standardized strategies to combat cybercrime, which is driving the adoption of new regulations similar to this one. This convention establishes a foundation upon which states in the region can enact their laws, strengthen law enforcement and criminal justice systems, respectively, and promote closer cooperation with other signatories. This convention is a crucial initiative to promote cybersecurity and the rule of law in the Americas, with the goal of enhancing online security for both society and organizations.

The second additional protocol to the Convention on Cybercrime (Budapest Convention) was adopted on November 23, 2021, and entered into force on January 1, 2023. The protocol aims to strengthen cooperation and the disclosure of electronic evidence in criminal cases related to cybercrime.

Countries in the region that have signed the protocol include Argentina, Chile, Colombia, Costa Rica and Dominican Republic.

Institutions and Agencies Responsible for Cybersecurity

Given the widespread concern that governments may increase their support or direct involvement in disruptive cyber operations due to the expanding threat landscape, cybersecurity defenses are also increasing in scope and sophistication. This is why institutionalization as an enabler of cyber governance is crucial.

We can define cyber governance as a comprehensive cybersecurity strategy that integrates with an organization's operations and prevents the disruption of activities due to cyber threats or attacks. Cybersecurity governance features include accountability, decision-making, risk management, plans, strategies, as well as processes and procedures that enable institutional effectiveness.

Cybersecurity Incident Response Teams (CSIRTs) can make a difference in the coordinated and efficient response to an attack, thereby helping to mitigate its consequences.

CSIRTs provide cybersecurity services to prevent, detect, mitigate, and respond to cyber incidents within a defined community. They have an organizational structure with established processes and a catalog of technological tools, along with a budget, mandates, service catalog, specialized personnel, a network of contacts, communication plans, an enabling legal framework that allows them to act, and many other elements that form the basis for managing cyber incidents in a defined served community, as well as supporting that community in the best possible way.

Currently, there is an increase in CSIRTs in various sectors in the region, including the military, government, healthcare, and banking, among others. While there are similarities, there are also differences. In some cases, they have been established as part of a National Cybersecurity Strategy, while in others, they have arisen from bills or ministerial or presidential decrees or public policy issuance. However, the structure depends on the dynamics of each country, government, economy, legal organizational structure, and political and sociocultural context in which they operate.

Country	CSIRT	Type
Argentina	CSIRT-MINSEG CSIRT-PBA BA-CSIRT CERT-UNLP CSIRT-NQN CERT.ar	Government Government Government Government Government National
Barbados	CIRT-BB	National
Bolivia	CSIRT-Bolivia	National
Brazil	CTIR Gov	National
Chile	CSIRT-CL	Government
Colombia	COCIB CSIRT-MDN CSIRT-EJC CSIRT-CCOCI ColCERT DICAE CSIRT-PONAL	Military Government Military Military National Military Military
Costa Rica	CSIRT-CR	National
Ecuador	COCIBER EcuCERT	Military National
Guatemala	CRIC_GT CSIRT-GT	Military National I
Guyana	CIRT.GY	National
Jamaica	Ja-CIRT	National
Mexico	CSIRT-SEDENA-MX CSIRT-SEMAR-MX CERT-MX	Military Military National

Country	CSIRT	Type
Panama	CSIRT-Panamá	National
Paraguay	CERT-PY	National
Peru	CITELE_EP CSIRT-MGP CSTPERU CSIRT-PE	Military Military Military National
Dominican Republic	CSIRT-Defensa CSIRT-RD SPRICS	Government National National
Suriname	SurCSIRT	National
Trinidad and Tobago	TTCSIRT	National
Uruguay	CERTuy DCSIRT-UY	National Military

The differentiating element of these CSIRTs is the trust they generate within the organizations that are part of the serviced community. The institutions to which they provide services should not fear reporting an incident or seeking support, especially in times of crisis because a CSIRT is an entity that primarily offers support, recommendations, and mentorship but does not impose, judge, or regulate.

To understand the personnel landscape, the current average number of people working in a public CSIRT in the region is six, of which:

These centers in the region are exposed to a high turnover rate resulting from the knowledge acquired in the CSIRT and the private sector's interest in recruiting qualified personnel to face cybersecurity challenges.

The establishment of CSIRTs in the region without a fixed and ongoing budget allocation is an obstacle to establishing compensation packages commensurate with the high performance required of operational personnel, thereby hindering talent retention and operational sustainability.

It is worth noting that these centers in the region have played a very important role, including their participation in electoral processes, national and regional sports events, intersectoral exercises, the design of national cybersecurity strategies, situations of escalating social conflicts, national and regional summits, academic coordination, as well as the coordination of public-private initiatives.

National Cybersecurity Policies and Strategies

The articulation of public policies and cybersecurity strategies has evolved in the region due to the growing digitization of societies and economies, as well as the risks and threats.

Currently, some countries in the region have established or are in the process of creating national cybersecurity plans and strategies. These strategies aim to improve the resilience of critical infrastructure, strengthen legal frameworks, enhance incident response capabilities, and educate citizens and organizations about cybersecurity.

It is evident that collaborative efforts in the field of cybersecurity have been recognized as a key area for countries in the region. Various international organizations, including the OAS, the European Union, and the IDB, have played a decisive role in promoting cooperation and knowledge exchange among countries in the region. Considering that joint initiatives and regional cybersecurity exercises promote trust-building and the development of collective capabilities in response to cyber threats. These actions reflect a national and comprehensive approach to cybersecurity through cyber diplomacy.

Training and education in cybersecurity are becoming increasingly critical on a regional level, where governments, academia, and industry stakeholders are collaborating to train cybersecurity professionals and raise awareness at all levels of society. These efforts are crucial to address the shortage of trained cybersecurity professionals and foster a security mindset.

Aspect	Country	Year
National Strategy	Mexico	2017
	Guatemala	2018
	Nicaragua	2020
	Costa Rica	2017
	Ecuador	2022
	Panama	2013, 2021
	Belice	2020
	Jamaica	2015
	Dominican Republic	2018, 2022
	Barbados	2023
	Trinidad and Tobago	2012
	Brazil	2020
	Argentina	2019
National Policy	El Salvador	2022
	Colombia	2011,2016,2020
	Chile	2017-2023
National Plan	Paraguay	2017

INFRASTRUCTURE AND CAPABILITIES IN CYBERSECURITY

Technological Infrastructure in the Region

The region has been undergoing a digital transformation, with increased Internet penetration and the adoption of digital technologies in various sectors. While this transformation brings economic benefits, it also introduces cybersecurity challenges. Many governments and organizations in the region are still working to adapt their cybersecurity infrastructure to protect critical infrastructure and confidential data in this evolving digital landscape.

Digital transformation has grown rapidly in recent years in the region, driven by a combination of factors, including technological advancements, internet connectivity, and innovation. Governments, organizations, and society in the region are increasingly adopting technologies to enhance competitiveness, efficiency, and to drive economic growth and development.

The key to this transformation in the region is the expansion of internet access. Efforts to close the digital divide have intensified, with governments and the

private sector investing in the development of infrastructure to bring high-speed internet to previously underserved areas. This expanded connectivity paves the way for greater adoption of digital services and online platforms, changing the way people work, communicate, and access information.

Human Resources and Cybersecurity Training

In the region, the development of human talent has been constantly evolving to meet the growing need for qualified professionals. In recent years, there has been increased awareness of the importance of cybersecurity due to the growing frequency and sophistication of cyber threats in the region. As a result, various educational institutions, government agencies, and private organizations have taken steps to improve training programs and promote cybersecurity awareness.

Human Talent and Workforce

The modern cybersecurity landscape has galvanized passion and persistence within its workforce, which continues to change and evolve with the surrounding world. It is estimated that there are currently more than 3.1 million unfilled cybersecurity vacancies worldwide, with over 520,000 of them located in Latin America and the Caribbean.

According to the OAS in its 2022 Cybersecurity Workforce Report for Latin America and the Caribbean there is a significant issue of cybersecurity job vacancies because it is challenging to find the right talent. To address this problem, educational institutions in the region are creating new cybersecurity programs and courses. Additionally, organizations that provide education, training, and certification, as well as technology companies, are enhancing their offerings to better equip cybersecurity professionals.

Despite these efforts, the shortage of cybersecurity skills in the region is causing severe issues in the job market, and this problem is expected to persist in the near future. To strengthen our defenses against cyber threats, it is crucial to cultivate a more diverse cybersecurity workforce with both technical and non-technical skills. Promoting greater gender diversity in this field is also important for its growth and maturity. The top priority is aligning what educational institutions teach with the actual needs of the job market to bridge the cybersecurity skills gap.

It is pointed out that in the region, there is a lack of standardization efforts regarding cybersecurity, especially in terms of how cybersecurity roles are defined and described and the associated skills for these roles, as well as how the workforce is trained. The absence of unified standards for knowledge, competence, and skills that students should develop to meet the needs, and that organizations should consider when creating talent search profiles, can result in inefficiencies in the cybersecurity job market, impacting the interaction between sellers and consumers in this market.

However, in the region, there is not enough educational supply to generate adequate competencies and capabilities in cybersecurity. The demand for cybersecurity education by post-secondary students is not increasing rapidly enough. Furthermore, the demand for cybersecurity skills in the industry sectors also makes it difficult for academia to attract academics, researchers, and professors with knowledge, practical experience, research backgrounds, and academic aspirations. There are also difficulties in attracting and retaining qualified cybersecurity professors, mainly because such high-quality professionals demand above-average salaries. Tertiary education providers must ensure that cybersecurity is considered a desirable study option to attract the best and most motivated students.

Ciberlac Network

The Latin America and Caribbean Cybersecurity Excellence Network (Ciberlac Network) is a regional network of universities and research centers in the field of cybersecurity. The IDB acts as the driving and coordinating institution of the network.

The Ciberlac facilitates collaboration and the exchange of knowledge, experiences, and resources among the member institutions, promoting the creation of synergies to enhance their educational and research capabilities. With the mission of contributing to reducing the shortage of cybersecurity professionals in both the industry and academia and enhancing the level of preparedness in this field in the countries of the region by fostering the development of human capital, research, and innovation.

Country	Academy
Argentina	Buenos Aires' University
	National University of La Plata
Chile	University of Chile
Colombia	Higher War School "General Rafael Reyes Prieto"
	Pontifical Javeriana University
	Northern University
Costa Rica	Costa Rica Technological Institute
	Latin University of Costa Rica
Ecuador	Catholic University of Cuenca
	International University of Ecuador
	North Technical University
Mexico	National Polytechnic Institute
	Monterrey Tech
	Metropolitan Autonomous University
	University of Guadalajara
	National Autonomous University of Mexico
Panama	Tecnology University of Panama
Paraguay	National University of Caaguazú
Peru	Continental University
	National University of San Agustín
	Pontifical Catholic University of Peru
Dominican Republic	Caribbean University
Uruguay	University of the Republic
	Technological University
Strategic allies	Brazilian National Academic Network

Collaboration and Regional Cooperation in Cybersecurity

The digital age has brought the Latin America and the Caribbean region unprecedented opportunities in terms of connectivity, digital economy, and technological advancements. However, with this progress, significant challenges have also emerged, especially in the field of cybersecurity.

Cyberspace knows no physical borders. Threats, such as ransomware and phishing attacks, can originate in one country and simultaneously affect multiple nations. For this reason, it has been essential for LAC countries to cooperate and share real-time information to effectively identify and combat these threats.

Cybersecurity is a constantly evolving domain. Threats emerge rapidly, and today's solutions may not be effective tomorrow. Cooperation has allowed countries to share alerts, identified vulnerabilities, and best practices through existing regional cooperation networks like the Organization of American States (OAS) CSIRTAmericas and the Forum of Incident Response and Security Teams (FIRST), providing everyone with a better opportunity to prepare and respond.

Many countries in the LAC region have limited resources. Cooperation has facilitated the sharing of open-source technologies, tools developed by other teams, and cybersecurity experts, enabling each country to leverage available resources in the region more effectively.

Differences in cybersecurity laws and policies can create gaps that cybercriminals exploit. Regional cooperation leads to the harmonization of laws and regulations, making it easier to prosecute and sanction cybercrimes.

International cooperation in the region has manifested in joint training programs, expert exchanges, and simulation exercises through capacity-building organizations and programs such as LAC4, Cyber4Dev, and EU Cybernet, ensuring that professionals stay updated with the best strategies and tactics.

A secure cyber environment can be attractive to investments and businesses looking to operate in a reliable environment. Cooperation not only strengthens security but can also act as a catalyst for economic development.

One of the most prominent examples of regional collaboration in cybersecurity is the European Union's Cybersecurity Strategy. This strategy promotes cooperation among EU member states in combating cyber threats, including the establishment of the European Union Agency for Cybersecurity (ENISA) and the European Union Computer Emergency Response Team (CERT-EU).

Another example is the Asia-Pacific Economic Cooperation (APEC), which has established an Expert Working Group on Cybersecurity (EWG-C) to promote cooperation and information exchange among member economies and address common cyber threats. APEC has also developed a Cyber Incident Response Framework (CIF) that provides guidance on how to respond to cyber incidents.

The region has also been part of the initiatives and actions carried out by the Global Forum for Cyber Expertise (GFCE); an initiative created by The Netherlands in 2015 during the Global Cyberspace Conference .

The GFCE is a multi-stakeholder network consisting of more than 180 members and partners from governments, international organizations, industry, non-governmental organizations, academic institutions, technical groups, and civil society with the purpose of strengthening international development cooperation of cyber capabilities by connecting needs, resources and expertise and making practical knowledge available to the global community.

Member countries and organizations in the region that are actually part of GFCE are: Argentina, Chile, Canada, Chile, Colombia, Curacao, Dominica, Dominican Republic, Ecuador, Guatemala, Mexico, Peru, Surinam, Uruguay, United States of America, Organization of American States (OAS), The International Telecommunication Union (ITU) and the Latin America and the Caribbean Cyber Competence Centre (LAC4).

Cyberdiplomacy as a cross-cutting axis for regional and global cooperation and harmonization

Cyberdiplomacy has been adopted as the application of diplomacy to geopolitical issues arising in cyberspace. Cyberdiplomacy in the Latin America and the Caribbean region has had asymmetric development, with different levels, approaches, and speeds. Some cyberdiplomacy training initiatives have been driven, among others, by the Latin American and Caribbean Economic System (SELA), the Organization of American States (OAS) through the Inter-American Committee against Terrorism (CICTE), and the European Union through the EU Cybernet project and its Latin America and Caribbean Cyber Competence Centre (LAC4).

The development of cyberdiplomacy in the region brings several benefits, such as facilitating communication among diplomatic actors, strengthening cyber resilience and trust among countries through cooperation and dialogue on cybersecurity, cyber defense, and cybercrime issues, and preventing conflicts arising from cyber incidents. It also aims to protect human rights and fundamental freedoms in cyberspace, promoting multilateralism and global governance.

The Open-Ended Working Group (OEWG) of the United Nations has been a mechanism for promoting dialogue and cooperation on matters related to security and stability in cyberspace. The second OEWG was established in 2021 (the first one was from 2019 to 2021) and has held several sessions and consultations with UN member states and other interested parties. The current OEWG process is expected to conclude in 2025 with the adoption of a final report containing recommendations on norms, principles, confidence-building measures, and international cooperation in cybersecurity.

The participation of the Latin American and Caribbean region in the OEWG (GTCA) has been active and constructive, contributing its perspectives and experiences on the challenges and opportunities presented by cyberspace. Some countries in the region, such as Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Uruguay, and Dominican Republic, have submitted their written contributions to the OEWG and have participated in the group's in-person and virtual meetings. Additionally, some regional organizations, such as the Economic Commission for Latin America and the Caribbean (ECLAC) or the Economic System for Latin America and the Caribbean (SELA),

have organized parallel events to the OEWG to discuss topics of interest to the region.

The final report of the 2021 OEWG contains several recommendations on the topics addressed by the group, such as:

- Recognizing and reaffirming the application of international law, including the United Nations Charter, to cyberspace.
- Respecting and promoting human rights and fundamental freedoms in cyberspace, as well as digital inclusion and cooperation for development.
- Adopting and applying voluntary, non-binding, action-oriented norms for responsible state behavior in cyberspace, based on norms agreed upon by the Governmental Group of Experts (GGE).
- Developing and implementing confidence-building measures among states to reduce the risks of misunderstandings, escalations, and conflicts in cyberspace.
- Establishing and strengthening international cooperation mechanisms to prevent, respond to, and mitigate cyber incidents, as well as to assist states affected by malicious activities in cyberspace.
- Enhancing national and regional capacities in cybersecurity, cyber defense, and cybercrime through the exchange of best practices, technical assistance, and training.

In the context of cyberdiplomacy, initiatives are also being developed to combat cybercrime through the process of drafting a convention against cybercrime within the United Nations, initiated in 2020 when the General Assembly adopted resolution 74/247, establishing an Ad-Hoc Special Committee to develop a legally binding international instrument on combating cybercrime.

The aim of the AHC is to draft a convention that addresses the challenges posed by cybercrime, such as the lack of legislative harmonization, insufficient international cooperation, human rights protection, and capacity building. The AHC builds on previous work conducted by the Intergovernmental Expert Group on Cybercrime (IEG-Cybercrime), established in 2018, which presented its final report in 2020 with recommendations on the principles and essential elements for a convention on cybercrime.

The AHC also considers the Council of Europe Convention on Cybercrime (Budapest Convention). However, the AHC aims to draft a more universal convention adapted to the new challenges and opportunities presented by cyberspace.

Some of the main challenges in drafting a convention against cybercrime have been:

- The lack of a common and agreed-upon definition of what constitutes cybercrime and which behaviors should be criminalized.
- The diversity of legal systems and national legislations that regulate the use of information and communication technologies (ICT) and the prosecution of cybercrimes.
- The need to ensure respect for human rights, civil liberties, due process guarantees, and the right to privacy of individuals using cyberspace or who are victims of cybercrime.
- The difficulty of establishing effective mechanisms for international cooperation among states and with other relevant actors, such as internet service providers, to prevent, investigate, and penalize cybercrime, especially when it has a transnational character.

Furthermore, countries in Latin America and the Caribbean have participated in the sessions of the Open-Ended Working Group of Governmental Experts (AHC), which aims to draft a legally binding international instrument on cybercrime to strengthen domestic legal frameworks and enhance the effectiveness of cooperation and the exchange of digital evidence. The AHC receives technical assistance from the United Nations Office on Drugs and Crime (UNODC), which has organized regional and subregional meetings to facilitate the exchange of experiences and best practices among states.

International Initiative Against Ransomware

Following the joint statement by the United States White House on the International Ransomware Initiative in 2022, Brazil, Dominican Republic, and Mexico, reaffirmed their joint commitment to counter all elements of ransomware threats and discussed the next steps. They committed to continue building collective resilience against ransomware, cooperating to disrupt ransomware, pursuing responsible actors, countering illicit finances that support the ransomware ecosystem, and working with the private sector to defend against ransomware attacks.

This commitment urges the use of all appropriate tools of national power to achieve its objectives, where they jointly commit to the following actions in support of this effort:

- Holding ransomware actors accountable for their crimes and not providing them with safe havens.
- Combating the ability of ransomware actors to profit from illicit income through the implementation and enforcement of anti-money laundering and counter-terrorism financing (AML/CFT) measures, including “know your customer” (KYC) rules, for virtual assets and virtual asset service providers.
- Disrupting and bringing to justice ransomware actors and their facilitators, to the fullest extent allowed by each partner’s applicable laws and relevant authorities.
- Collaborating in ransomware disruption by sharing information, when appropriate and in accordance with applicable laws and regulations, about the misuse of infrastructure to launch ransomware attacks to ensure that national cyber infrastructure is not used in ransomware attacks.

This statement emphasizes that diplomatic engagement remains an essential tool in the international community’s fight against ransomware attacks.

Transformative Impact of the OAS in the Region

Through the Organization of American States (OAS), specifically the Inter-American Committee against Terrorism (CICTE), a regional entity dedicated to preventing and combating terrorism in the region, the Cybersecurity Program dedicates regional efforts to: (a) policy development, (b) capacity building (including training and exercises), and (c) research and dissemination.

They have trained over 2,000 women in cyber exercises and over 600 young students in digital security training to enter the cybersecurity field in the region. More than 15,000 citizens and public and private officials have been trained in cyber operations, cybersecurity, diplomacy, cybersecurity leadership, and international cybersecurity regulations.

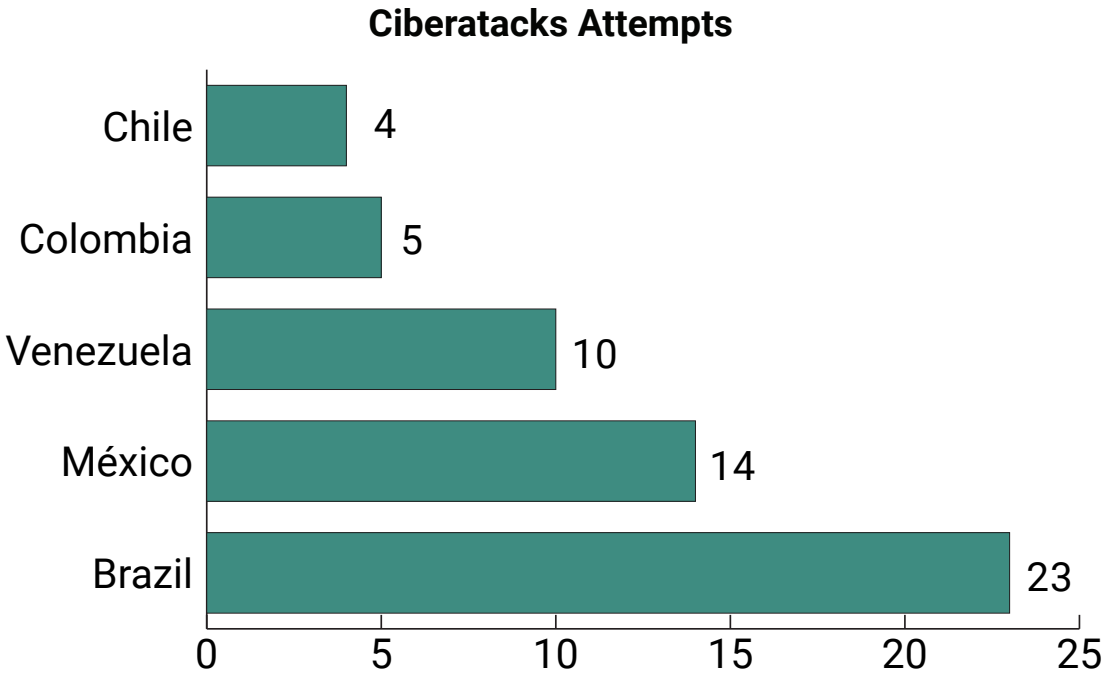
CYBERSECURITY THREATS AND VULNERABILITIES

Types of Cyber Threats and Attacks

Around the world, the Internet and digital media have revolutionized how society, government, and businesses connect, interact, and conduct transactions. This transformation has driven economic growth and social development, fostered innovation, and improved transparency.

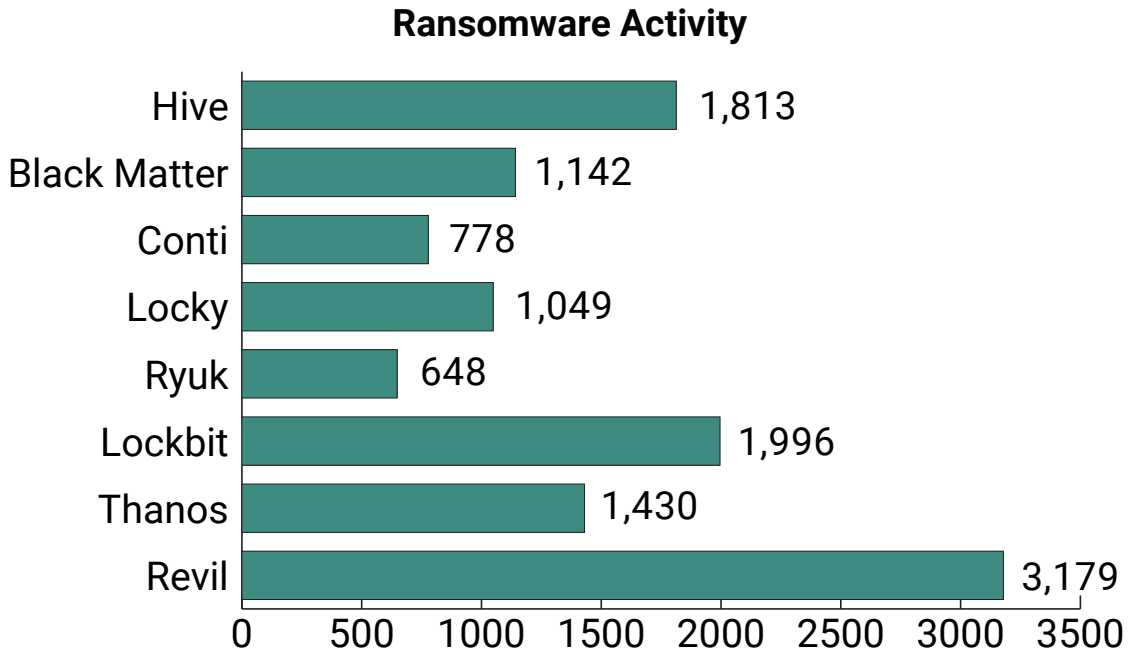
The region has proven to be a very attractive landscape for cybercriminals due to its outdated digital infrastructure, rudimentary policies, and limited resources. While this environment created fertile ground for cybercrime, it has also attracted the interest of those looking to invest in improving cybersecurity. These investors include tech giants like the United States and China, who are currently vying for cybersecurity investments in the region.

According to Fortinet's Global Threat Landscape Report for 2023, it provides a comprehensive overview of the evolving dynamics of cyber threats and their impact on the region. It reveals a staggering figure of 63 billion attempted cyberattacks targeting Latin America and the Caribbean in the first half of 2023, highlighting the urgent need for both governments and organizations to take immediate and effective cybersecurity measures.



The report highlights that only Mexico experienced more than 14 billion attempted cyberattacks. This made Mexico the second most attacked country in the region, following Brazil, which experienced 23 billion attempts. Following them, Venezuela, Colombia, and Chile entered the statistics, dealing with 10 billion, 5 billion, and 4 billion attempted attacks respectively during the first half of the year.

The increasing sophistication of recent cyberattack strategies is enabling more precise attacks, resulting in a decrease in ransomware incident detection. This intriguing development underscores the need for organizations to remain vigilant, as attackers shift their focus to precision over quantity.



Ransomware activity has experienced significant growth, with various malicious actors and international cybercriminal groups targeting businesses across all industries, governments, and even entire economies. There's been a notable increase in the use of Ransomware as a Service (RaaS), where ransomware creators provide it to third parties in exchange for a monthly fee or a percentage of the profits obtained.

During the first half of 2022, 10,666 ransomware signatures were found in the region, compared to only 5,400 detected in the latter half of 2021. Additionally, some ransomware actors offer their victims 24/7 technical support to expedite ransom payment and the restoration of encrypted systems or data.

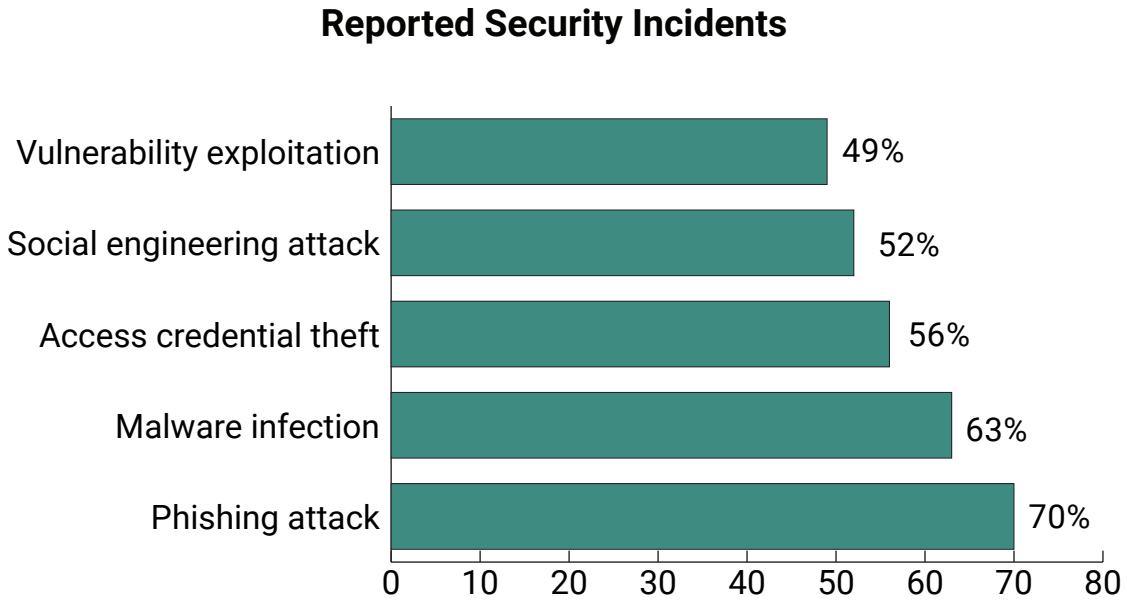
The ransomware market has become highly professionalized, with a well-established business model. Threat actors use independent services to negotiate data ransoms, assist victims in making payments, and mediate disputes among cybercriminal groups. For instance, the WannaCry variant includes a language translator and even a support chat.

The most active ransomware campaigns in the region during the first half of 2022 were Revil, primarily detected in Mexican territory, followed by LockBit and Hive. Conti ransomware, on the other hand, gained significant media attention due to its recent high impact in Costa Rica.

Destructive malware, such as wipers, increased by over 50%, while cybercriminal supply chains grew in complexity and sophistication to counter evolving defenses. The region experienced over 360 billion cyberattack attempts in 2022 ,with 137 billion attempted cyberattacks in the first half of that year.
In addition to the extremely high numbers, the data reveals an increase in the use of more sophisticated and targeted strategies, such as ransomware. During the first six months of 2022, approximately 384,000 ransomware distribution attempts were detected worldwide, with 52,000 of them targeting Latin America.

Top 5 exploitation techniques with the highest number of detections in the region during the last year 2022-2023.

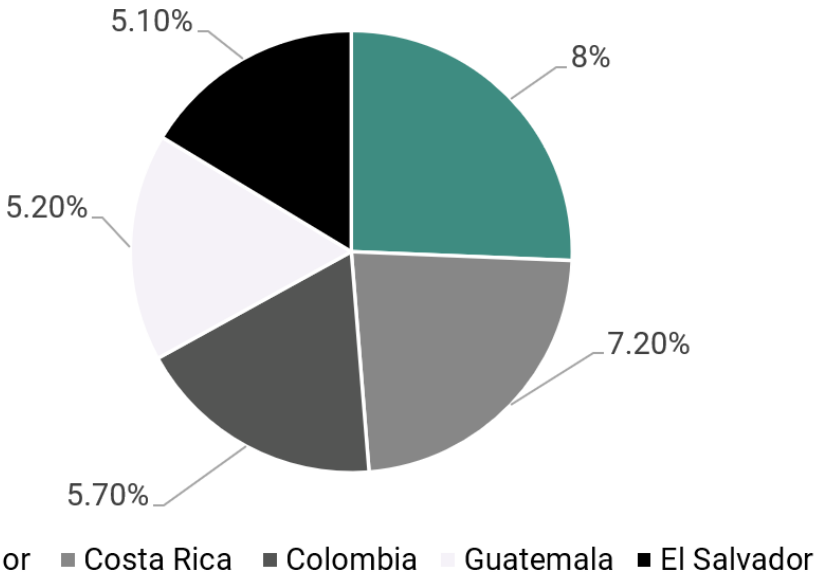
It's important to note that not all vulnerabilities are critical, and there may not be mechanisms available to exploit all of them. Of particular concern are the top five vulnerabilities used by cybercriminals in Latin America during 2022, two of which were discovered 10 years ago and affect widely used services. One of them is CVE-2012-0143, which exploits a vulnerability in Microsoft Windows that allows for remote code execution, and the second is CVE-2012-0159, which abuses a vulnerability in Microsoft Windows that also allows remote access without authentication to a vulnerable system.



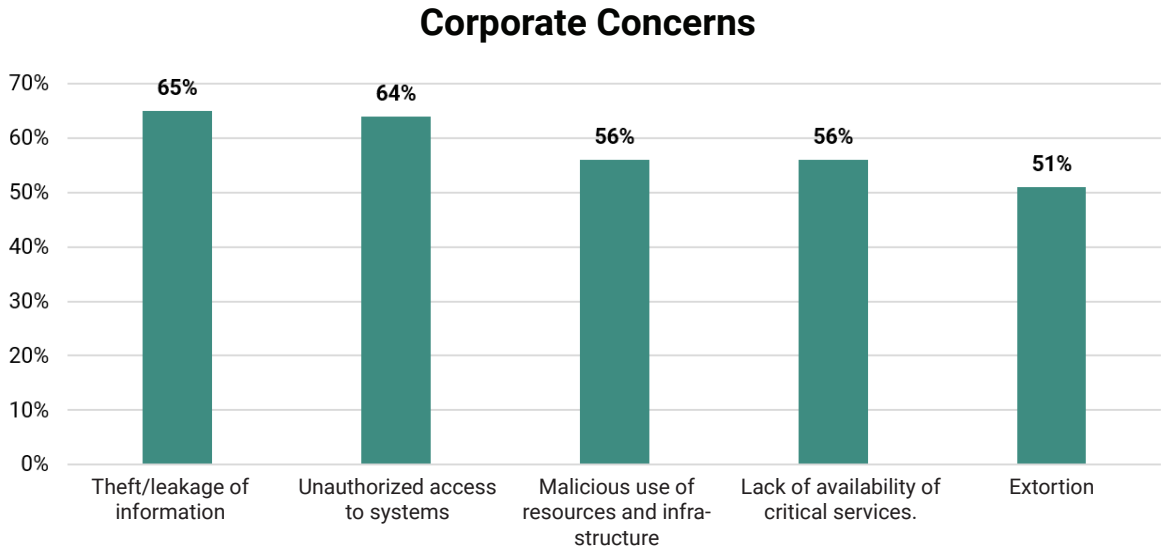
The most reported security incidents in 2022: 70% consider phishing as the most common form of attack, followed by malware attacks at 63%, and in third place, those seeking to steal access credentials at 56%.

Furthermore, considering that there was a 26% increase in the number of reported vulnerabilities in 2022, it is worth mentioning that 49% of the companies confirmed that they received attempted attacks aimed at exploiting a vulnerability.

Malicious Code Campaigns



In the region, 69% of organizations experienced a security incident during 2022. Regarding the countries with the highest percentage of detections of malicious code in phishing campaigns, Ecuador is at 8%, followed by Costa Rica at 7.2%, Colombia at 5.7%, Guatemala at 5.2%, and El Salvador at 5.1%.

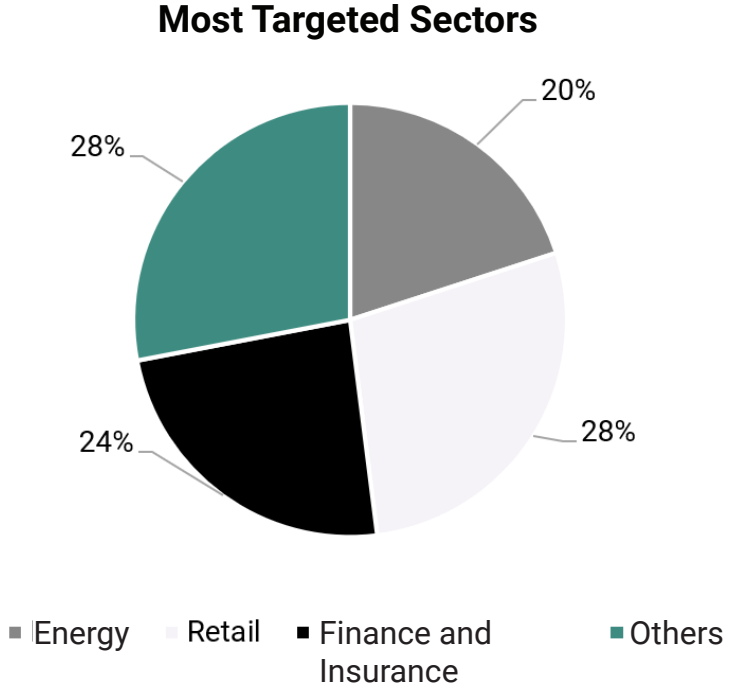


Considering that 66% of organizations' greatest concern is the theft or leakage of information, which suggests the need for the implementation of protective technologies and awareness; it is important to consider that this may be linked to other factors resulting from each organizational dynamic and culture, as well as their technological infrastructure.

On the other hand, 64% of them are concerned about unauthorized access to systems due to its connection with the sophisticated capabilities of malicious actors, considering espionage campaigns or the theft of confidential files. This concern is linked to the rise in vulnerability exploitation attacks that utilize backdoors, or the use of malicious code such as ransomware or Remote Access Trojans (RAT)

The sectors and Areas that Attackers Target

According to IBM's 2023 X-Force Threat Intelligence Index, the region is gaining importance for cybercriminals. Although Latin America accounted for 12% of the attacks, the region moved from the fifth place among the world's most attacked regions to the fourth place. Brazil, Colombia, Mexico, Peru, and Chile were the most attacked Latin American countries in 2022.



Incidents in Latin America ran counter to global industry trends. Retail and wholesale trade were the most targeted, accounting for 28% of the attacks. Finance and insurance came second, with 24% of cases, followed by energy and manufacturing, both at 20%.

Business Email Compromise (BEC) incidents decreased in the region, ranking third in 2022 with 11% of incidents. These types of attacks occur when access to a server is gained to achieve unknown end goals. To gain access, attackers primarily used spear phishing links, malicious attachments, and the exploitation of valid accounts.

Cybercriminals exploit email conversations. Thread hijacking in email conversations significantly increased in 2022, with attackers using compromised accounts to reply to ongoing conversations, posing as the original participant. In the region, email conversation hijacking accounted for 11% of the attacks.

Being extortion the preferred method of threat actors. In the region, one of the most common impacts of cyberattacks last year was extortion, primarily achieved through ransomware or BEC attacks, reflecting the global trend. Cybercriminals primarily target the most vulnerable sectors, businesses, and regions using extortion schemes and applying high psychological pressure to force victims to pay.

The number of cybercriminals focused on credit card information in phishing kits dropped by 52% in one year, indicating that cyber attackers are prioritizing personal identification information such as names, emails, and addresses, which can be sold at a higher price on the dark web or used for further operations.

Legacy security vulnerabilities continue to do the job. The percentage of security exploits related to vulnerabilities decreased by 10 percentage points from 2018 to 2022, as the number of vulnerabilities reached another record in 2022.

The most impersonated brands include major technology companies. Stolen credentials from these services are valuable for accessing accounts that victims use to manage their online presence. This shift in the list towards a more diverse one may be due to improved ability to identify the brands that a kit can impersonate, not just the one it is attacking by default.

Cyberattack Trends and Notable Cases

The latest cyber threat report from Kaspersky indicates approximately 1.15 million ransomware attack attempts in Latin America over the past year, with an average of around 2 blockings per minute. In particular, the report highlights that the WannaCry ransomware still constitutes a significant portion of its detections, accounting for 40.59% of cases. It's worth noting that this particular threat actor has been inactive for a considerable period.

These detections are linked to the vulnerability exploited by the WannaCry group in 2017, which remains unpatched on numerous computers in the region.

Malicious activity in the region has remained relatively stable over the past year. While this might suggest some consistency in the threat landscape, it's important to remember that cyber threats are constantly evolving, and stability doesn't necessarily equate to reduced risk.

There is a significant increase of 617% in malware attacks against computers and mobile devices. This alarming trend in malware attacks indicates that cybercriminals are actively targeting individuals and organizations in Latin America.

Phishing attacks have also increased by 617%, with an average of 544 attacks per minute. Phishing attacks are a common method for stealing sensitive information and credentials. The government and financial sectors have been the hardest hit, posing a significant threat to critical infrastructure and financial institutions.

The resurgence of economic activities after the pandemic appears to be a significant factor contributing to the rise in fraudulent messages. Cybercriminals often seize important events or economic situations to launch phishing campaigns, taking advantage of people's vulnerabilities and uncertainties.

The emergence of AI-driven tools to create fraudulent content indicates that cybercriminals are using advanced technology to automate their attacks. This could make it more challenging for traditional security measures to detect and effectively mitigate these threats.

Brazil, Mexico, Peru, Colombia, Ecuador, Chile, and Argentina are among the most affected countries in Latin America. These countries represent a significant portion of the region's population and economy, making them lucrative targets for cybercriminals.

Financial data is the primary target of phishing attempts, followed by banking topics, payment methods, financial services, and cryptocurrencies. This indicates that cybercriminals are primarily focused on financial gains.

The significant 50% growth in banking trojans is concerning. These trojans are designed to steal banking information and can have a severe impact on individuals and financial institutions. The dominance of Brazilian trojans in the region underscores the need for specific security measures.

It's noteworthy that while Latin America is experiencing an increase in banking trojan attacks, the global trend shows a decrease. This suggests that cybercriminals may be shifting their focus to specific regions where defenses may be weaker.

Cybersecurity measures in the region must adapt to these changing dynamics to effectively protect individuals, businesses, and critical infrastructure. Collaboration between governments, businesses, and cybersecurity experts is crucial to mitigate these threats and ensure a safer digital environment.

State of Cyber Emergency in Latin America

In April 2022, Costa Rica fell victim to a massive ransomware attack that affected over 20 government institutions, including the Ministry of Finance, the Ministry of Public Security, and the Costa Rican Social Security Fund.

The President of Costa Rica was forced to declare a national state of emergency as the ongoing crisis was costing the nation an estimated USD $38 million per day. Ransomware attacks have become a global cybersecurity concern, affecting many countries, including Costa Rica. In these attacks, malicious software encrypts a victim's data, and the attackers demand a ransom in exchange for the decryption key. Victims are often individuals, businesses, or government organizations.

They were targeted by the cybercriminal group "Conti," known to cybersecurity experts as the largest ransomware collective operating at the time, having extracted about $180 million from their targets in 2021. Using compromised credentials, they managed to install malware on a device within the Ministry of Finance's network, which was enough to spread the infection. The attacker extracted hundreds of thousands of gigabytes of information about Costa Ricans, posting a sample on the dark web market. They encrypted the ministry's systems, making it nearly impossible for the government to process payments or collect taxes, and froze the customs agency. To release their control over the ministry's system and not publish the rest of the stolen data, the group demanded $10 million dollars.

CYBERSECURITY PREPAREDNESS AND RESPONSE LEVEL

Maturity and Preparedness Level in the Region

The Inter-American Development Bank (IADB) in its 2016 and 2020 Cybersecurity Reports, using the methodology of the Cybersecurity Capability Maturity Model for Nations (CMM), analyzes the maturity levels corresponding to essential and specific aspects of cybersecurity, including: (a) cybersecurity policy and strategy; (b) cyber culture and society; (c) cybersecurity education, training, and skills; (d) legal and regulatory frameworks; and (e) standards, organizations, and technologies. These are further subdivided into a set of factors that describe and define what it means to possess cybersecurity capability in each factor and indicate how to improve maturity.

For example, the 2016 IDB report indicated that four out of every five countries lacked cybersecurity strategies or critical infrastructure protection plans. By early 2020, 12 countries had approved national cybersecurity strategies, including Colombia (2011 and 2016), Panama (2013), Trinidad and Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), Mexico (2017), Guatemala (2018), Dominican Republic (2018), Argentina (2019), and Brazil (2020), among several others in progress.

This report measures the five dimensions through 49 indicators on a scale from 0 to 100, where 0 is the initial level and 100 is advanced. The report clearly illustrates the regional progress and commitment in developing cyber capabilities in the past four years, with significant improvements in capabilities during the 2016-2020 period. As all countries have shown improvements in this area, the regional average increased to 39.88 points, reflecting a collective effort and interest in the subject. It is also important to highlight the individual efforts of governments in Brazil with a rating of 59.2, Chile 56.3, Colombia 59.2, Uruguay 69.4, and Mexico 56.5, which have prioritized the issue and increased their scores by more than 20 points since 2016. However, there is still a long way to go for the Latin American region in developing its cyber capabilities and reaching maturity levels.

LATAMC Cyber Capabilities Index

No.	Country	2016	2020	Difference
1	Uruguay	45.1	69.4	24.4
2	Colombia	35.8	59.2	23.4
3	Chile	33.9	56.3	22.4
4	Mexico	35.3	56.5	21.2
5	Guyana	19.5	40.5	20.9
6	Dominican Republic	30.3	49.7	19.4
7	Paraguay	26.6	45.7	19.1
8	Brazil	40.1	59.2	19
9	Trinidad and Tobago	30.3	49.3	19
10	Costa Rica	26.4	42.7	16.3
11	Panama	26.7	41.7	15
12	Argentina	34.3	48.5	14.2
13	Jamaica	28.2	41.6	13.4
14	Nicaragua	17.3	29.7	12.5
15	Barbados	21.2	33.3	12.1
16	Bolivia	23.7	35.6	11.9
17	Ecuador	24.3	36.2	11.8
18	Peru	28.7	40.5	11.8
19	Honduras	18.8	30.6	11.8
20	Bahamas	21.1	32.9	11.8
21	Antigua and Barbuda	19.6	31.2	11.7
22	Guatemala	21.5	32.9	11.4
23	Surinam	20.9	31.4	10.5
24	St Vincent and the Grenadines	19.8	30	10.3
25	Saint Kitts y Nevis	22.3	31.8	9.5
26	St Lucia	19.3	28.7	9.4
27	Belize	22.3	31.3	9
28	Grenada	19.1	27	7.9
29	Venezuela	24.6	32.3	7.8
30	El Salvador	23.8	31.3	7.5
31	Dominica	21.5	28.9	7.4
32	Haiti	19.2	24.5	5.4

They have had the Global Cybersecurity Index (GCI) as a reliable reference that measures the commitment of countries to cybersecurity at a global level, to raise awareness about the importance and different dimensions of the problem. As cybersecurity has a wide field of application, covering many industries and various sectors, the level of development or commitment of each country is evaluated along five pillars:

(i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development and (v) Cooperation, and then they are combined into an overall score.

Global Cybersecurity Index

Ranking	Country	2015	2017	2018	2020
1	United States of America	0.824	0.91	0.926	100**
2	Canada	0.794	0.81	0.172	97.67**
3	Brasil	0,706	0.593	0.557	96.6
4	Mexico	0,324	0.66	0.629	81.68
5	Uruguay	0,618	0.647	0.681	75.15
6	Dominican Republic	0,118	0.162	0.43	75.07
7	Chile	0,382	0.367	0.47	68.83*
8	Costa Rica	0,353*	0.336	0.221*	67.45
9	Colombia	0,588	0.569	0.565	63.72
10	Cuba	0,029*	0.058	0.481	58.76
11	Paraguay	0,206*	0.326	0.603	57.09
12	Peru	0,324*	0.374	0.401	55.67
13	Argentina	0,412*	0.482	0.407	50.12
14	Panama	0,294	0.485	0.396	34.11
15	Jamaica	0,235*	0.339	0.407	32.53**
16	Surinam	0,118*	0.155	0.11	31.2
17	Guyana	0,118	0.269	0.132	28.11
18	Venezuela	0,206	0.372	0.354	27.06
19	Ecuador	0,353	0.466	0.367	26.3
20	Trinidad and Tobago	0,206	0.098	0.188	22.18
21	Barbados	0,176	0.273	0.173	16.89
22	Bolivia	0,118*	0.122	0.139	16.14
23	Antigua and Barbuda	0,118*	0.179	0.247	15.62

Ranking	Country	2015	2017	2018	2020
24	Bahamas	0,147*	0.137	0.147	13.3
25	El Salvador	0,206*	0.208	0.124*	13.3**
26	Guatemala	0,206	0.114	0.251	13.13
27	Saint Kitts y Nevis	0,147	0.066	0.065	12.44**
28	St Vincent and the Grenadine	0,000	0.189	0.169	12.18**
29	St Lucia	0,118*	0.053	0.096	10.96**
30	Belize	0,176*	0.182	0.129	10.29
31	Grenada	0,118	0.115	0.143	9.41
32	Nicaragua	0,147*	0.146	0.129	9**
33	Haiti	0,059*	0.04	0.046	6.4
34	Dominica	0,059*	0.01	0.019	4.2
35	Honduras	0,000*	0.048	0.044	2.2**
23	Antigua and Barbuda	0,118*	0.179	0.247	15.62

Note: ** No responses to the questionnaire/data collected by the GCI Team. *Based on secondary data by ABI Research. Source: Global Cybersecurity Index 2015 , 2017 , 2018 , 2020

The Academy of Electronic Government (eGA) has developed a National Cybersecurity Index, which is an appropriate tool for national cybersecurity capacity development. This methodology serves as a systematic guide for the development of a trustworthy information society and, on the other hand, is an index that describes the current situation in different countries and allows countries to compare themselves. The index provides clear materials of public evidence.

This methodology measures the following aspects through its twelve indicators, which are grouped into four dimensions: (a) Development of cybersecurity policies, (b) Analysis and information on cyber threats, (c) Education and professional development, (d) Contribution to global cybersecurity, (e) Protection of digital services, (f) Protection of essential services, (g) Electronic identification and trusted services, (h) Protection of personal data, (i) Response to cyber incidents, (j) Cyber crisis management, (k) Combating cybercrime, and (l) Cyber military operations.

Nacional Cyber Security Index

Country	Global Ranking	Regional	National Cyber Security Index	Digital Development Level	Difference
Dominican Republic	29	1	71.43	45.21	26.22
Argentina	48	2	63.64	60.43	3.21
Paraguay	45	3	63.64	42.58	21.06
Peru	50	4	62.34	48.23	14.11
Uruguay	55	5	59.74	63.86	-4.12
Chile	54	6	59.74	61.44	-1.70
Ecuador	67	7	53.25	45.57	7.68
Colombia	69	8	53.25	52.08	1.17
Brazil	71	9	51.95	59.11	-7.16
Panama	75	10	50.65	48.43	2.22
Costa Rica	77	11	49.35	58.87	-9.52
Jamaica	85	12	41.56	48.18	-6.62
Mexico	90	13	37.66	51.46	-13.8
Trinidad and Tobago	99	14	33.77	52.60	-18.83
Bolivia	105	15	31.17	42.09	-10.92
Nicaragua	107	16	29.87	32.70	-2.83
Venezuela	111	17	28.57	43.14	-14.57
El Salvador	119	18	24.68	39.17	-14.49
Guatemala	118	19	24.68	35.43	-10.75
Honduras	120	20	22.08	35.09	-13.01
Suriname	121	21	22.08	51.50	-29.42
Grenada	125	22	20.78	58.00	-37.22
Bahamas	126	23	20.78	65.10	-44.32
Barbados	130	24	19.48	73.10	-53.62
Belize	133	25	18.18	37.10	-18.92
Cuba	136	26	16.88	29.10	-12.22
St Lucia	144	27	12.99	46.30	-33.31
Antigua and Barbuda	148	28	11.69	57.10	-45.41
Saint Kitts and Nevis	149	29	11.69	72.40	-60.71
Guyana	155	30	10.39	42.91	-32.52
Haiti	160	31	7.79	26.46	-18.67
St Vincent and the Grenadine	161	32	7.79	55.40	-47.61
Dominica	169	33	3.90	56.90	-53.00

Nota: Información capturada el 30 de Julio del 2023. Fuente: Índice Nacional de Seguridad Cibernética.

Nota: Information captured on July 30, 2023. Source: National Cybersecurity Index.

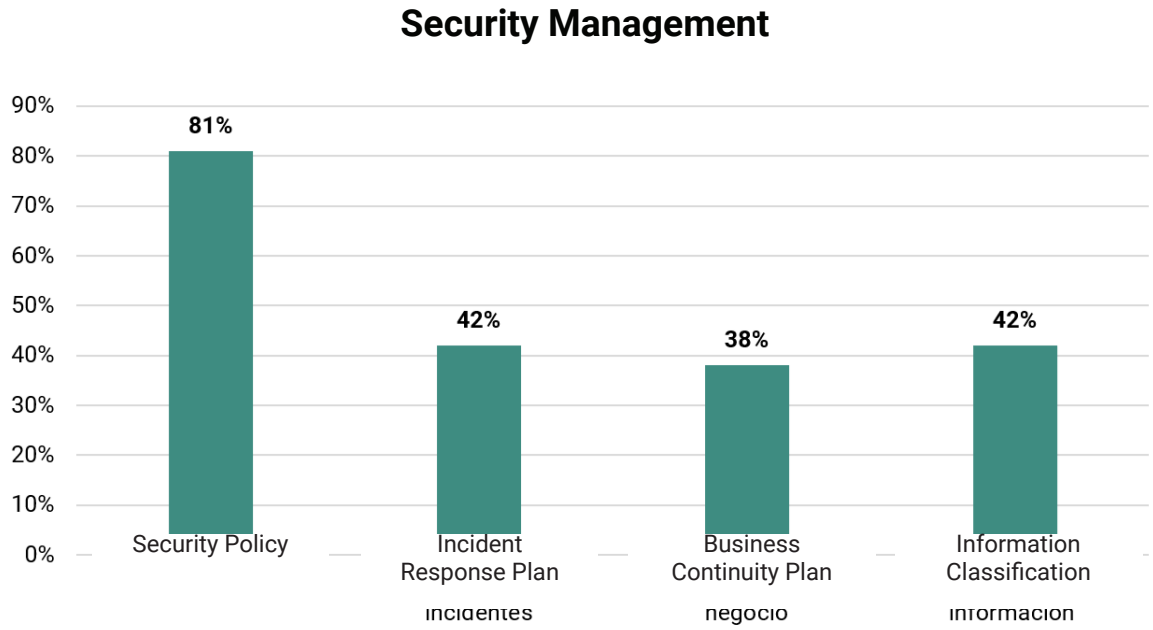
It is important to highlight that these measurement indixes are dynamic evaluations based on the evidence that each country provides as support and justification for the actions designed, developed, and executed within each evaluated dimension. Therefore, countries may have different positions in each of the indices, reflecting the relevance of each instrument for the evaluated countries.

Implemented Solutions

When establishing controls, distinctions can be made between those based on technology, such as a firewall solutions, and those related to management, like increasing awareness or developing information protection processes, among others. This is why organizations in the region have implemented security technologies, with the most significant ones in 2022.

Solution	Percentage
Backup	88%
Firewall	87%
VPN	72%
Antimalware Solution	58%
Email Filtering Solution	48%
IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	35%
Endpoint Detection and Response (EDR)	34%
Two-factor Authentication Solutions	34%
Encryption Technologies	23%
Data Loss Prevention	22%
Patch Management Solution	14%
Mobile Device Security Solutions	13%
Threat Intelligence	13%

A new trend in priorities is emerging, as a large number of companies fell victim to ransomware attacks and other threats directly targeting their data. Backup systems, implemented in 88% of work devices, were the most widely adopted security solution in organizational settings. Firewalls, at 86%, were the second most commonly used technology, with VPN solutions ranking third at 72%.



Following the continuous improvement of technologies, organizations in the region are focusing on security management practices and policies. These are not only essential for preventing security incidents but also for swiftly recovering operations after a cyberattack. In a noteworthy trend, 81% have implemented a specific security policy, marking a 10% increase compared to the previous year, 2022. Additionally, 41% have established an incident response plan, reflecting a 4% increase from the previous year.

Response and Incident Management Capabilities

The Academy of Electronic Government (eGA) in the National Cybersecurity Index highlights the maturity of response and incident management capabilities to effectively detect, respond to, and mitigate cybersecurity incidents. These capabilities encompass a range of processes, procedures, and resources designed to manage and recover from cyber threats and attacks. Below, we can observe the progress of these capabilities in the region:

Incident and Crisis Management Indicators

Country	Cyber incidents response	Cyber crisis management	Fight against cybercrime	Military cyber operations
República Dominicana	5	3	9	6
Argentina	3	3	9	6
Paraguay	5	3	9	3
Perú	6	1	9	4
Uruguay	5	1	6	3
Chile	3	1	9	6
Ecuador	5	1	4	4
Colombia	3	1	9	4
Brazil	3	1	4	6
Panama	3	3	9	1
Costa Rica	5	1	9	1
Jamaica	3	1	7	4
Mexico	3	1	7	1
Trinidad and Tobago	5	1	4	0
Bolivia	5	1	7	3
Nicaragua	0	1	7	0
Venezuela	3	0	7	0
El Salvador	3	1	4	0
Guatemala	0	1	7	0
Honduras	0	1	7	0
Suriname	3	0	4	1
Grenada	0	0	4	1
Bahamas	0	0	7	1
Barbados	0	0	4	0
Belize	0	0	4	1
Cuba	3	0	0	0
Saint Lucia	0	0	1	0
Antigua and Barbuda	0	0	1	1
Saint Kitts and Nevis	0	0	1	0
Guyana	3	0	1	1
Haiti	0	0	0	0
Saint Vincent and the Grenadines	0	0	1	0
Dominica	0	0	0	0

Nota: Information captured on July 30, 2023. Source: National Cybersecurity Index

Cybersecurity Exercises and Simulations

Regional Exercise CyberCrabs

This exercise had the mission of increasing overall awareness of different cybersecurity risks and incidents and promoting collaboration on possible responses when they occur in the region. The exercise contributed to improving information sharing among the participating countries in the region and exploring the best decision-making mechanisms for simultaneously responding to similar cyber incidents.

The exercise included the following countries from the region: Antigua and Barbuda, Bahamas, Belize, Curacao, Dominica, Dominican Republic, Guyana, Jamaica, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Trinidad and Tobago, including CARICOM IMPACS, the Organization of Eastern Caribbean States, and the Eastern Caribbean Central Bank.

The Latin American and Caribbean Cyber Competence Center (LAC4), in cooperation with CARICOM IMPACS, the OAS, and the National Cybersecurity Center (CNCS) of the Dominican Republic, organized the tabletop exercise (TTX) to test crisis cyber management procedures and cross-border information exchange.

TAIEX INTPA Workshop on Strategic Cybersecurity for Central America

In 2023, the TAIEX INTPA Workshop on Strategic Cybersecurity for Central America and the Dominican Republic was held at the Latin American and Caribbean Cyber Competence Center (LAC4) in Santo Domingo, Dominican Republic. It focused on countries in the Latin American and Caribbean (LAC) region, including Belize, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, and Panama. The event, organized by EU CyberNet and the European Union Delegations of Costa Rica and the Dominican Republic.

Its main objectives were to increase awareness and understanding of the cyber threat landscape and cybersecurity needs in the Central American region, explore cooperation opportunities among Central American countries, and provide participants with expert guidance and a platform for sharing and learning from existing practices.

BEST PRACTICE AND RECOMMENDATIONS

Recommendations to Improve Cybersecurity Preparedness

Cybersecurity is a dynamic and evolving field, and staying ahead of emerging threats requires a proactive and adaptable approach. By leveraging regional collaboration, international best practices, and a commitment to cybersecurity education and innovation, Latin America and the Caribbean can continue to enhance their cybersecurity preparedness and resilience.

- Invest in cybersecurity education and training programs to develop a skilled workforce capable of addressing evolving threats. Collaborate with universities and industry partners to create relevant curricula.
- Foster collaboration between governments and the private sector to share threat intelligence, best practices, and resources. Jointly develop cybersecurity initiatives and incident response plans.
- Strengthen and enforce cybersecurity legislation and regulations, including data protection laws. Create incentives for organizations to prioritize cybersecurity and hold them accountable for breaches.
- Enhance efforts for international cooperation and collaboration through information-sharing partnerships and networks to stay updated on global cybersecurity threats and solutions.
- Collaborate with neighboring countries to improve regional cybersecurity resilience.
- Allocate resources for the acquisition of cybersecurity technologies, such as intrusion detection systems, firewalls, and advanced threat analysis tools.

- Conduct cybersecurity awareness campaigns to educate individuals and organizations about risks and best practices for staying safe online.
- Develop and periodically update incident response plans to ensure a swift and coordinated response in the event of a cyberattack.
- Encourage the execution of cross-border incident response simulation exercises.
- Establish working groups to respond to incidents from countries with lower capabilities.

Future Perspectives and Emerging Challenges

To better understand the true nature of cybersecurity challenges, organizational leaders must shift their frame of reference beyond their own perimeter and toward their broader role in the interconnected community. This community encompasses partners, suppliers, customers, government entities, competitors, and more.

- The proliferation of Internet of Things (IoT) devices and increased interconnectivity of critical infrastructure poses significant challenges. Protecting these systems from cyberattacks is crucial to prevent disruptions.
- As AI and machine learning technologies advance, so do the capabilities of cybercriminals who can leverage these tools for more sophisticated attacks.
- As data continues to be a valuable asset, data privacy regulations will become more complex. Adhering to international standards and protecting citizens' data will be a priority.
- Ensuring the security of the supply chain, especially for critical infrastructure and government systems, is a growing concern as attackers target the weakest links in the chain.
- Ransomware attacks continue to evolve, and organizations must be prepared to defend against them and have incident response and recovery strategies in place.
- Some countries in the region that already have a national cybersecurity strategy exhibit significant variability in the implementation and application of these strategies.
- Attention must be paid to e-commerce in the region as it has exposed businesses and consumers to new cybersecurity risks, requiring enhanced cybersecurity measures.

- Many countries in the region still face economic and resource limitations that can hinder their ability to invest in robust cybersecurity measures.
- The shortage of skilled cybersecurity professionals in the region persists, creating a gap in effective defense against cyber threats.
- Cybersecurity is increasingly intertwined with geopolitics. Countries in the region may face cyber threats from state-sponsored actors or representatives.
- Quantum computing necessitates timely adoption of secure, robust cryptographic algorithm development for industries. Organizations must begin preparing for the quantum threat to ensure the long-term security of their data and communications.

CONCLUSIONS

In conclusion, it is undeniable that the governments of Latin America and the Caribbean have demonstrated an unwavering commitment to strengthening their cybersecurity capabilities. They have recognized the urgent need to bolster their cyber defenses and have taken significant measures in this direction. National cybersecurity strategies aligned with global standards have been developed, and relevant regulations have been updated to ensure adaptation to evolving digital threats.

In this context, collaborative initiatives, both regionally and internationally, have played a crucial role in enabling the exchange of threat intelligence and best cybersecurity practices. However, the region faces notable challenges, such as resource limitations and a shortage of highly skilled cybersecurity professionals. The constant evolution of digital threats raises questions about the region's capacity to safeguard its digital space.

It is crucial to highlight that the digital divide remains a relevant obstacle, as some segments of the population still lack access to essential digital services and educational opportunities in this field. Consequently, maintaining a proactive focus on cybersecurity education and capacity development is imperative. Promoting the formation of a strong workforce in this field and ensuring digital inclusion for all citizens will be essential for long-term success in protecting the region against cyber threats.

COLLABORATIONS

Principal Author
Carlos Leonardo
Cybersecurity Consultant

Contributions

Ministry of Foreign Affairs of the Kingdom of the Netherlands

César Moliné Rodríguez
Regional LAC4 Director

Estevenson Solano
Cybersecurity Consultant

Anthony Cruz
Cybersecurity Consultant

Claudio Peguero
Ambassador for Cyber Affairs of the Dominican Republic

Reyson Lizardo
Director of Digital Agenda of the Dominican Republic

Design & Layout
Henry González
HAGM Industrial