CYBERSECURITY IN LATIN AMERICA:

National Strategies in 2024

Derechos Digitales
AMÉRICA LATINA

CYBERSECURITY IN LATIN AMERICA:
National Strategies in 2024

This publication was created by Derechos Digitales, an independent non-profit organization, founded in 2005, whose mission is the defense, promotion, and development of human rights in digital environments in Latin America.

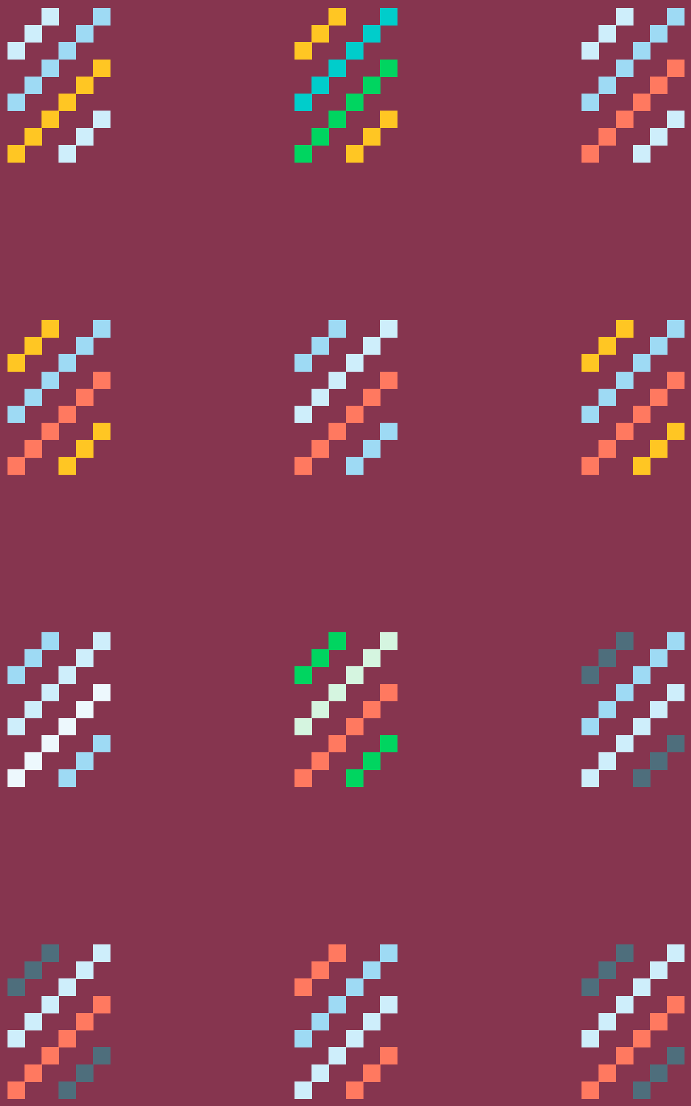
Author: Juan Carlos Lara
English and Portuguese translation: Dafne Melo
Design: Comunas Unidas

December, 2024.

This publication was made possible thanks to Derechos Digitales being a member of the CYRILLA Collaborative.

Derechos
Digitales
AMÉRICA LATINA

INDEX



EXECUTIVE SUMMARY

Cybersecurity has become a priority issue for Latin American governments, given the increase in digital threats and the growing dependence on technological infrastructures. This report provides an introductory account of national cybersecurity policies and strategies in the region, identifying commonalities and challenges that persist in implementing those policies.

The document highlights the diversity of approaches in the region, with strategies varying in terms of scope, maturity, and implementation capacity. In some cases, such as Argentina and Ecuador, strategies are well defined but face challenges in implementation due to a lack of technical and human resources; in others, such as Peru, the lack of formalized documents limits the impact of cybersecurity efforts.

This analysis concludes that in order to move towards a secure and resilient digital environment, it is crucial to prioritize regional collaboration, strengthen local capacities, and align national strategies with international standards. Amidst the main challenges identified is the need to strengthen national technical capacities, multisectoral coordination, and international cooperation. In addition, the region needs to advance in the creation of specific regulatory frameworks that support national strategies and promote a culture of cybersecurity among its citizens.

1. INTRODUCTION

Cybersecurity in Latin America has evolved unevenly, reflecting a diversity of national contexts and strategic priorities. This document maps already adopted or under development cybersecurity policies and strategies in different countries in the region, from those formalized and in full implementation to initial planning and consultation efforts. The integration of national and international perspectives is essential to understanding the regional landscape.

This analysis overlooks a detailed consideration of the institutional and legal frameworks underpinning the strategies, as well as the concrete actions proposed to address the growing cyber threats. From Brazil, with its consolidated E-Ciber strategy, to cases such as Honduras and El Salvador, where progress is incipient, there is a significant gap in capabilities and resources which influences policy effectiveness. This disparity requires a very different scale of effort.

The goal of this text is to provide a comprehensive view of cybersecurity in Latin America in 2024, assessing achievements, and identifying areas requiring urgent attention and opportunities to strengthen regional cooperation. This perspective will enable stakeholders to elaborate more coordinated and effective responses to emerging threats in cyberspace.

2. NATIONAL CYBERSECURITY STRATEGIES IN LATIN AMERICA

2.1. Argentina: *Second National Cybersecurity Strategy*

Argentina has made significant progress in its approach to cybersecurity with the implementation of the Second National Cybersecurity Strategy, approved by Resolution 44/2023 of the Secretariat of Public Innovation in September 2023[1]. Developed by the National Cybersecurity Committee, this document establishes national guidelines for cyberspace protection, aiming to prevent actions that could impact the administration of the State, organizations, essential services, and the general public.

The new strategy addresses issues such as gender perspective and human rights incorporation, attention to vulnerable sectors, and specific considerations related to emerging technological developments, such as the Internet of Things (IoT), 5G, and cloud services. It also focuses on digital sovereignty and promotes collaborative multi-stakeholder governance.

The document includes eight Guiding Principles, namely: Peace and Security in Cyberspace, Respect for Human Rights and Fundamental Freedom, Capacity Building and Federal Strengthening, International Cooperation, Cybersecurity Culture and Shared Responsibility, Strengthening Socioeconomic Development, Security for People in Vulnerable Situations or Historically Discriminated, Gender Perspective and Human Rights.

[1] Available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

The goals to which the 42 measures mentioned are subordinated are the following: strengthening the institutional system to address cybersecurity at the federal level; protection of critical national infrastructures; protection and recovery of public sector information systems; strengthening of prevention, detection and response capabilities; cybersecurity awareness, training, and education; development of a regulatory framework according to digital challenges; international cooperation in cybersecurity; promotion of the national cybersecurity industry.

2.2. Brazil: *E-Ciber*

The National Strategy for Cyber Security or “E-Cyber” was approved by Decree No. 10.222, in February 2020[2]. Its purpose is to consolidate Brazil's regional leadership in cybersecurity. It is part of the National Information Security Policy, established by Decree No. 9.637 of December 2018, which defines principles and objectives for information security in the federal public administration. E-Ciber was developed with the participation of more than forty government agencies, private institutions and the academic sector, and its main objective is to strengthen cybersecurity in the country, improving the resilience of critical infrastructures and national public services.

The vision of Brazil's National Cyber Security Strategy is to make Brazil “a country of excellence in cyber security”. To achieve this, three fundamental strategic objectives were defined: to make Brazil a more prosperous and trusted country in the digital environment; to increase its resilience to cyber threats; and to strengthen Brazil’s role in cybersecurity in the international arena. This seems coherent with Jair Bolsonaro’s government since the strategy was approved during his administration.

The policy’s strategic actions include fostering national and international cooperation for the exchange of information on cyber threats; developing cyber incident prevention, monitoring, and response capabilities; protecting critical information infrastructures with a comprehensive approach; promoting public awareness of the importance of cybersecurity; establishing technical training programs in cybersecurity; encouraging research and development of advanced technological solutions; and actively participating in international forums related to cybersecurity.

E-Ciber’s term was due until 2023. In June 2023, under a different administration, it was announced that the strategy would be extended to 2024[3]. A new policy is still pending and already being worked on.

[2] Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

[3] "Governo prorroga por um ano a Estratégia Nacional de Segurança Cibernética", Convergência Digital, June 6, 2023. Available at: https://convergenciadigital.com.br/seguranca/governo-prorroga-por-um-ano-a-estratgia-nacional-de-segurana-ciberntica/

2.3. Chile: *PNCS 2023-2028*

The first National Cybersecurity Policy (PNCS, an acronym for Política Nacional de Ciberseguridad, in Spanish) was implemented between 2017 and 2022, establishing the basis for a more secure cyberspace. Subsequently, on December 4, 2023, the new PNCS for the period of 2023-2028 was officially published[4]. The Interministerial Committee on Cybersecurity (CICS, an acronym for Comité Interministerial sobre Ciberseguridad, in Spanish) has been the body responsible for the development and coordination of these policies, ensuring collaboration between various government and private entities, as well as public hearings and consultations prior to the finalization of each PNCS.

The PNCS 2023-2028 maintains the five fundamental goals already present in its predecessor: resilient infrastructure, people's rights, cybersecurity culture, national and international coordination, and promotion of industry and scientific research. In addition, it incorporates four cross-cutting objectives: human rights approach, gender perspective, sustainable development, and international cooperation.

In a significant step forward for the PNCS, the Framework Law on Cybersecurity and Critical Information Infrastructure was enacted in March 2024, creating the National Cybersecurity Agency (ANCI, an anacronym for Agencia Nacional de Ciberseguridad, in Spanish). This governing body is responsible for regulating, overseeing, and sanctioning all public and private bodies that provide essential services, strengthening the institutional framework for cybersecurity in Chile.

Although the PNCS 2023-2028 establishes clear guidelines, the detailed action plan specifying the measures and timelines to achieve the proposed objectives has not yet been published. It is expected that this complementary document will be released soon to guide the effective implementation of the policy.

2.4. Colombia: *Reliance and Digital Security Policies*

In 2016, the country adopted the National Digital Security Policy through a document called CONPES 3854, establishing the basis for a more secure and reliable digital environment. Subsequently, in 2020, the National Policy on Trust and Digital Security (CONPES 3995) was published[5], whose goals are: to strengthen the digital security capabilities of citizens, the public sector and the private sector in the country; to update the governance framework in digital security to increase its degree of development; and to analyze the adoption of models, standards and frameworks in digital security, with emphasis on new technologies.

In accordance with these efforts, the Colombian government has proposed the creation of the National Agency for Digital Security and Spatial Affairs, a technical and specialized entity aimed at planning, coordinating, and managing digital security risks in the country, as well as strengthening trust and security in the digital sphere. This bill was presented to Congress in July 2023 and has advanced in its legislative process, being approved in the first debate in November of the same year. The Agency will be responsible for coordinating cybersecurity

[4] Available at: https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf?utm_source=chatgpt.com

[5] Available at: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

actions, including the protection of critical information infrastructures, the response to cyber incidents, and the promotion of a digital security culture in Colombian society.

These are all efforts of a policy-level strategy to enhance Colombia's cybersecurity capabilities[6], which in addition to the creation of the Agency, this strategy includes reinforcing the Colombian Cyber Incident Response Center (ColCERT), establishing a cybersecurity center in Caldas, and improving training and education in cybersecurity specializations.

2.5. Costa Rica: *National Cybersecurity Strategy 2023-2027*

In 2017, Costa Rica implemented its first National Cybersecurity Strategy, establishing a framework to protect its critical infrastructures and promote a digital security culture. However, in the face of increasing cyber threats and technological evolution, the need to update this strategy was recognized. In November 2023, the Ministry of Science, Innovation, Technology and Telecommunications (MICITT, an acronym for Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, in Spanish) presented the new National Cybersecurity Strategy 2023-2027[7], with the goal of enhancing the country's resilience against cyber threats and guaranteeing a secure digital environment for citizens.

The National Cybersecurity Strategy 2023-2027 is articulated around five major pillars: governance and coordination; legal and regulatory frameworks; infrastructure protection and cyber-resilience: education, training and awareness; and cooperation and alliances. These pillars seek to establish a comprehensive framework for action to prevent and mitigate risks and threats in the digital environment, foster innovation, and the development of cybersecurity solutions, strengthen incident response capacity and promote a solid security culture in Costa Rican society.

In terms of organization, the MICITT leads the implementation of the strategy in coordination with the Computer Security Incident Response Center (CSIRT-CR), which, as the entity in charge of coordinating cyber and information security in the country, operates as an essential component of this strategy. The strategy incorporates the active participation of public institutions, private companies, civil society, and academia, ensuring a multisectoral approach to cybersecurity strengthening in the country.

2.6. Ecuador: *ENC*

On August 3, 2022, the country presented its first National Cybersecurity Strategy (ENC, anacronym for Estrategia Nacional de Ciberseguridad, in Spanish), developed by the Ministry of Telecommunications and Information Society (MINTEL). This strategy seeks to provide citizens with more secure access to digital services and strengthen the protection of their personal data, in the context of the recent enactment of its first comprehensive national law on data protection.

[6] "Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad", MINTIC, July 19, 2023. Available at: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276939:Ministro-TIC-presenta-la-estrategia-de-cuatro-puntos-para-hacer-de-Colombia-una-potencia-en-Ciberseguridad

[7] Available at: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%20 10Nov2023%20SPA.pdf

The ENC is structured along six lines of action: national governance and coordination, cyber resilience, combating cybercrime, national cyber defense and cyber intelligence, cybersecurity skills and capabilities, and international cooperation.

The implementation of the ENC involves the active participation of various public and private institutions, as well as collaboration with international organizations specialized in cybersecurity. MINTEL leads the coordination of these actions, working together with entities such as the National Cybersecurity Committee, to ensure a comprehensive and effective approach to the protection of Ecuadorian cyberspace.

2.7. Guatemala: *National Cybersecurity Strategy*

Guatemala published its National Cyber Security Strategy on June 20, 2018[8], developed by the Ministry of the Interior in collaboration with various national and international actors. The drafting process included consultations and validations with more than 160 representatives from different sectors of Guatemalan society, seeking to strengthen security in cyberspace and protect citizens' personal data.

The strategy is articulated around the following fundamental axes: capacity building, critical infrastructure protection, legal and regulatory framework, awareness raising and education, and international cooperation. It also includes specific action plans with concrete measures, although it does not detail their total number.

The implementation of the strategy has faced challenges, mainly due to the absence of a specific legal framework to support the proposed actions. Nevertheless, efforts have been made to set up the National Cyber Security Committee, which is responsible for coordinating and monitoring policies in this area. The validity of the strategy is subject to periodic revisions to adapt to new threats and technological advances in the digital sphere.

2.8. Mexico: *ENCS*

Mexico published its National Cybersecurity Strategy (ENCS, an acronym for Estrategia Nacional de Seguridad Cibernética, in Spanish) in November 2017, developed with the collaboration of the Organization of American States (OAS)[9]. The process of developing the ENCS, called "Towards a National Cybersecurity Strategy", was carried out from March to October 2017, promoting spaces for dialogue, discussion, and learning through forums and workshops that involved various actors of Mexican society.

The ENCS establishes five strategic goals: protecting society and its rights; preserving the country's economic prosperity; maintaining public order, peace, and national security; strengthening international cooperation; and promoting a reliable digital government. Moreover, it is based on guiding principles such as a human rights perspective, a risk management approach, and multidisciplinary and multi-stakeholder collaboration.

Since its publication, the implementation of the ENCS has faced some challenges, including the need to harmonize efforts among various institutions and sectors. Despite these

[8] Available at: https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf

[9] Available at: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

challenges, progress has been made in promoting a culture of cybersecurity and in training specialized personnel. The validity of the strategy is subject to periodic reviews to adapt to the constantly evolving digital environment and new cyber threats.

2.9. Nicaragua: *National Cybersecurity Strategy 2020-2025*

Nicaragua approved its National Cybersecurity Strategy 2020-2025 through Presidential Decree No. 24-2020, published on September 29, 2020[10]. This strategy was developed by the Nicaraguan Institute of Telecommunications and Post (TELCOR, Instituto Nicaraguense de Telecomunicaciones y Correos) and the Ministry of Foreign Affairs, with the goal of guaranteeing a sovereign, secure, and reliable use of cyberspace in the country.

The strategy is based on four guiding principles: guaranteeing sovereignty and protecting citizens' rights in cyberspace, risk management and resilience, protection and defense of cyberspace, and international cooperation. It is also structured into five strategic goals: strengthening cybersecurity governance, protecting critical information infrastructures, developing national cybersecurity capabilities, promoting a culture of cybersecurity in society, and fostering international cooperation in cybersecurity.

The implementation of the strategy is planned for the period 2020-2025, with periodic evaluations to adapt to the country's needs and emerging threats in the digital sphere. However, its implementation has raised concerns among human rights organizations and sectors of civil society, who fear that it could be used to restrict freedom of expression and increase government control over cyberspace, as has been the case with the country's controversial Cybercrime Law.

2.10. Panama: *National Cybersecurity Strategy 2021-2024*

Panama published its National Cybersecurity Strategy 2021-2024 on December 15, 2021, through Resolution No. 17 of the National Authority for Government Innovation (AIG, anacronym for Autoridad Nacional para la Innovación Gubernamental)[11]. This strategy updates the 2013 National Cybersecurity Strategy, reflecting the evolution of information and communication technologies, and the need to strengthen security in Panamanian cyberspace.

The strategy is structured around four key pillars: protecting the privacy and fundamental rights of citizens in cyberspace, deterring and punishing criminal behavior in cyberspace, strengthening the security and resilience of the nation's critical infrastructure, and fostering a national culture of cybersecurity.

For its implementation, the AIG has coordinated workshops and awareness campaigns, such as "Panama Cibersegura", aimed at promoting a culture of cybersecurity in society. In addition, the role of CSIRT Panama has been strengthened as the national information security incident response team, responsible for preventing, identifying, and resolving cyber-attacks affecting the country's critical infrastructure. The strategy is in effect until 2024, with periodic evaluations to adapt to new threats and technological advances.

[10] Available at: https://legislacion.asamblea.gob.ni/indice.nsf/c3639d8c1d72577006256fe800533609/e9e4a6071fa07177062585b9005fd3db

[11] Available at: http://www.gacetaoficial.gob.pa/pdfTemp/29434_A/88864.pdf

2.11. Paraguay: *National Cybersecurity Plan*

Paraguay adopted its National Cybersecurity Plan in 2017, approved by Decree No. 7052/17[12]. This plan was developed under the leadership of the Presidency of the Republic, through the National Secretariat of Information and Communication Technologies (SENATICs, anacronym for Secretaría Nacional de Tecnologías de la Información y Comunicación), in coordination with the Ministry of Foreign Affairs and with the support of the OAS. The drafting process involved various sectors, including the private sector and civil society, with the goal of establishing public policies to strengthen the security of critical assets and promote a secure and resilient cyberspace.

The plan is structured along several lines of action: awareness and culture, research, development and innovation, critical infrastructure protection, cyber incident response capacity, investigation and prosecution capacity, and national coordination. Moreover, it defines specific objectives and an action plan for the implementation of the national cybersecurity policy, with the participation of government entities, the private sector, academia, and civil society.

In 2024, the Ministry of Information and Communication Technologies (MITIC), through the General Directorate of Cybersecurity and Information Protection (DGCPI) and the CERT-PY, began updating the national strategy for the period 2024-2028, once again with the support of the OAS. This process includes dialogue and roundtables with key actors of the national cybersecurity ecosystem, seeking to consolidate an updated public policy that responds to the emerging challenges in the digital sphere.

2.12. Dominican Republic: *National Cybersecurity Strategy 2030*

The Dominican Republic approved its National Cybersecurity Strategy 2030 through Decree No. 313-22 of June 14, 2022[13], valid until December 31, 2030. This strategy aims to strengthen the national cybersecurity framework, promoting the creation of secure, reliable, and resilient digital environments that promote an inclusive digital society that respects fundamental rights.

The strategy is structured along several fundamental lines: strengthening regulatory framework, development of cybersecurity capabilities and competencies, protection of critical information infrastructures, risk management and response to cyber incidents, cybersecurity awareness and culture, and national and international cooperation.

For its implementation, a Board of Directors has been established, chaired by the Ministry of the Presidency, which coordinates the actions of the National Cybersecurity Center (CNCS, anacronym for Secretaría Nacional de Tecnologías de la Información y Comunicación). The CNCS is responsible for executing the policies and plans derived from the strategy, including the operation of the CSIRT-RD, the national cyber incident response team. The strategy provides periodic evaluations to adapt to new threats and technological advances, ensuring the protection of Dominican cyberspace and the digital trust of its citizens.

[12] Available at: https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

[13] Available at: https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

3. ONGOING STRATEGY FORMULATION PROCESSES

The other countries in the region do not have national strategies or policies on cybersecurity, although in several cases there are measures applicable at the central government level or in related regulations. In many of these cases, national strategies or policies have been announced or are under development.

Although El Salvador does not yet have a definitive text, it is developing its National Cybersecurity Strategy to strengthen the protection of digital information and critical infrastructure of the State, as a commitment to the Digital Agenda 2020-2030[14]. However, during 2024 the country has approved the Cybersecurity and Information Security Law, which establishes principles, a legal framework, and guidelines to structure, regulate, audit, and oversee cybersecurity measures in public institutions. This law requires the implementation of cybersecurity management systems, the development of information security strategies, and the maintenance of updated records of the actions carried out in this area.

Honduras also lacks a strategy and a national CSIRT, which limits its ability to respond to cyber incidents and safeguard its digital infrastructure.. The Honduran Digital Government Plan 2023-2026[15] commits to the issuance of a National Cybersecurity Strategy and Action Plan, as well as the creation of a cyber incident team.

Peru has a working document entitled National Digital Security and Trust Strategy 2021-2026, prepared by the Digital Government Secretariat of the Presidency of the Council of Ministers (PCM)[16]. The document proposes a comprehensive framework to strengthen cybersecurity and promote trust in the digital environment, articulated in axes such as security culture, capacity building, protection of critical assets, standards, digital services, and legal framework. However, the document has not been adopted as official policy.

Uruguay is in the process of developing its National Cybersecurity Strategy 2024-2030, led by the Agency for Electronic Government and the Information and Knowledge Society (Agesic)[17]. The strategy is structured in six pillars: governance and regulation; critical infrastructure protection; technical and human capabilities; education and awareness; risk management; national and international cooperation. Its development includes public

[14] Available at: https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf

[15] Available at: https://www.diger.gob.hn/sites/default/files/2024-02/Plan%20de%20Gobierno%20Digital%20Honduras.pdf

[16] Referenced on the website of the Secretariat of Government and Digital Transformation. Available at: https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital

[17] "Co-creation of the National Cybersecurity Strategy," Agesic, September 10, 2024. Available at: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/cocreacion-estrategia-nacional-ciberseguridad

consultations and multi-sector workshops, integrating the perspectives of key stakeholders to design a comprehensive cybersecurity framework. This effort complements the recent enactment of Law 20.327, which sets provisions to prevent and penalize cybercrime. As of the closing date of this report, there was no finalized version of the strategy.

Venezuela has taken steps towards the consolidation of a National Cybersecurity Strategy, although it does not have a formalized document. In August 2024, the government created the National Cybersecurity Council, through Decree No. 42,939, with the goal of coordinating policies in this area, advising the Executive, and proposing specific regulations[18]. Cyberspace was declared a public and strategic interest, emphasizing the need for measures to protect critical infrastructures and guarantee digital sovereignty. Despite the lack of an integrated strategy, the country has a National Information Security System, under the supervision of the Superintendence of Electronic Certification Services (SUSCERTE, anacronym for Superintendencia de Servicios de Certificación Electrónica, in Spanish), which seeks to establish standards and conditions for secure use of information and communication technologies.

4. ANALYSIS

The cybersecurity landscape in Latin America showcases a variety of approaches and varying levels of maturity in the implementation of national strategies.. Countries such as Argentina and Brazil have made progress in formalizing policies that seek to strengthen resilience against cyber threats, while nations such as Honduras and Peru have not yet consolidated official strategic frameworks, which could limit their capacity to respond to digital incidents.

The influence of international organizations, especially the Organization of American States, has been decisive in providing advice and technical support for the development of these strategies. This support has allowed several countries to structure plans aligned with global standards, in addition to having technical support with respect to goals and proposed measures. More importantly, this support allows us to consider that, despite the dispersion of bodies and instruments, their contents may be promoting a coherent regional vision on cybersecurity.

The effective implementation of these policies faces significant challenges. The lack of specialized resources, both human and technological, and the absence of robust legal frameworks make it difficult to implement concrete measures. In addition, the rapid evolution of technologies and the tactics employed by malicious actors require constant updating and adaptation of national strategies.

It is imperative that the countries of the region strengthen international and regional cooperation, sharing experiences and best practices to address common threats. Likewise, the integration of cybersecurity into national development agendas and the promotion of a digital security culture among citizens are key to building a safer and more resilient digital environment in Latin America.

[18] "Official Gazette: National Cybersecurity Council Created," ISCOM, August 20, 2024. Available at: http://mippci.gob.ve/index.php/2024/08/20/gaceta-oficial-creado-consejo-nacional-de-ciberseguridad/

www.derechosdigitales.org