BRAZILIAN CYBERSECURITY STRATEGY (E-Ciber)

2025

BRAZILIAN GOVERNMENT

BRASIL

STANDING WITH THE BRAZILIAN PEOPLE

E-Ciber

Foreword

The Institutional Security Office of the Presidency of the Republic (GSI/PR) presents the new National Cybersecurity Strategy (E-Ciber), enacted by Decree No. 12.573/2025, which guides efforts to strengthen Brazil's national cybersecurity and resilience.

The strategy was developed based on the proposals of the National Cybersecurity Committee (CNCiber), composed of 25 members, including 16 government representatives and 9 from civil society.

Structured around four interconnected pillars, the E-Ciber promotes:

Actions to enhance protection and awareness among citizens and society, through formal and informal education initiatives for all ages;

The strengthening of the security and resilience of essential services and critical infrastructures, supporting ongoing digital transformation and mitigating risks;

Integration and cooperation among agencies and institutions, both within Brazil and internationally; and

Measures to safeguard national sovereignty and strengthen cybersecurity governance.

This is Brazil's second national cybersecurity strategy, incorporating third-generation features comparable to those of leading nations in the sector, aligning the country with the most advanced global practices, in line with a study by the Inter-American Development Bank (IDB).

The E-Ciber establishes 40 strategic actions, to be further developed in National Cybersecurity Plans, periodically updated by CNCiber. This document represents a significant step forward in cybersecurity, in the resilience of essential services and critical infrastructures, and in consolidating Brazil's digital sovereignty.

Institutional Security Office
Presidency of the Republic

TABLE OF CONTENTS

National Cybersecurity Strategy (E-Ciber) 2025

In 2023, the National Cybersecurity Policy (PNCiber) and the National Cybersecurity Committee (CNCiber) were established, involving representatives from government, academia, civil society, and the private sector. The objective was to improve the country's cybersecurity and cyber resilience, as well as to promote national and international cooperation in these fields.

It was CNCiber's responsibility to prepare the proposal that underpins this strategy, which seeks to chart the best course for achieving the objectives defined in the PNCiber. To this end, the Committee identified a set of priorities aimed at addressing Brazil's most urgent cybersecurity needs, ensuring more effective allocation of resources in the short and medium term, within a gradual and evolutionary process.

CNCiber is also responsible for risk management throughout the implementation of this public policy and, consequently, of the E-Ciber. The Committee envisions the creation of a national cybersecurity governance body, which will be tasked with coordinating actions and establishing mechanisms for regulation, oversight, coordination, and control in this field. This body will also cover the protection of essential services and critical infrastructures, as well as the management of significant cyber crises.

1 Global cyber landscape

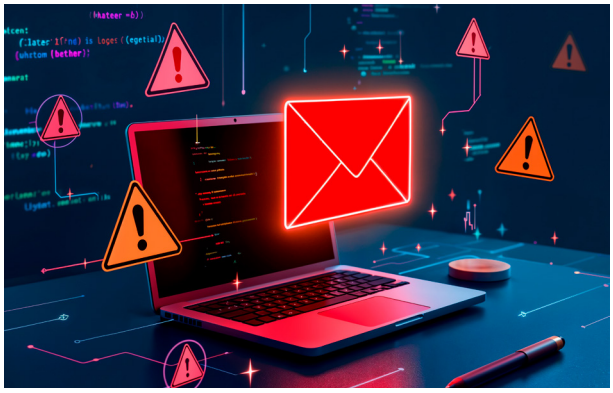
In January 2023, the World Economic Forum (WEF) presented its Global Risk Report, stating that "technology will exacerbate inequalities, while cybersecurity risks will remain a constant concern." The report also pointed out that cybercrime and cyber insecurity had become a new element among the top 10 global risks for the coming decade.

In January 2024, the WEF released an update of the report, which ranked cybersecurity as the 5th greatest global risk. It further indicated that worldwide losses resulting from cyber incidents could reach around 14% of global GDP. Projected onto Brazil's 2024 GDP, this corresponds to approximately 1.5 trillion reais.

In the 2025 edition, the report identified cyber espionage and cyber warfare as the fifth leading concern within a two-year horizon, likely influenced by heightened economic and political tensions and contemporary military conflicts.

As cyberspace emerges as a preferred arena for transnational crime and for geopolitical competition and friction, its offensive and defensive uses are increasingly integrated into the strategic calculations of states and non-state actors, with direct implications for the international order.

1.1 Threats



Cyber threats have the capacity to endanger a large number of individuals and organizations, including those that operate essential services and critical infrastructures, which play a central and highly sensitive role in society.

While socially pressing issues such as hunger, or limited access to electricity or sanitation, are typically addressed through investment and prioritization, the cyber domain involves motivated adversaries with varying resources and technical capabilities — requiring constant vigilance and action by the State.

The main types of threats against essential services and critical infrastructures include: phishing; large-scale denial-of-service attacks; ransomware; leaks of private or institutional information; cyber espionage; service interruptions; and Advanced Persistent Threats (APTs).

These malicious actions, perpetrated by both state and non-state actors, vary in scope, sophistication, and motivation. They may be driven by political, religious, military, economic, intelligence, sabotage, or purely criminal objectives.

Emerging technologies such as Artificial Intelligence and Quantum Computing are expected to make this scenario even more challenging, as these innovations enhance the capabilities of malicious actors.

The development of offensive cyber capabilities, depending on their scale, may have impacts comparable to kinetic attacks and decisively compromise national interests.

1.2 National context

In June 2022, the High-Risk List of Public Administration (LAR), published by the Federal Court of Accounts (TCU), reported that "in 2021, 73.1% of public services delivered by the federal government were fully digital, corresponding to 3,598 services." When partially digital services are taken into account, the percentage rises to 86.7%. The report emphasized: "These numbers alone demonstrate the scale of risks and the potential harm caused by security failures or service unavailability."

The 2024 LAR reported a 56% increase in cyber incidents affecting the Federal Public Administration, warning that "this raises concerns about the ability of public organizations to protect their (strategic and personal) data and maintain service delivery to Brazilian society." It further stressed that cybersecurity, self-determination, and the ability to economically, strategically, and technologically harness both personal and critical data constitute the three core dimensions of digital sovereignty.

Assessments of Brazil's cybersecurity maturity, conducted in 2020 and 2023 using the University of Oxford's Cybersecurity Maturity Model, showed that Brazil remains below the midpoint ("Established") across all criteria. While there was slight improvement in 50% of the items, 29% remained unchanged, and 21% worsened. Brazil moved from a 40% compliance rate in 2020 to 44% in 2023 — still insufficient for the country's digital exposure level.

For a society striving to improve quality of life through technological progress, these numbers are a clear warning, underscoring the urgency of investments and of adopting a consistent regulatory and normative framework. Moreover, cyber incidents significantly impact human rights, citizenship, the economy, and sustainable development.

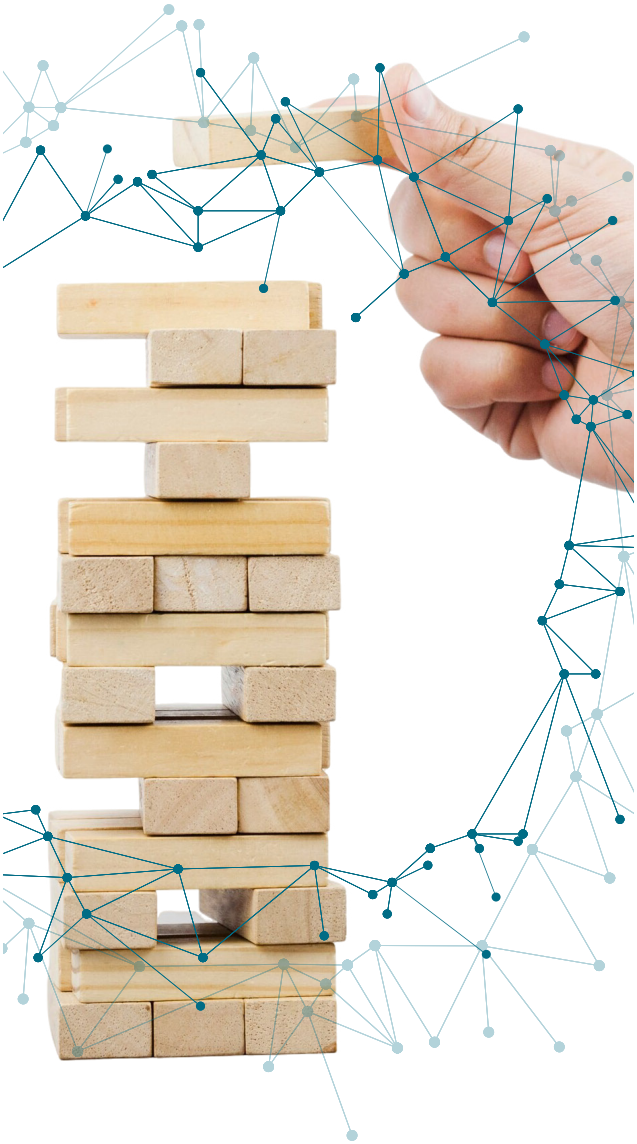
The 2024 Global Cybersecurity Index Report by the International Telecommunication Union (ITU) recognized Brazil's progress, citing the approval of the PNCiber, creation of CNCiber, and ratification of the Budapest Convention on Cybercrime, among other actions. The report positioned Brazil among the model countries in development in the areas of legal, technical, organizational, awareness and capacity-building measures, and international cooperation. Although the index does not measure capability implementation, these milestones reflect the growing maturity of the Brazilian State in this field.

In the face of cyber threats, organizations require means to identify, protect, respond to,

1.3 Challenges

and recover from incidents. Effective prevention and response demand situational awareness, cooperation, and coordination, ideally organized under a centralized command and control structure.

The primary challenge for Brazilian society in cybersecurity is to establish national coordination of actions — whether existing or planned — by different public and private actors, encompassing all levels and branches of government. This coordination must balance risks and pressing needs, while ensuring synergy in the use of limited human and material resources, thereby safeguarding the continuity and acceleration of Brazil's ongoing digital transformation.



It must also harness the opportunities of emerging technologies, such as the use of artificial intelligence and machine learning tools to analyze, identify, and respond to cyberattacks.

Another critical challenge is the scarcity of consistent and periodic national data and indicators that would allow proper diagnosis and monitoring of the cybersecurity landscape, tailored to Brazil's specific needs.

Additionally, greater awareness among public and private managers of the risks and threats of cyberspace is needed. Cybersecurity must be treated as a stabilizing factor of modern societies, an investment that ensures the proper functioning of all sectors of the economy and the continuity of business, minimizing the likelihood of incidents or disruptions of essential services.

The E-Ciber addresses these and other key issues, guiding the actions Brazil must take to become more secure and resilient against current and future threats, while benefiting from the opportunities that technology offers and integrating into the expanding global cybersecurity value chain.

The present strategy represents the second version of Brazil's national document on this

1.4 Evolution of E-Ciber

topic. In line with the findings of the 2024 Global Cybersecurity Index Report by the International Telecommunication Union (ITU), the evolution of national maturity can be inferred by analysing several key points, such as those presented in the table below. This table provides a comparative summary between the current E-Ciber and its predecessor:

TOPIC	E-Ciber 2020	E-Ciber 2025	DESCRIPTION OF IMPROVEMENT
Governance	Centralized governance proposal.	Governance integrated with national sovereignty as one of the four strategic pillars.	The new strategy proposes the development of regulation, inspection, coordination and control mechanisms.
National Technological Development	Generic Focus on the Cybersecurity Industry.	Specific incentive for national technologies, solutions, and reduction of technological debt.	Strengthens independence and reduces reliance on foreign technologies.
Inclusion and Diversity	Not addressed.	Inclusion of underrepresented groups (children, adolescents, the elderly, and neurodivergent).	The new strategy encourages the protection of vulnerable groups.
Cyber Maturity	Sporadic evaluation.	Clear goal of reaching the 'Established' level in all maturity requirements.	The improvement brings a structured monitoring of Brazil's evolution in cybersecurity.
Protection of Critical Services and Critical Infrastructure	Focus on general critical infrastructure.	Expanded to include essential services and their infrastructures.	Improves preparedness and resilience, with standards and certifications.
Support for SMEs and Startups.	Incentive to research and development.	Detailing mechanisms to encourage startups and SMEs.	The new strategy includes specific actions to create an innovative environment for small businesses.
International cooperation	Anticipated partnerships.	Intensification of partnerships and exchange with an emphasis on capacity building.	Expands joint cybersecurity capacity-building activities.
Education and Awareness	Awareness campaigns.	Development of a cybersecurity culture, with focus on managers.	The new strategy promotes a culture of cybersecurity that is sustainable and rooted in society.

TOPIC	E-Ciber 2020	E-Ciber 2025	DESCRIPTION OF IMPROVEMENT
Communication and Incident Response	Proposal to improve communication between sectors.	Promoting risk management and cyber incident protection and response.	The improvement favours a more agile and effective response, improving the ability to respond to cyber incidents.
Adoption of Emerging Technologies	Generic incentive.	Reduction of the country's technological debt in emerging and disruptive technologies.	The new strategy emphasizes the need for affirmative and incremental government actions to do so.
Extended Term	Term limited to a period of 4 years.	Indefinite validity, with short, medium, and long-term actions.	The new strategy considers and addresses issues with a broader horizon than the 4-year one, which constitutes a long-term strategy, adjusted through annual plans.

1.5 Objectives to be achieved

The effectiveness of the E-Ciber will be evaluated through progress made under the proposed Brazilian cybersecurity maturity model, which will serve as the baseline for the strategy.

The aim is for Brazil, within five years, to achieve at least the "Established" level across all maturity dimensions, without regressing in areas where it has already reached or exceeded this level.

The objectives of E-Ciber derive from those of the PNCiber:

- Ensure confidentiality, integrity, authenticity, and availability of hardware, software, and data used in electronic or digital information processing, storage, and transmission.
- Promote national sovereignty, prioritization of national interests, and due diligence in cyberspace.
- Encourage the adoption of cyber protection and risk management measures to prevent, avoid, mitigate, reduce and neutralize cyber vulnerabilities, attacks and incidents and their impacts.
- Develop education, culture and technical-professional training in cybersecurity in Brazilian society.
- Increase coordinated action and exchange of cybersecurity information between:

a) Union, states, Federal District and municipalities.

b) Executive, Legislative and Judiciary Branches.

c) private sector. and

d) society in general.

- Promote productive and technological autonomy in cybersecurity.
- To provide the national development of products, services and technologies aimed at cybersecurity.
- Intensify the fight against cybercrime.
- Implement collaboration strategies to develop international cooperation, and
- Foster scientific research, technological development, and innovation activities related to cybersecurity.

Thus, the strategy seeks to enable effective coordination nationwide in cybersecurity and cyber resilience, covering all government branches and levels, the private sector, and society as a whole, with special attention to essential services.

1.6 Expected benefits

2024 estimates from the World Economic Forum indicate that financial losses from cyber offenses in Brazil in 2024 may have reached 14% of global GDP (about 1.5 trillion reais, when projected for Brazil) with severe negative impacts on tax collection. Recent studies carried out specifically for Brazil indicate that this number may have reached 18% of the PID (something like 2.3 trillion reais). And this value grows every year.

It is expected that the implementation of E-Ciber will increase society's awareness, the preparation of institutions for prevention and resilience to cyber incidents, particularly regarding essential service providers and critical infrastructure operators, containing the evolution of losses and reducing the risk of interruption of relevant services that may generate instabilities in society.

The decree applies within the Federal Executive Branch and exerts an inductive and collaborative effect on other branches of government and on society at large.

2 Presentation

The E-Ciber 2025 was developed around four thematic pillars, which complement and support each other (Figure 1).

Figure 1

These thematic pillars group together a set of Strategic Actions, to be implemented through Strategic Initiatives that will be detailed in the National Cybersecurity Plan (P-Ciber), as established by the PNCiber.

2.1 Axis 1 – Protection and awareness of citizens and society

The protection and awareness of citizens and society aims to ensure the safe use of digital services, with special attention to people in vulnerable situations, such as children and adolescents, the elderly and neurodivergent people. To this end, the following strategic actions were prioritized:

- **Safe performance in cyberspace:** encouraging the adoption of responsible and safe behaviors by users when using digital tools, with the promotion of practices that reduce cyber risks.
- **Support for victims:** promotion of the expansion of support services for people affected by crimes and other illicit practices in the digital environment, with a focus on reception and guidance.
- **Identification and authentication:** encouragement of the use of user identification and authentication mechanisms according to the needs of each digital service, always respecting privacy.
- **Training of teachers and managers:** seeking the qualification of education professionals, both from the public and private networks, to enable them to teach topics related to cybersecurity.
- **Cybersecurity in education:** encouraging the inclusion of cybersecurity content in school curricula at all levels, promoting the formation of more digitally aware citizens.
- **Participation in forums and events:** integration of students, professionals and researchers in forums, congresses and technical activities focused on cybersecurity.
- **Guidance for small businesses:** provide micro and small enterprises and startups with guidance on cyber-risk management and post-incident recovery.
- **Flexible compliance plans:** evaluation of adaptable cybersecurity compliance models so that public agencies can implement them according to their reality.
- **Contingency planning and exercises:** encourage the development of institutional incident-response plans and the performance of tests and simulations to evaluate cybersecurity levels.
- **Combating cybercrime:** promoting integrated action between different sectors of society to prevent and combat digital crimes, fraud, and other threats in cyberspace.
- **Dissemination of international instruments:** publicize the Convention on Cybercrime (Budapest Convention) and other national and international instruments in force in Brazil.

- **Actions against cybercrime:** support for initiatives that increase the effectiveness of cybercrime operations by improving investigations and responses.
- **Notification channels:** encouragement of the legal and technical improvement of the structures available for reporting cybercrimes, aiming to make them more accessible and effective.
- **Capacity-building for law-enforcement bodies:** promote continuous training for professionals in institutions responsible for investigating and suppressing cybercrime, improving their operational capacity.

2.2 Axis 2 – Security and resilience of essential services and critical infrastructures

This pillar seeks to provide effective tools to prevent and respond to cyber incidents, through the following strategic actions:

- **Promotion of risk management by regulators:** encouragement for entities with regulatory functions to promote the management of cyber risks and adopt measures to protect and respond to cyber incidents in their respective sectors.
- **Strengthening regulation and control:** development of regulatory, inspection, coordination, and control mechanisms to ensure the security, resilience, and continuity of essential services, with a special focus on the safe use of information and operational technologies.
- **Risk alert mechanisms:** adoption of alert systems that warn of relevant risks in the provision of digital services, enabling quick and effective responses.
- Cybersecurity high-risk list: creation and maintenance of a high-risk list that serves as a basis for sectoral cyber risk management**.**
- **Minimum standards for sensitive data:** encouraging the definition and adoption of minimum cybersecurity standards for the protection of relevant and sensitive data, especially in critical contexts.
- **National cybersecurity seal:** institution of a national certification seal to indicate the level of security of cyber assets, providing greater reliability to certified products, services and systems.
- **Cyber incident insurance:** incentive for essential service providers and critical infrastructure operators to increase their resilience measures, such as taking out specific insurance to cover damages resulting from cyber incidents.

- **Exercises and simulations:** promotion of periodic exercises and simulations, both in specific sectors and in multisectoral contexts, with the aim of testing and strengthening the cyber resilience of essential services.
- **Continuous regulatory improvement:** encouragement for the constant updating of regulations related to cybersecurity, including the definition of minimum control standards and the preparation of technical guides.
- **Security in data interoperability:** seeking to strengthen security in the exchange and sharing of data between systems, as well as in the digital channels used for the provision of services.
- **Support for Brazilian companies:** incentives for national companies to seek and use products and services that are aligned with minimum cybersecurity standards, promoting a safer digital ecosystem.

2.3 Axis 3 – Cooperation and integration between public and private bodies and entities

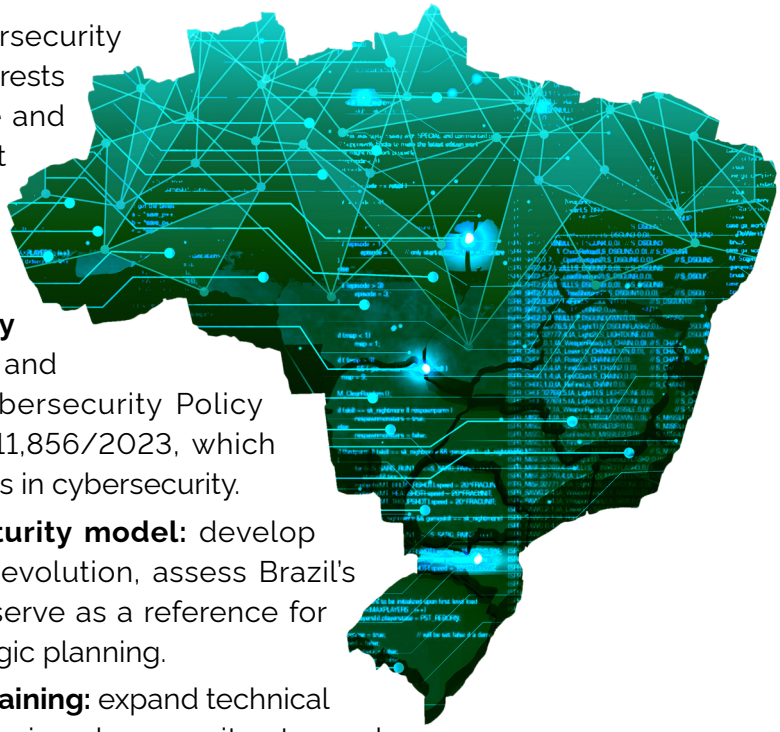
This pillar promotes debate and information-sharing on cybersecurity at the national and international levels, based on the following strategic actions:

- **Creation of specialized cybersecurity structures:** foster the establishment of computer security incident prevention and response teams, essential for rapid action amid growing cyber threats; promote Information Sharing and Analysis Centers (ISACs) to enable coordinated responses; and encourage the establishment of specialized laboratories capable of conducting tests, research, and development in cybersecurity.
- **National cyber-incident reporting:** create a unified mechanism for reporting cyber incidents nationwide, facilitating rapid response, threat mapping, and coordination between public and private actors.
- **Cooperation with academic institutions and agencies:** strengthening relationships of trust and collaboration between academic institutions and national and international agencies, seeking the development of joint cybersecurity and cyber defence actions,

fostering the sharing of information and experiences, promoting the coordinated disclosure of vulnerabilities, and acting to combat cybercrimes and other illicit activities in the digital environment.

- **Strengthening cybersecurity in neighbouring countries:** support for expanding the cybersecurity capacity of countries in Brazil's strategic surroundings, through bilateral or multilateral initiatives, with the aim of promoting regional stability and cybersecurity.
- **Brazil's international participation:** encouragement of Brazil's active presence in international forums and organizations focused on cybersecurity, favouring the exchange of experiences, the definition of good practices, and alignment with global digital protection standards.

2.4 Axis 4 – National sovereignty and governance



National sovereignty and cybersecurity governance aim to protect the interests of Brazilian society in cyberspace and ensure a reliable digital environment that favours Brazil's economic and technological growth, based on the following strategic actions:

- **National Cybersecurity Policy:** update, disseminate, and implement the National Cybersecurity Policy established by Decree No. 11,856/2023, which guides Brazil's strategic actions in cybersecurity.
- **National cybersecurity maturity model:** develop a model to measure sector evolution, assess Brazil's cybersecurity maturity, and serve as a reference for adjustments to national strategic planning.
- **Technical and professional training:** expand technical training and capacity-building in cybersecurity at a scale commensurate with national demand, preparing qualified professionals to serve all sectors of the economy.
- **Reducing technological debt:** pursue affirmative and incremental actions to reduce external dependency on emerging and disruptive technologies, strengthening the national technological base.
- **Security conformity assessment:** encourage the development of capabilities to continuously assess the security conformity of cybersecurity-related products, services, and technologies, increasing the reliability and quality of solutions used in the country.
- **Secure information exchange systems:** encouraging the use of secure systems for sharing sensitive information in the field of cybersecurity, promoting greater data protection and integrity.
- **Incentives for the private sector:** support the private sector in creating and offering cybersecurity products, services, and technologies, with special attention to micro and small enterprises and startups.

- **Partnerships with research institutes:** foster partnerships with Brazilian research and development institutes to strengthen national scientific and technological output in cybersecurity, including technology residencies (supervised placements in cybersecurity topics).
- **Research lines and scholarships:** promote research lines in undergraduate and stricto sensu graduate programs, and grant scholarships to train Brazilian specialists and faculty in cybersecurity.
- **Development of national solutions:** incentive to the production of national products, services and technologies that contribute to the improvement of cybersecurity in Brazil, reducing external dependence and promoting local innovation.

2.5 The National Cybersecurity Plan (P-Ciber)

As a national strategy, E-Ciber has an open-ended time horizon and establishes that its Strategic Actions will be translated into short- and medium-term Strategic Initiatives, which will be incorporated into the National Cybersecurity Plan (P-Ciber). The P-Ciber will be updated annually or biennially, drafted by CNCiber and approved by the Institutional Security Office of the Presidency of the Republic (GSI/PR), following the concurrence of the government representatives sitting on the Committee. The Plan will detail the strategic initiatives, including their implementation schedule and corresponding governance arrangements.

Credits

Luiz Inácio Lula da Silva
President of the Federative Republic of Brazil

Geraldo Alckmin
Vice President

Marcos Antonio Amaro dos Santos
Minister of State, Chief of the Institutional Security Office of the Presidency of the Republic

Washington Rocha Triani
Executive Secretary of the GSI/PR

Lincoln Bernardes Júnior
Deputy Executive Secretary

Office for Information and Cybersecurity

André Luiz Bandeira Molina
SSecretary for Information and Cybersecurity

Luiz Fernando Moraes da Silva
Director, Department of Cybersecurity

Danielle Ayres
Director, Department of Information Security

Marcelo Antonio Osller Malagutti
Special Advisor to the Minister

Advisory Staff

Marco Aurélio de Andrade Lima
Chief of Staff to the Minister

Col. (Brazilian Army) R/1 Sergio Martins Rocha
Chief Military Advisor

Social Communication

Heron Clementino de Andrade
Chief, Special Advisory Office for Social Communication, GSI/PR

Editorial Layout
1st Lt. (Brazilian Army) Djalma Martins

Drafting, text revision and translation
Marcelo Antonio Osller Malagutti
Carlos Eduardo de Souza Gomes Fonseca
Maj (Brazilian Army) Mayara Azeredo Alves
First Secretary Reynaldo Collares


COMITÊ NACIONAL DE CIBERSEGURANÇA
CNCIBER