Brazil Cybersecure 2025: Building a Trustworthy Digital Future

This document presents the proposal for the second international meeting on Brazil's role in Cybersecurity.

1.PLANNING

1.1 Date:

October 29–30, 2025

1.2 Venue

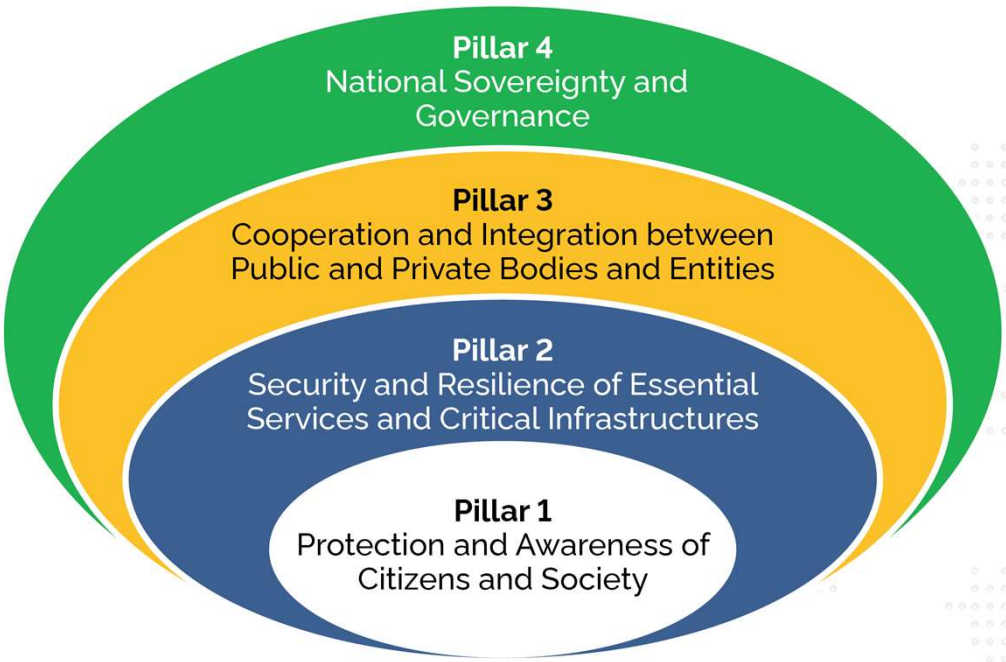
The meeting will be held at the Superior School of Defense (ESD) in Brasília, Federal District

1.3 Theme

1.3.1 Central Theme

"Brazil Cybersecure 2025: Building a Trustworthy Digital Future"

The event aims to bring together national and international experts to discuss current cybersecurity issues, organized into panels of up to four participants (moderator and panelists), with a focus on the thematic pillars of the new National Cybersecurity Strategy (E-Ciber):



1.4 Format

1.4.1 Conception

The event is structured around the four thematic pillars of the National Cybersecurity Strategy (E-Ciber). Each thematic pillar will comprise at least two panels, with topics defined according to the strategic actions of each pillar. Each panel will be moderated by a member of the National Cybersecurity Committee (CNCIBER).

The selection of panelists was guided by the relevance of their professional background to the subject matter of each panel. An effort was made to diversify the participating institutions in comparison with 2024.

Each panel will include up to **four** participants, consisting of up to **three** panelists and **one** moderator.

1.4.2 Schedule

- ✓ The meeting will take place over two days, October 29 and 30, 2025.
- ✓ On October 29, the event will begin at 8:00 a.m. and conclude at 5:15 p.m.
- ✓ On October 30, the event will begin at 8:45 a.m. and is scheduled to conclude at 5:15 p.m.
- ✓ Each panel will last 50 minutes, with a 10 minute tolerance, and 15-minute break.

1.4.3 Capacity

The event is being planned for 300 participants.

1.4.4 Target Audience

Primarly:

- ✓ Public servants from the Executive, Legislative, and Judiciary branches
- ✓ Indirect public administration and state-owned enterprises
- ✓ Academia and research institutions
- ✓ Organized civil society
- ✓ Professional associations and representative chambers
- ✓ Defense and public security institutions.

1.4.5 Modality

In-person, with recording and simultaneous interpretation in Portuguese, Spanish, and English.

Agenda

Day 1 – 10/29/2025

08:00 - 09:00	**Registration**
09:00 - 10:30	**Opening Session**
10:30 – 10:45	**Signing of Agreements and Memoranda of Understanding**
10:45 – 11:00	**Coffee Break**

Pillar 4: National Sovereignty and Governance

11:00 – 11:50	**PANEL 1 – Governance Structures of Nations** This panel aims to discuss the governance structures of different countries, highlighting the main advantages and limitations of each model. The objective is to analyze international best practices and understand the coordination among various actors, the definition of cybersecurity responsibilities, and the balance between regulation, digital sovereignty, and international cooperation. Based on this discussion, the panel seeks to explore pathways to strengthen cybersecurity governance in the Brazilian context. Moderator: André Luiz Bandeira Molina – CNCIBER – Brazil P1: Edward Chen – Singapure P2: Kamoshita Makoto – Japan P3: Daniel Alvarez – Chile
12:00 – 13:30	**Lunch**

Agenda

Pillar 4: National Sovereignty and Governance

13:30 - 14:20	**PANEL 2 – Evolution of Cybersecurity Maturity** In recent years, Brazil has demonstrated progress in the development of a normative framework for cybersecurity. However, there are still elements to be developed to position the country at the highest levels in the field. This panel will therefore reflect on the current stage of Brazil's cybersecurity maturity, its institutional challenges, and potential pathways to consolidate sovereign and sustainable cyber capabilities. Moderator: Santiago Paz – IDB P1: Leonardo Rodrigo Ferreira – SGD (DIGITAL GOVERNMENT SECRETARIAT) – Brazil P2: Julio Marinho – CODATA – GTD (DIGITAL TRANSFORMATION GROUP) – Brazil P3: Carlos Renato Braga – TCU (FEDERAL COURT OF ACCOUNTS) – Brazil
14:30 – 14:45	**Coffee Break**

Pillar 4: National Sovereignty and Governance

14:45 - 15:35	**PANEL 3 – Cyber Sovereignty and Emerging Technologies** The assertion of sovereignty in cyberspace has become a strategic issue for states in light of the rapid evolution of emerging technologies. Discussions on sovereign cloud, the dominance of emerging technologies by a small number of powers, generative artificial intelligence, and quantum technologies are at the top of the agenda in a series of initiatives worldwide. This panel aims to discuss the necessary steps to develop policies and capabilities that ensure autonomy in these strategic areas, and how the public and private sectors can cooperate within this digital ecosystem. Moderator: Hamilton José Mendes da Silva – CNCIBER – Brazil P1: Eduardo Peixoto – CESAR Institute – Brazil P2: Ulrich Ahle – GAIA X – Germany P3: Vanderson Rocha Covre – CEPESC – Brazil
15:45 – 16:00	**Coffee Break**

Agenda

Pillar 4: National Sovereignty and Governance

16:00 - 16:50	**PANEL 4 – Perspectives on Regional Sovereignty** In the pursuit of asserting sovereignty in cyberspace, regional cooperation plays a particularly relevant role. The exchange of knowledge and experiences, as well as the coordination of positions with our neighbors — with whom we share many common challenges and priorities — represents a strategic asset for advancing our interests at the international level. MERCOSUL, in particular, with its legal and institutional framework and the recent establishment of the Cybersecurity Commission, constitutes a privileged forum for the promotion of regional sovereignty. Moderator: Ambassador Carlos Márcio Bicalho Cozendey – MRE – Brazil P1: Ariel Waissbein – Argentina P2: Carlos Leonardo – Dominican Republic P3: Fabiana Santellan – Uruguay
17:00 – 17:15	**Closing of the first day** Closing of the Discussions - Representative of IDB

Agenda

Day 2 – 10/30/2025

08:45 - 09:00	**Day 1 recap** GSI

Pillar 3 – Cooperation and Integration between Public an Private Bodies and Entities

09:00 – 09:50	**PANEL 5 – Information Sharing as a Mechanism for Collective Cybersecurity** Cybersecurity information sharing has become an established international practice for promoting trust and multi-sector cooperation. In this context, ISACs (Information Sharing and Analysis Centers) are also being effectively supported by GSI to strengthen national cybersecurity. This panel proposes to explore the role of information-sharing mechanisms as a means to build trust, exchange intelligence, and enable coordinated responses to cyber incidents among government, private sector, and academia. Moderator: Rony Vainzof – CNCIBER – FIESP – Brazil P1: Tod Eberle – Shadowserver – USA P2: Leandro Ribeiro – ABCIS – Brazil P3: Minhye Sofia Park – South Korea
10:00 – 10:15	**Coffee Break**

Agenda

Pillar 3 – Cooperation and Integration between Public an Private Bodies and Entities

10:15 – 11:05	**PANEL 6 – Trust-Building Networks – National and Subnational** The development of integrated and trusted networks to address complex cyber challenges at the national and subnational levels is now a reality. In this context, Brazil, through ReGIC (Integrated Cybersecurity Management Network), stands out as an example of maturity in this field, currently integrating approximately 160 members, including federal, state, and municipal organizations, public companies, and other key national actors. This panel aims to discuss initiatives of this kind and understand their importance in building a more robust cybersecurity ecosystem capable of agile incident response. Moderator: Martina Berguer – IDB P1: Loriza Andrade Vaz de Melo – SGD (DIGITAL GOVERNMENT SECRETARIAT) – Brazil P2: Lilian Santos – GTD (DIGITAL TRANSFORMATION GROUP) – Brazil P3: Natan Santos – CTIR Representative of Salvador City Hall – Brazil

Pillar 2 – Security and Resilience of Essential Services and Critical Infrastructures

11:15 - 12:05	**PANEL 7 – Regulation as a Factor for Enhancing Resilience and Regulatory Harmonization** Regulation is a central element for strengthening the resilience of essential services and critical infrastructure. This panel will discuss how consistent and coordinated regulatory frameworks contribute to the prevention, response, and recovery from cyber incidents. The debate will also address the challenges of regulatory harmonization across sectors and countries, promoting the exchange of best practices and the role of the state as a facilitator of effective and sustainable cybersecurity regulations at both national and regional levels. Moderator: Counselor Edson Holanda – ANATEL – Brazil P1: Werllen Lauton Andrade – ANAC – Brazil P2: Arthur Pereira Sabbat – ANPD – Brazil P3: Adriana Drummond Vivan – ANEEL – Brazil
12:05 – 13:30	**Lunch**

Agenda

Pillar 2 – Security and Resilience of Essential Services and Critical Infrastructures

13:30 - 14:20	**PANEL 8 – Best Practices for Essential Services and Critical Infrastructure** The protection of essential services and critical infrastructure is a strategic challenge involving multiple sectors and levels of government. This panel will discuss the best practices adopted, including cybersecurity strategies and protocols developed by operators of essential services and critical infrastructure, as well as the advancements brought to this area by the National Cybersecurity Policy (PNCiber), the National Cybersecurity Strategy, and the National Information Security Policy (PNSI). Moderator: Luiz Fernando Moraes da Silva – SSIC/GSI/PR – Brazil P1: Rene Summer – ICC P2: Everton Schonardie Pasqual – Itaipu – Brazil P3: Ana Estela Haddad – MS/SSD – Brazil
14:30 – 14:45	**Coffe Break**

Pillar 1 – Protection and Awareness of Citizens and Society

14:45 – 15:35	**PANEL 9 – Cybercrime and Its Implications: Challenges and Strategies for Building a Secure Digital Environment** Societal concern about cybercrime is growing, often manifesting as financial crimes, prompting the state to protect individuals and support victims of such criminal activities. The discussion on promoting integrated actions for prevention, response, and effective enforcement against illicit practices—such as financial fraud, money laundering, digital identity theft, cyber espionage, among other cybercrimes—should be a priority for both the state and society. This panel aims to understand contemporary challenges in developing integrated strategies, encompassing digital literacy, improved legal frameworks, accessible and effective reporting channels, interinstitutional cooperation, and social awareness to strengthen a culture of integrity and promote solutions that mitigate the human, financial, and social impacts of cybercrime. Moderator: Valdemar Latance Neto – PF/MJSP – Brazil P1: Luciano Kuppens – National Council of Justice (CNJ) – Brazil P2: Leandro Volochko – MP/MT – Brazil P3: Walter Faria – Representative of Brazilian Federation of Banks (FEBRABAN) – Brazil

Agenda

15:45 – 16:00	**Coffe Break**

Pillar 1 – Protection and Awareness of Citizens and Society

16:00 - 16:50	**PANEL 10 – Cyber Education and Cyber-Risk Literacy** The omnipresence of technology in our daily lives, both for individuals and organizations, requires not only digital literacy but also literacy regarding the risks that technologies may pose, including the potential threats they can introduce. This panel will discuss the major barriers that society faces in understanding the threats of digital life. Moderator: Danielle Ayres – SSIC/GSI/PR – Brazil P1: Thaís Vanconcelos Batista – Brazilian Computer Society (SBC) – Brazil P2: Raul Amarelle Valera – INCIBE – Spain P3: Emílio Nakamura – Rede Nacional de Ensino e Pesquisa (RNP) – Hackers do Bem – Brazil
17:00 – 17:15	**Closing - GSI and IDB**