Brazil

Last Updated: October 2021

CYBERSECURITY POLICY

Strategy Documents

Estratégia Nacional de Segurança Cibernética (National Cybersecurity Strategy) (E-Ciber), 2020-2023

President of the Republic

- 10 Strategic Steps
- Recommendations focus on:
  - Cyber governance programs;
  - National encryption systems;
  - Anti-piracy policies;
  - Cybersecurity requirements in public sector contracts;
  - Digital certification use;
  - Education of the public on cybersecurity;
  - Measures for handling restricted information.

Source

February 2020

Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0 (Information and Communications Security and Cyber Security Strategy 2015/2018)

Government of Brazil

Principles include:

- Establishing a central body and a national system, aiming to coordinate, monitor and evaluate the implementation and execution of national policies in information and communications security and cybersecurity;
- Improving and updating the legal framework in the areas of information and communications security, and cybersecurity;
- Increasing the resilience of information assets and critical infrastructures.

Source Source 2

2015

Livro Branco de Defesa Nacional (Defense White Paper)

Ministry of Defense

- Cyber identified as a fundamental strategic sector for national defense;
- Efforts in the cyber sector aim to ensure confidentiality, availability, integrity and authenticity of data circulating in Brazil's networks, which are processed and saved;
- The Army Center for Cyber Defense is adding efforts to those of other existing government organizations, including through protection against cyber attacks;
- The Navy Research Institute is responsible for the development of technologies necessary for the Navy, in particular in the area of cyber warfare;
- Priority projects include one related to cyber defense with, inter alia, the construction of the permanent headquarters of the Cyber Defense Center and the acquisition of the supporting infrastructure, and acquisition of cyber defense hardware and software solutions (to be implemented in 2010-2023).

Source

2012

Estratégia Nacional de Defesa, Decree N. 6.703 (National Defence Strategy)

President of the Republic

- Cyber identified as one of the three fundamental sectors for national defence of strategic importance;
- The Brazilian Navy to gain autonomy in cyber technologies that guide submarines and their weapons systems, and enable them to work in network with other naval, land and air forces;
- Enhanced cyber capabilities through the development of cyber training in industrial and military fields;
- Intensified strategic partnerships in cyber with States, in particular the Community of Portuguese Language Countries (Comunidade de Países de Língua Portuguesa).

Brazil

Last Updated: October 2021

Source

18 December 2008

STRUCTURE

National Centre or Responsible Agency

Comando de Defesa Cibernética, ComDCiber (Cyber Defense Command)
Ministry of Defense

- Unit within the Brazilian Army;
- Composed by representatives from all armed forces;
- Responsible for planning, coordinating, directing, integrating and supervising cyber operations in the defense area.

Source Source 2

2016

Key Positions

Head
Comando de Defesa Cibernética, ComDCiber (Cyber Defense Command)

Source

Head
Centro De Defesa Cibernética (Cyber Defense Center)

Source

Dedicated Agencies and Departments

Centro de Defesa Cibernetico (CDCiber) (Cyber Defense Center)
Ministry of Defense

- Part of the Cyber Defense Command.

Source

Federal Police's Unit for Combating Cybercrime (URCC)
Federal Police of Brazil

- Law enforcement agency responsible for preventing and responding to cybercrime;
- Competencies range from the investigation of crimes against federal public institutions to infactions with inter-state and international ramifications.

Source

Departamento de Segurança da Informação (Department of Information Security)
Institutional Security Cabinet (Gabinete de Segurança de Informações)

Source

Brazil

Last Updated: October 2021

National CERT or CSIRT

CTIR Gov

Department of Information and Communications Security (Departamento de Segurança de Informações e Comunicações)

Services of CTIR Gov include:

- Incident analysis;
- Incident response support;
- Coordination in response to incidents.

Source

2004

LEGAL FRAMEWORK

Legislation

Law No. 12.965, Marco Civil da Internet

Establishes principles, guarantees, rights and obligations for the use of the Internet in Brazil, and provides guidelines for the actions of the Union, the States, the Federal District and the municipalities in this regard.

Source

23 April 2014

Criminal Code

Article 154-A: Unauthorised access to a computer device connected or not connected to a network, in order to obtain, tamper or destroy data or information without the explicit or tacit authorization of the device owner; or in order to obtain illegal advantage.

Source

Views on International Law

Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266

The Group of Governmental Experts established pursuant to the he General Assembly resolution 73/266, adopted its report by consensus on 28 May 2021. In paragraph 73 of the Group's report (A/76/135), it is stated that, in accordance with the Group's mandate, an official compendium of voluntary national contributions of participating governmental experts on the subject of how international law applies to the use of ICTs by States will be made available on the website of the Office for Disarmament Affairs.

Source

July 2021

COOPERATION

UN Processes

Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

Brazil

Last Updated: October 2021

2004, 2009, 2014/2015, 2016/2017, 2019/2021

Expressed Views at the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Source Source 2

2019/2020

Bilateral and Multilateral Cooperation

Bilateral Cooperation on Cyber and Internet Policy, US-Brazil

Director of the Department of Science, Technology, and Innovation at the Ministry of External Relations; Secretary for Digital Policy at the Ministry of Science, Technology, Innovation, and Communications

- Agreed to explore a series of technical exchanges and conduct consultations to share best practices on data protection, cross border data flows, ICT procurement, international security in cyberspace, cybersecurity, and military and law enforcement cooperation.

Source

14 May 2018

Cooperation, Europol-Brazil

Strategic agreement to cooperate in combatting cybercrime and other cross-border criminal activities.

Source

April 2017

German-Brazilian cyber consultations

Bilateral consultations between government representatives, high-level representatives of business, academia, civil society.

Source

22-23 February 2016

16th Meeting of the Joint Committee, Framework Agreement for Cooperation, Brazil-EU

Ministry of External Relations

Released a final communiqué, welcoming the future establishment on a Brazil-EU dialogue on international cyber policy.

Source

28 April 2015

Cyber cooperation, Argentina-Brazil

Agreement on bilateral cyber security meeting, cyber warfare training, and creation of a bilateral organization aimed at analyzing cyber defense cooperation actions

Source

12-13 September 2013

Cooperation, Brazil-Turkey

Ministry of Defense

Creation of five working groups to study partnerships in different sectors, including in cyber defense.

Source

22 August 2013

Brazil

Last Updated: October 2021

Memorandum of Understanding, Indo-Brazil-South Africa (IBSA) Forum

Framework for cooperation on the Information Society

Source

13 September 2006

Membership

- **International Telecommunications Union (ITU)**
- **Organization of American States (OAS)**
- **United Nations (UN)**