



## CYBERSECURITY POLICY

### ✓ Strategy Documents

#### National Cybersecurity Policy (2017-2022)

Government of Chile

- Identifies public policy measures for 2017-2018, and identifies the national standards and institutions involved in cybersecurity,
- Provides a risk and threat overview;
- Identifies the following policy objectives to reach by 2022:
  1. Robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach;
  2. Protection of people's rights in cyberspace;
  3. Development of a cybersecurity culture based on education, good practices and accountability in the management of digital technologies;
  4. Cooperation actions with other stakeholders in the field of cybersecurity and active participation in international forums and discussions;
  5. Promoting the development of a cybersecurity industry serving its strategic objectives.

[Source](#) [Source 2](#)

2017

#### Libro de la Defensa Nacional

Ministerio de Defensa Nacional

Chile's sovereignty in cyber space must be protected, using the Tallinn Handbook 2.0 as a template.

[Source](#)

2017

### ✓ Implementation Frameworks

#### Digital Agenda for 2020

Government of Chile

- Roadmap designed to guide the country's digital development through the definition of objectives, courses of action and measures;
- Measure 25 focuses on developing a cybersecurity policy.

[Source](#)

2015

## STRUCTURE

### 🌐 National Centre or Responsible Agency

#### Interministerial Committee on Cyber Security (Comité Interministerial sobre Ciberseguridad)

- Created by the Supreme Decree No. 533/2015;
- Proposed the National Cybersecurity Policy.

[Source](#)

2015

### 🌐 Key Positions



## Chile

Last Updated: February 2022

### Chair

Interministerial Committee on Cybersecurity

Undersecretary of the Interior

[Source](#) [Source 2](#)



### Dedicated Agencies and Departments

#### Investigations Policy, Cybercrime Investigation Brigade

Office of the Prosecutor

Responsible for investigating crime under the direction of the Office of the Prosecutor, including cybercrime.

[Source](#)



### National CERT or CSIRT

#### CSIRT

Ministry of the Interior and Public Safety

- Providing information and assistance to the Government's Cyberspace and the State's connectivity network;
- Administering a system of national and international cooperation in matters of cybersecurity;
- Promoting the strengthening of the legal framework in relation to Computer and Cybercrime crimes.

[Source](#) [Source 2](#)

## LEGAL FRAMEWORK



### Legislation

#### Law No. 19.223

Ministry of Justice

- Sub-category in the field of cybercrime related with the disturbance of the logical components of cyberspace called computer-related crimes;
- Sets out specific criminal definitions describing non-authorised access, theft and destruction of information systems.

[Source](#) [Source 2](#)

28 May 1993

#### Law No. 19.628

Ministry General Secretariat of the Presidency

- Law on the protection of private life;
- Sets out a series of principles and rights related to the management of personal data.

[Source](#) [Source 2](#)

6 August 1999

#### Law No. 18.168

Ministry of Transport and Telecommunications



## Chile

Last Updated: February 2022

- General Telecommunications Law, providing key physical and logical infrastructure for the national cyberspace;
- Sets out the protection, confidentiality and integrity of the information through the criminalisation of offences related to non-authorised interception;
- Ensures the principle of network neutrality.

[Source](#) [Source 2](#)

15 September 1982

### Criminal Code

- Article 135 §4: Unauthorised access to information contained in another's computer;
- Article 144: Destruction or alteration of computer programs or data.

[Source](#)

## COOPERATION



### Multilateral Agreements

#### Budapest Convention

PARTY

[Source](#)

1 August 2017 (entry into force)



### UN Processes

#### 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

#### U.S.-Chile Cyber Threats Cooperation Agreement

Defense Minister

Enhance defense and cooperation, specifically on cyber operations and protection of Chile's cyber domain

[Source](#) [Source 2](#)

16 August 2018

#### Agreement, Ecuador-Chile

President

Cooperation in issues related to defence, including cyberdefence and cybersecurity.

[Source](#)

30 October 2017

#### Resolution on Working Group on Cooperative and Confidence Building Measures for Cyberspace, Inter-American Committee against Terrorism

Presented by Chile, Colombia, Perú, Costa Rica, Canada, Guatemala and Mexico



## Chile

Last Updated: February 2022

Prepare a set of draft confidence-building measures, based on UN GGE reports to enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs

[Source](#)

10 April 2017

### Potential cooperation, Chile-Ukraine

National Defence Ministry

- Expression of interest in establishing defense cooperation during the LAAD 2017 Defence & Security exhibition in Rio de Janeiro (Brazil) by Ukraine;
- Cybersecurity among the main topics of cooperation.

[Source](#)

April 2017

### OAS Cyber Security Initiative (co-sponsor)

- Argentina, Chile, Mexico, and Estonia as co-sponsors
- Addresses cyber security issues based on a flexible and dynamic approach, in which cyber security policies and the provision of technical training are adapted to new trends and evolving needs

[Source](#)

16 April 2015

### Global Forum on Cyber Expertise, Member

A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building

[Source](#)

2015 (established)

### Chile - the UK; Memorandum of Understanding (MoU) on Cybersecurity

Chile's Treasury Minister and the UK's Minister of State at the Foreign and Commonwealth Office and the Department for International Development

- The MoU enables mutual cooperation on matters of cybersecurity and defense.

[Source](#)

10 September 2019



## Membership



**International Telecommunications  
Union (ITU)**



**Organization of American States (OAS)**



**United Nations (UN)**