Colombia

Last Updated: April 2020

CYBERSECURITY POLICY

Strategy Documents

National Digital Security Policy (CONPES 3854) (Política Nacional de Seguridad Digital)

The National Council of Economic and Social Policy of the Government of Colombia (Consejo Nacional de Política Económica y Social República de Colombia)

Defines five core areas of action, comprising Action and Follow-up Plan (Annex A):

1. Establishment of a clear institutional framework around digital security;
2. Creation of conditions allowing stakeholders to manage digital security risk in their activities;
3. Strengthen the security of individuals and the State in a digital environment at national and transnational levels;
4. Strengthening national defense and security with a risk-management approach;
5. Creation of permanent mechanisms to promote cooperation, collaboration and assistance in digital security.

Source

11 April 2016

Policy Guidelines on Cybersecurity and Cyberdefense (CONPES 3701) (Lineamientos de política para la Ciberseguridad y Ciberdefensa)

The National Council of Economic and Social Policy of the Government of Colombia (Consejo Nacional de Política Económica y Social República de Colombia)

Defines three specific objectives:

1. Implement appropriate mechanisms to prevent, provide assistance, control, and offer recommendations on cyber incidents and/or emergencies for protecting critical infrastructure;
2. Design and execute specialized cybersecurity and cyberdefense training plans; and
3. Strengthen the legal framework and law enforcement.

Source Source 2

14 July 2011

STRUCTURE

Key Positions

Commander, Joint Cyber Command (Comandante, Comando Conjunto Cibernético)

Source

Dedicated Agencies and Departments

Joint Cyber Command (Comando Conjunto Cibernético)

General Command, Military Forces

- Established by CONPES 3701, strengthened by CONPES 3854;
- Tasked with strengthening the technical and operational capabilities of the country to enable it to confront computer threats and cyber attacks through the implementation of protection measures, as well as introduction of cyberdefense protocols;
- Protects critical infrastructure, reducing the computer risks to the country's startegic information;
- Tasked with developing neutralization and response capabilities for dealing with computer incidents and attacks against the country's security and defense.

Source Source 2

Colombia

Last Updated: April 2020

Colombian Police Cybercenter (Centro Cibernético Policial)
Ministry of Defense, National Police of Colombia

- In charge of cybersecurity in Colombian territory, offering information, assistance and protection against cybercrime;
- Activities include prevention, assistance, investigation, and prosecution of computer crime in the country;
- Has a cybercrime observatory (observatorio cibercrimen).

Source Source 2

National CERT or CSIRT

ColCERT
Ministry of National Defense

- Responsible for coordination in cybersecurity and cyberdefense actions for the protection of Colombia's critical infrastructure in case of emergencies that threaten or compromise national security and defense;
- Develops and promotes procedures, protocols and guides on good practices and recommendations on cyberdefense and cybersecurity for critical infrastructures, and ensures their implementation and compliance.

Source

In Progress or Proposed

Cybersecurity and Cyberdefense Directorate (Dirección de Ciberseguridad y Ciberdefensa)
Deputy Minister of Defense for Policy and International Affairs (Viceministerio de Defensa para las Políticas y Asuntos Internacionales)

- Announced in the National Digital Security Policy (CONPES 3845, pp. 51-52);
- Would be responsible for the reporting of digital incidents, and guarantee the participation of stakeholders in digital security risk management.

Source

National Digital Security Coordinator (coordinador nacional de seguridad digital)
National Planning Department (Departamento Nacional de Planeación)
COMPES 3845 orders the nomination of a National Digital Security Coordinator by December 2016 in the Departamento Nacional de Planeación.
Source

LEGAL FRAMEWORK

Legislation

Decree 1704

Decree on the legal interception of communications.

Source

2012

Resolution No. 76434 of the Superintendence of Industry and Commerce (Superintendencia de Industra y Comercio)
Ministry of Trade, Industry and Tourism

Resolution on personal data protection.

Colombia

Last Updated: April 2020

Source

2012

Law 1621

Republic Congress

Establishes the basic framework for data protection, disclosure and reporting of security violations.

Source

2013

Criminal Code

- Article 192: Unlawful interception of communications;
- Article 269A: Illegal access to an information system;
- Article 269B: Illegitimate obstruction of information systems or telecommunication networks;
- Article 269C: Data interception;
- Article 269D: Unauthorised destruction, damaging, deleting, deteriorating, altering or suppression of data, or a data processing system, or its parts or components;
- Article 269E: Use of malicious software;
- Article 269F: Violation of personal data;
- Article 269G: Impersonation of websites to obtain personal data;
- Article 269H: Aggravating circumstances;
- Article 269I: Theft by computer and similar means;
- Article 269J: Unauthorised transfer of assets.

Source

2009 (amended)

COOPERATION

Multilateral Agreements

Budapest Convention

PARTY

Source

1 July 2004 (entry into force)

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

2014/2015

Expressed views to the Annual Report of the UN Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

2012, 2014, 2016

Colombia

Last Updated: April 2020

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

Cooperation, NATO-Colombia

Partnership aimed at developing common approaches to global security challenges, including cyber security.

Source

18 May 2017

Technical Assistance Mission, OAS-Colombia

Defense Ministry

Team of international experts sent by OAS to Colombia, to assist in a mission to improve cyber security.

Source

2014

Membership

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