



Venezuela (Bolivarian Republic of)

Last Updated: April 2020

CYBERSECURITY POLICY

STRUCTURE



National Centre or Responsible Agency

VenCERT

Ministry of Popular Power for University Education, Science and Technology (Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología)

- Main objectives include the prevention, detection and management of incidents related to information systems of the National Public Administration and public entities in charge of the management of critical infrastructures;
- Serves as the national coordinator for incident management;
- Also responsible to provide advice, support and training to ICT managers in State agencies or entities managing critical infrastructures, and to coordinate public and private initiatives related to ICT security through R&D projects, training, awareness-raising, and policy, standards and guidelines development.

[Source](#)

11 November 2008



Key Positions

Director General, Office of ICTs, Ministry of Popular Power for University Education, Science and Technology (Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología)

[Source](#)



Dedicated Agencies and Departments

División Contra Delitos Informáticos (Computer Crimes Division)

Center for Scientific, Penal and Criminal Investigations

Duties include: investigating computer crimes, study emerging forms of cybercrime, design strategies aimed at detecting organizations dedicated to illicit computer-related activities.

[Source](#)

7 October 2003



National CERT or CSIRT

VenCERT

Ministry of Popular Power for University Education, Science and Technology (Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología)

- Main objectives include the prevention, detection and management of incidents related to information systems of the National Public Administration and public entities in charge of the management of critical infrastructures;
- Serves as the national coordinator for incident management;
- Also responsible to provide advice, support and training to ICT managers in State agencies or entities managing critical infrastructures, and to coordinate public and private initiatives related to ICT security through R&D projects, training, awareness-raising, and policy, standards and guidelines development.

[Source](#)

11 November 2008



Venezuela (Bolivarian Republic of)

Last Updated: April 2020

LEGAL FRAMEWORK

Legislation

Ley de Infogobierno (Infogovernment Law)

National Commission of Telecommunications

Establishes the principles, bases and guidelines that govern the use of information technologies by public entities to foster transparency and promote security and defense of the country.

[Source](#)

October 2014

Ley Especial Contra Los Delitos Informáticos (Special Law on Computer Crimes)

Lists offences, including: unauthorized access; sabotage or damage to systems; sabotage of protected systems; espionage; forgery; violation of privacy.

[Source](#)

30 October 2001

Ley Sobre Mensajes de Datos y Firmas Electrónicas (Law on Electronic Signatures and Data Messages)

Recognizes the legal value of electronic signature, data messages and other information in electronic format.

[Source](#)

10 February 2001

COOPERATION

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

Membership



**International Telecommunications
Union (ITU)**



Organization of American States (OAS)



United Nations (UN)