

Judicial Police - National Unit to Combat Cybercrime and Technology Crime

The National Unit to Combat Cybercrime and Technological Crime, abbreviated by the acronym UNC3T, has the following competencies:

- A) Prevention, detection, criminal investigation and assistance of judicial authorities with regard to the crimes provided for in Law 109/2009, of 15 September;
- B) Prevention, detection, investigation and prosecution of judicial authorities in respect of crimes committed by means of resources or by means of computerized means, including:
 - i. In the Law of Protection of Personal Data;
 - ii. In the Code of Copyright and Related Rights, including interference and unblocking of forms of technological protection of goods and services;
- C) Prevention, detection, investigation and prosecution of the judicial authorities regarding crimes:
 - i. Against freedom and sexual self-determination, whenever practiced through or through computer systems;
 - ii. Debauchery through computer science;
 - iii. Computer fraud and communications;
 - iv. Concerning the interference and illegitimate manipulation of electronic and virtual means of payment;
 - v. Spying, when committed in the form of any computer program designed to carry out harmful actions which constitute an advanced and permanent threat.

2. The UNC3T shall ensure, in the framework of international cooperation, the permanent operational contact point provided for in Article 21 of Law 109/2009 of 15 September.

3 - The UNC3T collaborates and directly supports the actions of prevention, detection and mitigation developed by national entities with competences defined by law for the national security of cyberspace.

4 - UNC3T is also responsible for:

- A. To elaborate and maintain and up to date the National Plan of the Judicial Police for the Prevention and the Fight against Cybercrime, in particular, in articulation with the National Center of Cybersecurity;
- B. To execute protocols of technical and scientific collaboration with public and private entities, national or foreign, with previous approval of the national direction;
- C. Ensure the regular functioning of an informal advisory group for strategic, formative, legal, technical and scientific debate and advice on issues related to cybercrime, technological crime and cybersecurity;
- D. Ensure collaboration and direct participation in initial and ongoing training on cybercrime for staff of criminal investigation staff and support of the Judicial Police,

5 - In the UNC3T and under the dependence of its direction a technical and digital research team is created with the following functions:

- A. Optimize and manage the infrastructures and technological means assigned to the Unit;
- B. To support and advise, in technical, technological and legal terms, criminal investigation personnel in their investigations;
- C. Testing and developing specific tools for the investigation of cybercrime, technological crime and data decryption;
- D. Collecting, processing and disseminating data on cyber-intelligence to support investigations, international police cooperation and the prevention of cybercrime;
- E. To develop criminal counter information actions;
- F. Support technical actions for the collection of digital evidence, including covert actions and data interception;
- G. Support investigations requiring specialized technical expertise,

6 - UNC3T enjoys technical and scientific autonomy.