December 7, 2023

LEGAL ALERT

National Cybersecurity Policy 2023 – 2028 is published

On Monday 04 de December, Decree No. 164/2023 from the Ministry of the Interior and Public Security was published in the Official Gazette, approving the National Cybersecurity Policy that will be in force during the period 2023 - 2028, replacing the previous Policy, published on January 28, 2017, which was in effect between that same year and 2022.

The new Policy is established with the purpose of guiding the actions of the State in the field of cybersecurity, establishing an action plan, goals, and objectives in order to address the multiple challenges and obstacles faced by the country in this area. These challenges include the increase in cybercrimes, the vulnerability of infrastructure, and other relevant issues in cyberspace.

The novelties and innovations contained in the new Policy, compared to the previous one, are based on: (i) specific measures to address the main objectives; (ii) the inclusion of cross-cutting dimensions; and (iii) the relationship with other national objectives.

Specific Objectives of the Policy

To address the national issues related to cybersecurity, the new Policy focuses on five main objectives: a) resilient infrastructure; b) individuals' rights; c) cybersecurity culture; d) national and international coordination; and e) promotion of industry and scientific research. These objectives do not differ from those listed in the previous Cybersecurity Policy, but they do contain innovations, specifically regarding the particular measures to address each objective, which are outlined below.

1) Resilient Infrastructure

The Policy aims to strengthen the technical, physical, and logical elements of cyberspace, for which it considers essential:

- Promoting the processing of the framework bill on cybersecurity and critical information infrastructure, which establishes the National Cybersecurity

Agency.
- Strengthening the analysis of network information in cyberspace through investment in applied scientific research.

2) Rights of Individuals

The Policy aims for all individuals to be able to use the internet for various purposes in an environment of equity, inclusion, justice, and protection of diversity. To achieve this, it deems necessary:

- Strengthening the regulatory framework on personal data protection through the approval and implementation of the respective bill.
- Creating training opportunities for public officials on habits and basic digital security measures.
- Preventing the commission of cybercrimes.
- Identifying and correcting disparities in access to and use of cyberspace caused by a lack of knowledge in digital security.

3) Cybersecurity Culture

The Policy aims to develop a cybersecurity culture concerning education, good practices, and responsibility in handling digital technologies. To this end, it is considered necessary to:

- Design and implement a national awareness plan on cybersecurity and privacy.
- Generate and implement a core plan for the introduction and improvement of education in cyber hygiene and cybersecurity within the educational system from elementary to middle levels.
- Promote a culture of risk assessment and management within organizations.
- Encourage applied scientific research in cybersecurity to address future challenges the country may face.

4) National and International Coordination

The Policy promotes collaboration among public and private entities, as well as other governmental sectors and the industry, in conjunction with the future national cybersecurity authority. To achieve this goal, the policy highlights the importance of:

- Creating instances of collaboration and cooperation between public and private organizations in various fields.
- Establishing cooperative relationships with cybersecurity institutions in

advanced countries in the field.
- Actively promoting cyber diplomacy.
- Coordinating international cybersecurity policies.

5) Promotion of Industry and Scientific Research

Finally, the Policy promotes the development of a cybersecurity industry through:

- Focusing applied research on cybersecurity issues.
- Creating incentives for technological entrepreneurship in cybersecurity.
- Reviewing mechanisms for the procurement of cybersecurity services by the State.
- Promoting products and services from local cybersecurity companies nationally and internationally.
- Encouraging the integration and inclusion of gender mainstreaming in the development of the cybersecurity ecosystem.

Transversal Dimensions

A new element in relation to the previous policy is the establishment of four cross-cutting dimensions that must be considered in all initiatives aimed at protecting and promoting the rights of individuals:

- Gender equity
- Child protection
- Elderly protection
- Environmental protection

Relationship with Other National Objectives

The new Policy, in turn, considers three other policies that have been issued by the executive branch to address national objectives: a) Cyber Defense Policy; b) National Policy on Artificial Intelligence; and c) National Policy against Organized Crime.

The Cybersecurity Policy indicates being in close harmony with these latter policies, particularly by focusing on the planning and regulation of technologies in general, where cybersecurity holds great relevance.

Authors: Guillermo Carey; José Ignacio Mercado