/Carey

May 3, 2023

LEGAL ALERT

Bill that establishes a Framework Law on Cybersecurity advances in Congress

On April 26th, 2022, the Senate unanimously approved in particular (first constitutional procedure) the Bill that establishes a Framework Law on Cybersecurity and Critical Information Infrastructure. As a result, the legislative proposal passed to the second constitutional procedure waiting to be discussed by the Chamber of Deputies.

The project aims to establish the institutions, principles and general regulations that allow structuring, regulating, and coordinating cybersecurity actions of State Administration bodies and between them and individuals, as well as establishing the minimum requirements for the prevention, control, resolution, and response to cybersecurity incidents and cyberattacks.

The main elements of the project are listed below:

- **Institutionality.** The initiative contains a strong institutional focus, creating the **National Cybersecurity Agency** ("ANCI"), the Multisectoral Council on Cybersecurity and the** Computer Security Incident Response Teams **(National, Defense and Sectoral "CSIRTs"). The National Cybersecurity Agency will be a technical and specialized public service with regulatory, supervisory, and sanctioning powers. The Agency will regulate the actions of the State Administration agencies and private institutions in cybersecurity matters.
- **Operators of vital importance.** The Agency shall determine the services that are essential and shall identify within these the operators of vital importance, in accordance with the criteria established by law. These entities are subject to specific duties, including the obligation to implement information security management systems, develop and maintain business continuity plans and designate a cybersecurity delegate, among others.
- **General duties.** The bill will compel all State Administration bodies and private institutions to adopt the necessary measures to prevent, report and resolve cybersecurity incidents; to manage the associated risks; and to

contain and mitigate the impact that incidents may have on the operational continuity, confidentiality and integrity of the services provided. In addition, it establishes the prohibition to make payments of any kind in the event of digital kidnapping or ransomware attacks.

- **Duty to report cybersecurity incidents and cyberattacks.** All entities, whether public or private, except those exempted by the Agency, shall report within 3 hours to the National CSIRT cyberattacks and cybersecurity incidents that may have significant effects. They must also report their action plan as soon as it has been adopted.
- **Infringements and penalties.** The project sets forth categories of infringement (minor, serious and very serious), as well as the penalties associated with them, with fines of up to UTM 20,000 (USD 1,500,000.00 approx.).

Authors: Guillermo Carey; José Ignacio Mercado; Iván Meleda