March, 2022

BILL THAT ESTABLISHES A FRAMEWORK LAW ON CYBERSECURITY AND CRITICAL INFORMATION INFRASTRUCTURE ENTERS CHILEAN SENATE

On March 15th, 2022, the Bill that establishes a Framework Law on Cybersecurity and Critical Information Infrastructure was presented in the Senate.

The bill is structured around ten titles and forty-one articles, together with seven transitory articles, and aims to:

"*Establish the institutions, principles and general regulations that allow structuring, regulating and coordinating the cybersecurity actions of the State Administration bodies and between them and individuals; to establish the minimum requirements for the prevention, containment, resolution and response to cybersecurity incidents; to establish the attributions and obligations of the State bodies as well as the duties of private institutions that possess information infrastructure qualified as critical and, in both cases, the mechanisms of control, supervision, and responsibility for the infringement of the regulations.*"

Thus, the framework law bill establishes a series of definitions and principles, but also has a strong institutional focus, creating the **National Cybersecurity Agency**, establishing its duties and its basic institutional organic (art. 8), as well as the institutionalism and division of the work of both the **Technical Council of the National Cybersecurity Agency** and the **various CSIRTs (Computer Security Incident Response Teams)**, which are organized by area, and may be sectoral (constituted by sectoral overseers or regulators in their respective areas), or public sector (National, Government and Defense CSIRTs).

In addition to this, the project includes criteria and guidelines for the determination of **critical information infrastructure**, which entails specific obligations for the entities that manage such infrastructure, whether public or private, which must, for example, "*permanently apply the necessary technological, organizational, physical and information security measures to prevent, report and resolve cybersecurity incidents and manage risks, as well as contain and mitigate the impact on the operational continuity, confidentiality and integrity of the service provided*".

That said, it is important to note that the bill gives particular importance to 'sectorial' regulation and supervision, even recognizing the power of sectorial regulators and supervisors to issue general rules, circulars, technical standards, etc., in order to establish cybersecurity standards, which must consider the standards of the National Cybersecurity Agency (art. 7).

Carey y Cía. Ltda.
Isidora Goyenechea 2800, 43rd Floor.
Las Condes, Santiago, Chile.
www.carey.cl

Finally, the bill also creates a National Registry of Security Incidents (art. 16) in which the technical data and background information necessary to describe the occurrence of a security incident, with its study analysis, will be entered. Said information will be confidential. With regard to the CSIRTs (whether sectoral or public sector), a duty of confidentiality of important information is also established, which extends even to officials and persons who have become aware of sensitive information that are not part of the Agency).

AUTHORS: *Guillermo Carey, José Ignacio Mercado.*