March 03, 2025

Entry into Force of Key Provisions of the Cybersecurity Framework Law and Publication of Complementary Regulations in the Official Gazette

On March 1, 2025, **the pending provisions of Law No. 21,663, known as the Cybersecurity Framework Law, came into effect.** These provisions had been deferred until this date as established in Decree with Force of Law No. 1-21,663, published on December 24, 2024.

The provisions that came into force include:

1. **Article 5**: Qualification of operators of vital importance.
2. **Article 8**: Specific duties of operators of vital importance.
3. **Article 9: Obligation to report to the National CSIRT** (Computer Security Incident Response Team) any cyberattacks and cybersecurity incidents that may have significant effects.
4. **Title VII:** Regime of sanctions and infractions.

With the enactment of these provisions, as of this date, public and private institutions that provide essential services, as well as operators of vital **importance, are required to notify the National CSIRT of any cyberattack or cybersecurity incident that may have a significant effect, in accordance with Article 9 of the law.**

In line with this obligation, on March 1, 2025**, two regulatory documents were published in the Official Gazette,** outlining the requirements and procedures to comply with the incident reporting duty:

1. **Supreme Decree No. 295 of 2024 from the Ministry of the Interior and Public Security,** which approves the Cybersecurity Incident Reporting Regulation of Law No. 21,663. This decree establishes, among other aspects, **the minimum content that cybersecurity incident reports must contain and the obligations of public and private institutions that provide essential services**, as well as operators of vital importance, to report to the National CSIRT any cyberattacks and cybersecurity incidents that may have significant effects.
2. **Exempt Resolution No. 7 of 2025 from the National Cybersecurity Agency.** This resolution approves the taxonomy of cybersecurity incidents, classifying them into various categories according to their nature and effect. It also details the process and means for reporting to the National CSIRT, including the official platform available at **https://portal.anci.gob.cl, operational 24 hours a day, every day of the year.**

The publication of these documents in the Official Gazette complements the regulatory framework applicable to the mandatory reporting of cybersecurity incidents set forth in the Cybersecurity Framework Law, **establishing the criteria and procedures that obligated entities must follow to comply with this legal obligation.**

AUTHORS: *Guillermo Carey, José Ignacio Mercado, Iván Meleda.*

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