Legal Newsletter

March 2025

This newsletter contains the principal laws published, as well as decrees or general effect resolutions and regulations issued during the period. All of the above, in matters that may affect the various sectors where foreign investment is developed in Chile.

The information provided herein is for guidance purposes only and does not replace the information provided or interpretations made by the competent authorities on each matter.

Noteworthy Decrees and Resolutions

MARCH 2025

Exempt Resolution No. 7, of 2025, issued by the National Cybersecurity Agency ANCI)	Approves cybersecurity incident taxonomy
SUBJECT	Cybersecurity
PUBLICATION DATE	03-01-2025

The National Cybersecurity Agency (ANCI) has issued a resolution approving the cybersecurity incident taxonomy, establishing a framework for the classification and reporting of such events. This resolution is issued within the context of Cybersecurity Framework Law No. 21.663 and Supreme Decree No. 295, of 2024, issued by the Ministry of the Interior and Public Security, which regulates incident reporting and the response to digital threats.

The resolution requires public and private institutions that provide essential services, as well as operators of vital importance, to report cyberattacks and cybersecurity incidents that may have significant impacts to the National Cybersecurity Incident Response Team (CSIRT), as established in Law No. 21.663. Reports must include a description of the incident, classified according to observable impacts, and must be submitted through the platform provided by the National Cybersecurity Agency, available 24 hours a day, 365 days a year.

Additionally, specific criteria are established to assess the criticality of each incident and its impact on the operational continuity of the affected systems.

The incident taxonomy is structured into four areas of impact: 1. Illegitimate use of resources (e.g., unauthorized use of networks and IT systems); 2. Compromise of information confidentiality (e.g., exfiltration of personal data); 3. Disruption of essential services (e.g., denial-of-service attacks); 4. Alteration of information integrity (e.g., unauthorized modification of data).

Each of these areas is broken down into specific observable impacts and incident categories, providing a guide for the accurate identification and classification of cybersecurity incidents.

Decree No. 295, of 2024, issued by the Ministry of the Interior and Public Security	Approves regulations for cybersecurity incident reporting under Law No. 21.663
SUBJECT	Cybersecurity
PUBLICATION DATE	03-01-2025

These regulations aim to develop the regulatory framework for reporting cyberattacks and cybersecurity incidents that may have significant impacts, in accordance with the provisions of Cybersecurity Framework Law No. 21.663.

The regulations define several key concepts, such as “state administration”, “agency”, “cyberattack”, “cybersecurity incident”, and “operators of vital importance” in order to establish precise terminology for implementing the law. They also outline the obligation of public and private institutions that provide essential services, as well as those that have been classified as operators of vital importance, to report cybersecurity incidents.

Additionally, the regulations establish a reporting procedure which includes the submission of an early alert within three hours of becoming aware of the incident, a second report within the following 72 hours, and a final report within 15 days.

They also allow for partial reports to be submitted in the event of prolonged incidents, and require that reports be updated as necessary.

Furthermore, the regulations address the protection of personal data, establishing the obligation for all personal data or information to be omitted in reports, in compliance with Law No. 19.628 on the Protection of Private Life.

They also set out provisions for the incident reporting platform, which must be operational 24 hours a day, 365 days a year, and for the general instructions to be issued by the National Cybersecurity Agency to ensure proper reporting and receipt of reports.

Finally, the regulations contain transitory provisions governing their entry into force and the gradual implementation of electronic notifications.

The regulations will take effect from the date on which the National Cybersecurity Agency (ANCI) initiates its operations, and electronic notifications will be introduced in accordance with the gradual implementation rules provided in Decree with Force of Law No. 1, of 2020, issued by the Ministry of the Secretary General of the Presidency.

Decree No. 285, of 2024, issued by the Ministry of the Interior and Public Security	Approves the regulations for the classification process for operators of vital importance under Law No. 21.663
SUBJECT	Cybersecurity
PUBLICATION DATE	03-13-2025

These regulations aim to govern the process through which the National Cybersecurity Agency (ANCI) will determine which essential service providers, and which private institutions that are not considered essential service providers, will be classified as operators of vital importance.

The regulations set out the criteria that the agency must consider when designating an entity as an operator of vital importance. These criteria include dependence of the service on IT networks and systems, the significant impact that disruption could have on public safety and order, redundancy or single-source provision of the service, interdependence between services, and the relevance of the affected institution.

The classification process involves several stages, including the creation of a preliminary list of operators of vital importance, requests for technical reports from relevant sectoral bodies, a public consultation regarding private institutions, and the creation of a final list of classifying institutions. Deadlines are established for each stage, and the regulations outline the means by which private institutions and the general public may submit feedback during the process.

Being classified as an operator of vital importance entails a series of obligations and responsibilities in terms of cybersecurity, as established under Law No. 21.663.