LEGAL ALERT

Cybersecurity Incident Reporting Obligation to Become Effective

March 10th, 2025

Cariola Díez Pérez-Cotapos

Legal Alert Cybersecurity Incident Reporting Obligation to Become Effective

On Saturday, March 1, the obligation to report cyberattacks or cybersecurity incidents under **Law No. 21,663 cybersecurity framework (LMC)** came into force. Likewise, on that day, Resolution 295/2024 **was published in the Official Gazette,** which approves the regulation for reporting cybersecurity incidents, and **Resolution Ex. 7/2025**, which sets the taxonomy of incidents.

Obliged Entities: Entities qualified as essential service providers (PSE) or operators of vital importance (OIV).

PSE refers to any entity, regardless of its size,that provides any of these services: (a) electricity generation, transmission, and distribution; (b) fuel transportation, storage, and distribution; (c) water supply and wastewater treatment; (d) telecommunications, digital infrastructure, and IT services; (e) land, air, rail, and maritime transportation and infrastructure operation; (f) banking, financial services, and payment systems; (g) social security administration, including AFP, AFC, Isapres, and employer mutuals; (h) postal and courier services; (i) healthcare providers such as hospitals, clinics, and medical centers; and (j) pharmaceutical production and research.

The National Cybersecurity Agency (ANCI) will define the entities that will be considered OIVs, which has not ocurred yet.

Incidents to be reported: Any **cyberattack or cybersecurity incident with significant effects.**

- A cybersecurity incident is considered to have a **significant effect** if it is capable of producing **any of the following effects:** Interrupt the continuity of an essential service. Both the services delivered by suppliers, as well as the supply chain, of an entity that provides essential services or of a vital operator, must be considered.
- Affect the physical integrity or health of people.
- Affect the integrity or confidentiality of computer assets, or the availability of any network or computer system, even when this does not produce or has produced an immediate impact on the provision of the service.
- Using or entering computer networks or systems without authorization, even when this does not produce or has produced an immediate impact on the provision of the service.
- Affect computer systems that contain personal data.

How to report: The report of a cyberattack or cybersecurity incident with significant effects must be sent to the National Computer Security Incident Response Team (CSIRT Nacional) through the following channels:

Via reporting platform: https://portal.anci.gob.cl for which the ClaveÚnica of the person reporting is required. (ClaveÚnica is a digital credential issued by the Chilean State that allows citizens to access online services and procedures from various public institutions).

Alternative channels: The ANCI has informed that the following channels will remain available to report and communicate with the ANCI in case of contingencies: telephone (only in Chile) 1510, email ayuda@anci.gob.cl

Content of the report: The report must contain the information indicated in Resolution 295, including the affected entity, contact details of the cybersecurity delegate, information about the incident (date, time,

indications of the occurrence, potentially affected assets and resources, indicators of compromise), whether the action is classified as a crime, repercussions to other entities and any other data that is useful for the management of the incident.

The description of the incident must consider the **taxonomy of incidents indicated in Resolution Ex. 7/2025**, which contemplates four areas of impact and eleven observable effects.

Deadline for reporting: Once the entity has become aware of the occurrence of a cybersecurity incident, it must send an alert about its occurrence within a **maximum period of 3 hours from the time it becomes aware** of the incident. Then, after the maximum period of **72 hours**, it must send a **second report** to the National CSIRT and within a maximum period of **15 calendar** days from the sending of the early warning, the entity must prepare a final report.

Penalties: Failure to report cyberattacks or cybersecurity incidents is a serious infraction under the LMC, which is punishable by a fine of up to 10,000 UTM equivalent to approximately USD 715,396. Once the entities classified as OIV are defined, they may be sanctioned with a fine of up to 20,000 UTM, equivalent to approximately USD 1,415,277.

Reporting obligation relationship at the sectoral level

In the event that the obligated subject of LMC has the obligation to report incidents based on the sectoral regulation that is applicable to it (for example, in banking, financial or telecommunications matters), it must also comply with such obligation in the terms and forms established by the sectoral regulations.

Recommendations:

- Designate a person responsible for reporting incidents who has a ClaveÚnica, duly trained on the obligations of the LMC.
- Generate an action protocol in the event of cyberattacks or cybersecurity incidents with significant effects, which includes:

(a) Mechanisms for immediate detection and response, establishing procedures for the early identification of threats and the activation of containment measures to prevent their spread;

b) Mandatory notification process to the National CSIRT and the sectoral regulator if there is a reporting obligation, ensuring compliance with the reporting deadline(s);

c) Classification of the incident, according to the taxonomy defined by the ANCI, and the sectoral regulator if there is an obligation, considering its impacts on confidentiality, integrity and availability;

d) Mitigation and recovery plan, which includes immediate actions for the containment of the incident, the restoration of essential services and operational continuity;

(e) Detailed record of the incident and action taken; and

f) Training and periodic exercises, aimed at strengthening organizational resilience and optimizing the response to future incidents.

Contacts:

Carolina Filsfisch
Partner

Gabriel Pensa
Senior Associate

Eduardo Vilches
Senior Associate