04 de abril de 2024

# Cybersecurity Framework Law is published in the Official Gazette



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

On April 8th, 2024, Law No. 21,663 Cybersecurity Framework Law (the "Law") was published in the Official Gazette, after being enacted by the President of the Republic on March 26th, 2024..

The new Law entails the implementation of relevant aspects and changes in cybersecurity, which includes a series of effects and consequences, which are detailed below:

## I. *The Law: Five points to keep in mind*

### 1.- New institutionality

First, the Law implements a new institutional framework in this area, by creating the (i) *National Cybersecurity Agency* ("ANCI"); (ii) *Multisectoral Council on Cybersecurity* ("Council"); (iii) *the Interministerial Committee on Cybersecurity* ("Committee"); and (iv) *Computer Security Incident Response Teams* (each, "CSIRTs"), including the National CSIRT, the National Defense CSIRT, and other CSIRTs of State Administration agencies.

Regarding the **ANCI**, it will correspond to a decentralized public service, of a technical and specialized nature, whose main objectives will be to advise the President of the Republic on matters of cybersecurity, collaborate in the protection of national interests in cyberspace, coordinate the different institutions with competence in cybersecurity, ensure the protection, promotion and respect for computer security, among others.

In order to comply with the objectives indicated, the ANCI will have various attributions, among which are, (i) **regulatory powers**; (ii) **supervisory powers**; and (iii) **sanctioning powers**; among others.

The Law also provides for regulatory coordination mechanisms between the ANCI and sectoral entities in the event that the protocols, technical standards or general instructions it issues in the exercise of its functions have effects in the areas of competence of such sectoral entities. Sectoral authorities may also issue general regulations, technical standards, and instructions necessary to strengthen cybersecurity of institutions of their sector, in accordance with the respective regulation and in coordination with ANCI.

### 2.- Principles governing cybersecurity regulation

The Law introduces several principles that obligated institutions (indicated in point 3 below) must observe in their conduct. Some of these principles are: (i) damage control; (ii) cooperation with the authority; (iii) responsible response; (iv) computer security; (v) reasonableness; and (vi) security and privacy by default and by design.

### 3.- Scope of application

The Law will apply to institutions providing **services classified as "Essential",** on the one hand, and to those classified as **Operators of Vital Importance**, on the other.

As for Essential Services, these correspond to:

1. Those that are provided by the State Administration Bodies and by the National Electricity Coordinator.
2. Those provided under a concession under public law.
3. Those that are provided by private institutions that carry out the following activities:
    a. Generation, transmission or distribution of electricity;
    b. Transport, storage or distribution of fuels; supply of drinking water or sanitation;
    c. Telecommunications;
    d. Digital infrastructure;
    e. Digital services, information technology services managed by third parties;
    f. Land, air, rail or maritime transport, as well as the operation of their respective infrastructure;
    g. Banking, financial services and means of payment;
    h. Administration of social security benefits;
    i. Postal and courier services;
    j. Institutional provision of health care by entities such as hospitals, clinics, doctors' offices and medical centers;
    k. Production and/or research of pharmaceutical products.
    l. Other services that the ANCI may qualify as "Essential" by means of a reasoned decision of the National Director when their affectation may cause serious damage to the life or physical integrity of the population or its supply, to relevant sectors of the economic activities, to the environment, to the normal functioning of society, of the State Administration, to the national defense, or to the security and public order.

For its part, ANCI will be responsible for determining the providers of essential services that are qualified as operators of vital importance by means of a reasoned decision, that complies with the following requirements: (i) that the provision of such service depends on the networks and information systems; and (ii) that the affectation, interception, interruption or destruction of its services has a significant impact on security and public order; on the continuous and regular provision of essential services; on the effective fulfillment of the functions of the State; or, in general, of the services that the State must provide or guarantee.

Likewise, ANCI shall have the power to qualify private institutions that, although they do not have the quality of providers of essential services, also meet the requirements set forth in the preceding paragraph under certain assumptions.

### 4.- Cybersecurity obligations

Regarding the obligations contemplated by the Law, on the one hand, there are the **general duties**, applicable to both providers of Essential Services and those considered Operators of Vital Importance, which are obliged to:

1. **Duty to report to the National CSIRT cyberattacks and cybersecurity incidents that may have significant effects** under the terms of the Law, as soon as possible, within a maximum period of three hours, and in accordance with the other criteria and formalities established by the Law.
2. **Duty to permanently apply measures to prevent, report and resolve cybersecurity incidents**, which requires the implementation of the protocols and standards established by the ANCI, and the respective sectoral regulation.

On the other hand, the Law introduces **specific duties for Operators of Vital Importance**, who will be obliged, among other duties, to the following:

1. Implement an information security management system;
2. Develop and implement operational continuity and cybersecurity plans;
3. Carry out review operations, exercises, drills and analysis of computer networks and systems that compromise cybersecurity;
4. Take the necessary measures to reduce the impact and spread of a cybersecurity incident;
5. Obtain the cybersecurity certifications provided for by law; and
6. Have training, education and continuous education programs for its workers and collaborators, including cyber hygiene campaigns.

### 5.- Infractions and associated penalties

The Law provides for various penalties for non-compliance with its provisions, which are classified into 3 categories: **minor**, **serious,** and **very serious**.

By way of example, the law will consider as **minor** the late delivery of the information required by the ANCI that is not necessary for the management of a cybersecurity incident, as **serious** as the failure to comply with the obligation to report and as a **very serious** infraction, the delivery of manifestly false or erroneous information to the ANCI, and that it has been necessary for the management of a cybersecurity incident.

The Law also provides for specific infractions and penalties for non-compliance with the specific duties of Operators of Vital Importance.

As for the penalties provided for in the Law, these translate into the imposition of a fine for tax benefit:

1. Minor offences: Fine of up to 5,000 Monthly Tax Units (“UTM”);
2. Serious offences: Fine of up to 10,000 UTM; and
3. Very serious offences: Fine of up to 20,000 UTM.

In the case of Vital Operators of Vital Importance, these fines can even be up to double.

## II. *Next Steps & Effective Date (What's Coming)*

The President of the Republic must issue, within one year of the publication of the future law, one or more executive law decrees to determine a period for the entry into force of the rules of the future law, which may not be less than six months from the publication of the future law, the date of initiation of the activities of ANCI, among other matters.

***AUTORES:*** *Guillermo Carey, José Ignacio Mercado, Stefano De Cristofaro, Iván Meleda. Ricardo Alonso*