/Carey

April 2026

ANCI PUBLISHES SECOND PRELIMINARY LIST OF VITAL IMPORTANCE OPERATORS

On April 24, 2026, the National Cybersecurity Agency (ANCI) published in the Official Gazette the resolution approving the second preliminary list of Vital Importance Operators (VIOs), corresponding to the second stage of the first qualification process initiated in 2025.

This list includes both public and private entities providing essential services across multiple strategic sectors, significantly expanding the scope of organizations potentially subject to the enhanced cybersecurity regime established under Law No. 21,663 and its implementing regulation.

Sectors covered:

- Fuel transport, storage, or distribution.
- Drinking water supply and sanitation.
- Land, air, rail, or maritime transport and related infrastructure.
- Public service concessionaires.
- Social security administration.
- Postal and courier services.
- Pharmaceutical production and/or research.
- Essential services previously identified but not included in the first list, including electricity generation and distribution, telecommunications, digital infrastructure, IT services, healthcare providers, and government entities.

Deadline for observations:

Entities included in the preliminary list have 30 days from publication to submit observations and supporting documentation, pursuant to Article 13 of the regulation (Supreme Decree No. 285/2024).

Public consultation:

The resolution also initiates a public consultation process, for which ANCI will make available an electronic platform, in accordance with Article 11 of the regulation.

This news alert is provided by Carey y Cía. Ltda. for educational and informational purposes only and is not intended and should not be construed as legal advice.

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

Regulatory implications:

Entities ultimately designated as VIOs will be subject to enhanced cybersecurity obligations, including:

- Risk governance frameworks.
- Incident detection and response capabilities.
- Operational continuity measures.
- Mandatory incident reporting to the National CSIRT.

This second list represents a significant step in the implementation of Chile's cybersecurity framework, expanding the scope of regulated entities and anticipating operational and compliance requirements that will demand early preparation.

Authors: Guillermo Acuña; José Ignacio Mercado; Jaime Henríquez; Iván Meleda; Jorge Calvo