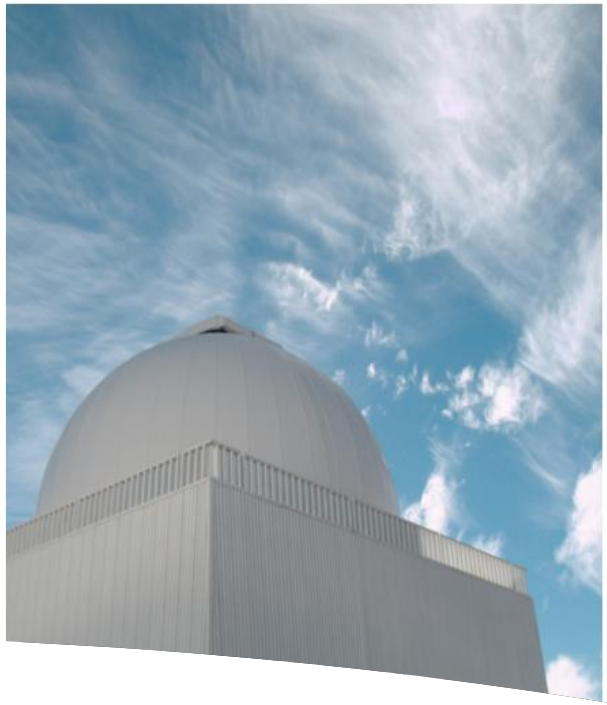
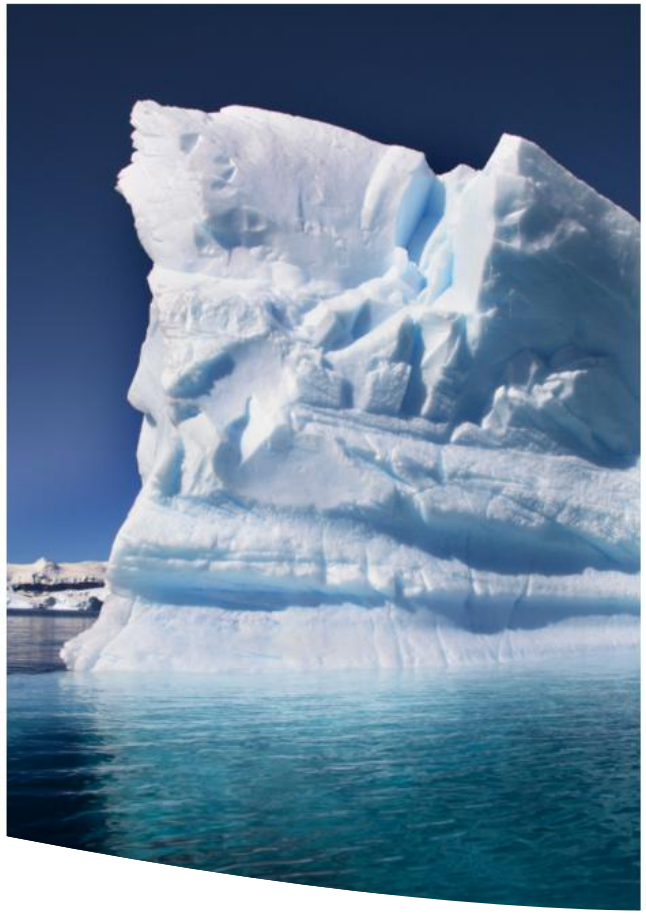
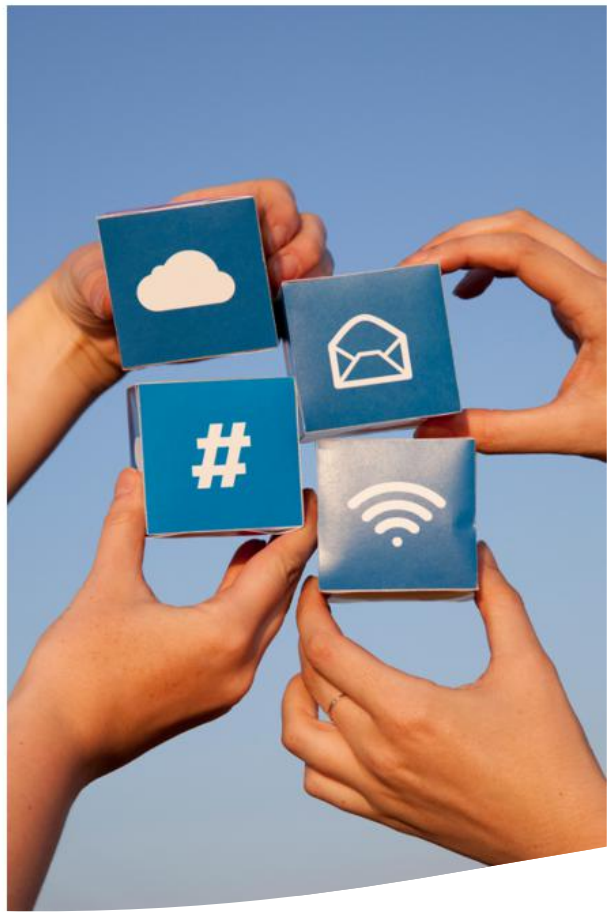


Chilean Cybersecurity Framework Law: An Opportunity to Strength Cybersecurity Services

Alejandro Lara - Cybersecurity & IT Services Engineer

REUNA
Ciencia y Educación en Red

Chilean Cybersecurity Framework Law

Key aspects (1) - Objective and Institutions

- Chilean Law 21.663[1] establishes a national framework to strengthen cybersecurity, protect critical infrastructure, and coordinate public and private response to cyber incidents.

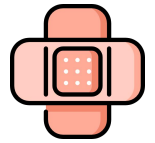
Key Institutional Elements

- ANCI: National Cybersecurity Agency
  - Autonomous public agency under the Ministry of the Interior.
  - Central authority for cybersecurity coordination, regulation, and supervision.
  - Issues binding technical regulations and oversees compliance.
  - Operates the National CSIRT and coordinates incident response at national level.

[1] https://www.bcn.cl/leychile/navegar?idNorma=1202434 (In Spanish)

Key aspects (2) - Service Operators and Reporting

- Essential Services Providers (ESP):
  - Entities (public or private) delivering critical services (e.g., energy, transport, water, finance, **telecom, health, pharmaceutical research, digital infrastructure**).
  - Must implement cybersecurity risk management frameworks and notify incidents.
  - Subject to ANCI's supervision and audits.
- Operators of Vital Importance (OVI):
  - Organizations whose systems' disruption could seriously affect national security or public order.
  - Require stricter security measures and periodic compliance certifications.
  - Must ensure 24/7 incident detection and response capabilities.
- Incident Reporting:
  - Immediate notification to ANCI upon detecting a cybersecurity incident.
  - Incidents are classified by severity; reporting deadlines vary by category.
  - ANCI may order containment, mitigation, or public communication measures.



The Opportunity

Strenghtening the R&E Cybersecurity in Chile

Services' development

Support to innovative ideas/projects

Collaboration

Training/Awareness activities

Services focused on the R&E community

- CSIRT.REUNA[2]: An open CSIRT for all the Chilean R&E institutions.

  Main goal: To support the resolution and/or mitigation of reported cybersecurity incidents, coordinate communication and response efforts with national and international stakeholders, and promote awareness and training activities.

Services for REUNA partner institutions[3]

- eduSCAN: Vulnerability scanning and mitigation platform.
- eduAware: Institutional awareness and training platform.

[2] https://csirt.reuna.cl/ (In Spanish)

[3] https://www.reuna.cl/servicios/identidad-y-seguridad/ (In Spanish)

Supporting innovative initiatives

- **Cybersecurity Core Competencies Program [4]**: A program featuring a competency framework and a tool for measuring and certifying those competencies - UV / ULagos / ICDT
- **Intrusion.aware**: Comprehensive platform for detecting and responding to cyberattacks using artificial intelligence - UAI

[4] https://www.reuna.cl/programa-competencias-esenciales/ (In Spanish)

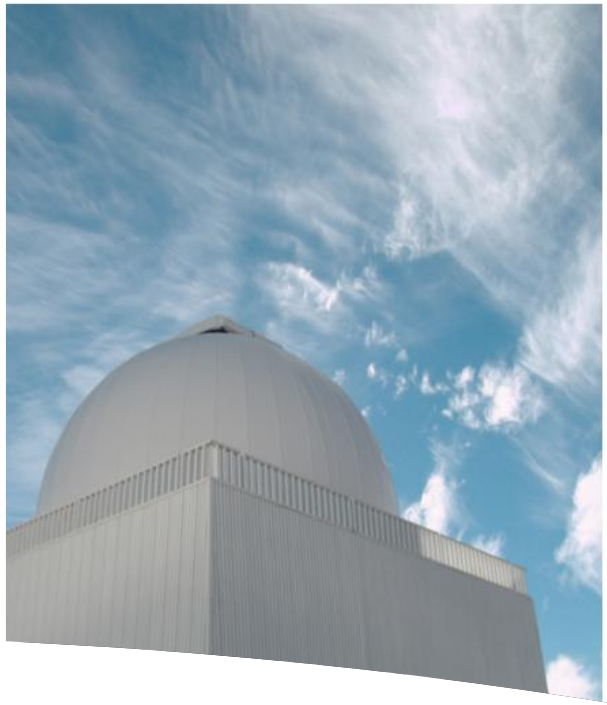
National & International Collaboration

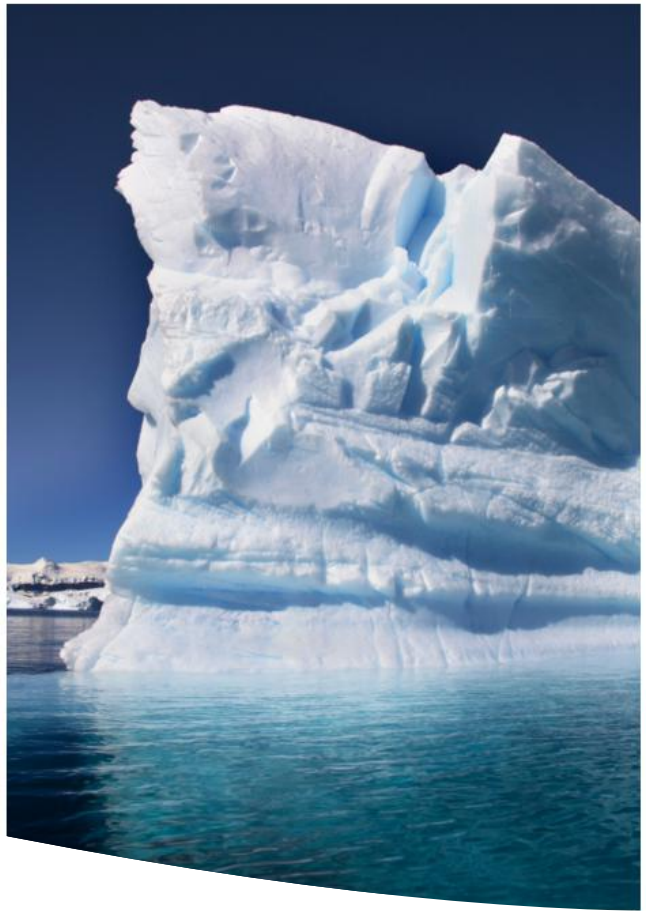
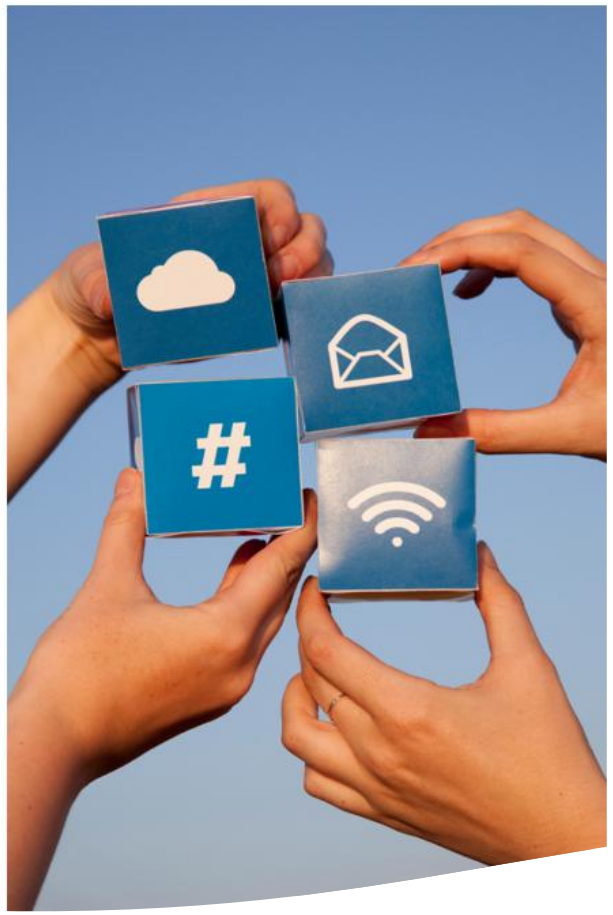
- REUNA Partner institutions
- Government
- NRENs
- Other organizations

Training and Awareness Activities [5]

- Open Webinars
- Technical workshops
- Legal workshops
- Courses

[5] https://csirt.reuna.cl/taller/ (In Spanish)



Thanks

Alejandro Lara
Cibersecurity & IT Services Engineer
alara@reuna.cl

REUNA
Ciencia y Educación en Red